PROCESSO LICITATÓRIO
PREGÃO ELETRÔNICO 006/2024
[UASG 926470 – PE 90006/2024]

Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP). Portaria da Presidência nº 38/2024, de 6 de fevereiro de 2024;

Agente de Contratação/Pregoeiro:
- **CARLOS ALBERTO KASPER,** Analista Legislativo;

Equipe de Apoio:
- **CRISTINA ITO DE LIMA,** Agente Administrativo;
- **RICARDO ANDRADE,** Analista Legislativo;
- **CLAUDIA CRISTINA DE ARAUJO**, Agente Administrativo.

PORTARIA DA PRESIDÊNCIA Nº 038/2024

O Presidente da Câmara Municipal de Foz do Iguaçu, Estado do Paraná, no uso de suas atribuições legais e considerando o Ato da Presidência nº 130/2023, de 11 de dezembro de 2023,

RESOLVE

Art. 1º Designar, a contar de 28 de janeiro de 2024, o servidor **CARLOS ALBERTO KASPER**, matrícula nº 201.489, ocupante do cargo efetivo de Analista Legislativo VI, como ***PREGOEIRO*** / **AGENTE DE CONTRATAÇÃO** da Câmara Municipal de Foz do Iguaçu.
Art. 2º Delegar ao Pregoeiro / Agente de Contratação, além das funções pertinentes, a coordenação da fase interna da licitação e a competência para firmar os respectivos atos e os instrumentos convocatórios, com exceção do Edital.
Art. 3º Designar os servidores abaixo relacionados como Equipe de Apoio para auxiliar o pregoeiro / agente de contratação na condução dos trabalhos:

- **CRISTINA ITO DE LIMA**, matrícula nº 201.752, Agente Administrativo IV;
- **RICARDO ANDRADE,** matrícula nº 200.552, Analista Legislativo VII;
- **CLÁUDIA CRISTINA DE ARAÚJO**, matrícula nº 201.500, Agente Administrativo V.

Art. 4º Esta Portaria terá vigência de 1 (um) ano, a contar de 28 de janeiro de 2024.
Art. 5º Revogar, a contar de 28 de janeiro de 2024, as Portarias da Presidências nºs 23, 24, 27, 199 e 200/2023.

Gabinete do Presidente da Câmara Municipal de Foz do Iguaçu, 06 de Fevereiro de 2024.

JOÃO MORALES
Presidente

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: 491D-962C-C88B-B6AF

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

JOAO JOSE ARCE MORALES (CPF 029.XXX.XXX-16) em 06/02/2024 14:13:07 (GMT-03:00)
Papel: Parte
Emitido por: AC SyngularID Multipla << AC SyngularID << Autoridade Certificadora Raiz Brasileira v5 (Assinatura ICP-Brasil)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://fozdoiguacu.1doc.com.br/verificacao/491D-962C-C88B-B6AF

Proc. Administrativo 279/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: CMFI-DG-DIRADM - Diretoria de Administração

Data: 06/08/2024 às 11:28:15

Setores envolvidos:

CMFI-PRESID-DG, CMFI-PRESID-DG, CMFI-DG-ATDG-DIRJUR, CMFI-DG-DIRADM, CMFI-DG-DIRTEC, CMFI-PRESID-DG-DIRFIN-CON, CMFI-PRESID-DG-DIRFIN-COM, CMFI-DG-DIRTEC-ATDT, CMFI-DG-DIRTEC-EATI, CMFI-PRESID-DG-ATDG-DIRJUR-EADJ, CMFI-PRESID, CMFI-PRESID-DG-DIRFIN-COM-EC, CMFI-PRESID-DG-DIRFIN-GESTCON, AGCONT, AGCONT-EAAC

PL - Fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 meses

Considerando o processo anteriormente instruído de numero Proc. Administrativo 243/2024 - Fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 meses.Considerando os despachos de numero 10 e 15 contidos no processo citado.

Encaminha-se,

DFD referente a renovação de licenças da solução de segurança (Proteção Anti-Virus, Anti-Malware e Anti-Ransomware + EDR) , visando verificação de alinhamento junto ao PAC.

_

Rafael Sanches
Diretoria de Tecnologia

Anexos:

Formalizacao_da_Demanda_SOLSEG_2_.pdf

DOCUMENTO DE FORMALIZAÇÃO DA DEMANDA (DFD)

Identificação do Solicitante			
Servidor	Robson Gregório	Matrícula	200.538
Diretoria	Diretoria de Tecnologia	Setor	TI

1. Justificativa da necessidade da contratação

Em 2021 a Câmara Municipal renovou as 130 licenças do antivírus que possuía e adquiriu 20 novas licenças devido ao aumento de equipamentos.

Tendo em vista de que o nosso sistema de antivírus irá expirar no mês 09/2024, consequentemente não haverá mais atualizações disponíveis e nem suporte, tornando os equipamentos de informática desta casa de leis vulneráveis a novos ataques, podendo danificar tanto os softwares como os hardwares, trazendo prejuízos aos trabalhos realizados pelos servidores desta casa de leis.

Como exposto a cima

2. Quantitativo de material/serviço a ser contratado

ITEM	Descrição	Unidade	Quantidade
01	Renovação do sistema de antivírus	Unid.	160

Valor previsto para solução **R$ 70.000,00**

3. Indicação da data pretendida para ser iniciado o recebimento dos materiais ou a prestação do serviço

A estimativa de entrega desta contratação 28/08/2024.

4. Indicação de vinculação ou dependência com o objeto de outro documento de formalização de demanda

Os documentos que são vinculados são ETP e TR.

5. Indicação do CNAE relativo ao objeto

6209-1/00
SUPORTE TÉCNICO, MANUTENÇÃO E OUTROS SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO

6. Indicação dos responsáveis pelo planejamento da contratação

Responsável pela Elaboração do Documento de Formalização da Demanda:

- Robson Gregório – Técnico em Informática

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: EF90-1488-7F9C-CA99

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

ROBSON GREGÓRIO (CPF 784.XXX.XXX-53) em 16/07/2024 10:12:29 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://fozdoiguacu.1doc.com.br/verificacao/EF90-1488-7F9C-CA99

Proc. Administrativo 243/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: CMFI-DG-DIRADM - Diretoria de Administração - A/C Nei S.

Data: 16/07/2024 às 10:01:00

Encaminha-se,

DFD referente a renovação de licenças da solução de segurança (Proteção Anti-Virus, Anti-Malware e Anti-Ransomware + EDR) , visando verificação de alinhamento junto ao PAC.

_

Rafael Sanches
Diretoria de Tecnologia

Anexos:

Formalizacao_da_Demanda.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Robson Gregório	16/07/2024 10:12:31	1Doc	ROBSON GREGÓRIO CPF 784.XXX.XXX-53

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **EF90-1488-7F9C-CA99**

DOCUMENTO DE FORMALIZAÇÃO DA DEMANDA (DFD)

Identificação do Solicitante			
Servidor	Robson Gregório	Matrícula	200.538
Diretoria	Diretoria de Tecnologia	Setor	TI

1. Justificativa da necessidade da contratação

Em 2021 a Câmara Municipal renovou as 130 licenças do antivírus que possuía e adquiriu 20 novas licenças devido ao aumento de equipamentos.

Tendo em vista de que o nosso sistema de antivírus irá expirar no mês 09/2024, consequentemente não haverá mais atualizações disponíveis e nem suporte, tornando os equipamentos de informática desta casa de leis vulneráveis a novos ataques, podendo danificar tanto os softwares como os hardwares, trazendo prejuízos aos trabalhos realizados pelos servidores desta casa de leis.

Como exposto a cima

2. Quantitativo de material/serviço a ser contratado

ITEM	Descrição	Unidade	Quantidade
01	Renovação do sistema de antivírus	Unid.	160

Valor previsto para solução **R$ 70.000,00**

3. Indicação da data pretendida para ser iniciado o recebimento dos materiais ou a prestação do serviço

A estimativa de entrega desta contratação 28/08/2024.

4. Indicação de vinculação ou dependência com o objeto de outro documento de formalização de demanda

Os documentos que são vinculados são ETP e TR.

5. Indicação do CNAE relativo ao objeto

6209-1/00
SUPORTE TÉCNICO, MANUTENÇÃO E OUTROS SERVIÇOS EM TECNOLOGIA DA INFORMAÇÃO

6. Indicação dos responsáveis pelo planejamento da contratação

Responsável pela Elaboração do Documento de Formalização da Demanda:

- Robson Gregório – Técnico em Informática

Proc. Administrativo 1- 243/2024

De: Nei S. - CMFI-DG-DIRADM

Para: CMFI-DG-DIRADM - Diretoria de Administração

Data: 16/07/2024 às 10:46:59

Informo que o objeto e os valores estão previstos e adequados ao PAC

–

Nei Schlotefeldt
Consultor Legislativo

Proc. Administrativo 2- 243/2024

De: Nei S. - CMFI-DG-DIRADM

Para: CMFI-DG-DIRTEC-EATI - Tecnologia da Informação - A/C Jeverson S.

Data: 16/07/2024 às 10:49:09

Tendo em vista que os valores estão previstos no PA 2024, encaminho para Planejamento prévio

–

Nei Schlotefeldt
Consultor Legislativo

Proc. Administrativo 3- 243/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: CMFI-PRESID-DG-DIRFIN-CON - Contabilidade

Data: 16/07/2024 às 11:33:24

Para indicação da rubrica orçamentária.

–

Rafael Sanches
Diretoria de Tecnologia

Anexos:

1_Termo_de_Referencia_Minuta.docx
ETP.docx
Modelo_Pesquisa_de_Mercado_Media.xlsx

Assinado digitalmente (emissão) por:

Assinante	Data	Assinatura	
Rafael Sanches Alencar	16/07/2024 11:33:51	1Doc	RAFAEL SANCHES ALENCAR CPF 006.XXX.XXX-96

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **3D32-3444-9528-2296**

Proc. Administrativo 4- 243/2024

De: Nathalie N. - CMFI-PRESID-DG-DIRFIN-CON

Para: CMFI-DG-DIRTEC - Diretoria de Tecnologia - A/C Rafael A.

Data: 17/07/2024 às 09:48:54

Prezado,

Encaminho em anexo, Declaração de Adequação Orçamentária e Financeira e Demonstrativo da Despesa Realizada até 17/07/2024.

_

Nathalie Pereira Do Nascimento
Chefe da Contabilidade

Anexos:

DDR_17_07_2_.pdf
DECLARACAO_DE_ADEQUACAO_ORCAMENTARIA_E_FINANCEIRA_Processo_Administrativo_243_2024_Renovacao_de_licencas_K

DEMONSTRATIVO DA DESPESA REALIZADA COM PAGAMENTOS NO PERÍODO DE 01/01/2024 ATÉ 17/07/2024

DDR - Analítico

Orgão:01-CÂMARA MUNICIPAL DE FOZ DO IGUAÇU

Unidade:01-CÂMARA MUNICIPAL DE FOZ DO IGUAÇU

Dotação Orçamentária	Descrição da Dotação Orçamentária	Até o Período						No Período				Saldo Orc. Restante
		Orçado	Total	Bloqueado	Empenhado	Liquidado	Pago	Bloqueado	Empenhado	Liquidado	Pago	
		Alterações				Saldo a Liquidar	Consignado				Consignado	Saldo a Pagar
01.01.01.031.0001.2002	COORDENAÇÃO, SUPERVISÃO E ADMINISTRAÇÃO GERAL Recursos destinados a contribuição à ACAMOP (Associação das Câmaras Municipais do Oeste do Paraná) e a anuidade ao IBAM (Instituto Brasileiro de Administração Municipal) e Outros.	1.117.468,40	1.117.468,40	0,00	362.267,71	140.167,70	135.851,82	0,00	362.267,71	140.167,70	135.851,82	755.200,69
		0,00				222.100,01	4.194,84				4.194,84	222.221,05
3.3.90.40.00	SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PESSOA JURÍDICA											
1.001	Recursos do Tesouro (Descentralizados) Exercício Corrente	1.117.468,40	1.117.468,40	0,00	362.267,71	140.167,70	135.851,82	0,00	362.267,71	140.167,70	135.851,82	755.200,69
		0,00				222.100,01	4.194,84				4.194,84	222.221,05
Total da Unidade:		1.117.468,40	1.117.468,40	0,00	362.267,71	140.167,70	135.851,82	0,00	362.267,71	140.167,70	135.851,82	755.200,69
		0,00				222.100,01	4.194,84				4.194,84	222.221,05
	Total do Orgão:	1.117.468,40	1.117.468,40	0,00	362.267,71	140.167,70	135.851,82	0,00	362.267,71	140.167,70	135.851,82	755.200,69
		0,00				222.100,01	4.194,84				4.194,84	222.221,05
	Total Geral:	**1.117.468,40**	**1.117.468,40**	**0,00**	**362.267,71**	**140.167,70**	**135.851,82**	**0,00**	**362.267,71**	**140.167,70**	**135.851,82**	**755.200,69**
		0,00				222.100,01	**4.194,84**				**4.194,84**	**222.221,05**

Este relatório foi configurado na coluna no período para calcular somente estornos de transações que ocorreram no período. Desta forma estornos de transações que ocorreram anterior a este período não serão computadas.

DECLARAÇÃO DE ADEQUAÇÃO ORÇAMENTÁRIA E FINANCEIRA

Processo Administrativo 243/2024 – Renovação de licenças Kaspersky

.

Eu, **João Morales**, Presidente desta Casa Legislativa, na qualidade de Ordenador da Despesa e em cumprimento às determinações no inciso II do artigo 16 da Lei Complementar nº 101, de 04 de maio de 2000, **DECLARO QUE AS DESPESAS RELACIONADAS AO OBJETO EM QUESTÃO TÊM ADEQUAÇÃO ORÇAMENTÁRIA E FINANCEIRA COM A LEI ORÇAMENTÁRIA ANUAL E COMPATIBILIDADE COM O PLANO PLURIANUAL E COM A LEI DE DIRETRIZES ORÇAMENTÁRIAS.**

Conforme estabelecido, a despesa correspondente será empenhada na seguinte dotação orçamentária:

2024:		
Item:	**Dotação:**	**Total:**
1 . KASPERSKY NEXT EDR OPTIMUM - 36 meses	01.01.01.031.0001.2002.3.3.90.40.99.05 - AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE	R$ 64.820,80
O remanescente correrá pelas dotações orçamentárias consignadas na futura lei orçamentária		

Foz do Iguaçu, 17 de julho de 2024.

JOÃO MORALES
Presidente

Proc. Administrativo 5- 243/2024

De: Rodrigo N. - CMFI-DG-DIRTEC-EATI

Para: Envolvidos internos acompanhando

Data: 17/07/2024 às 11:04:18

Jeverson Siqueira - CMFI-DG-DIRTEC-EATIfavor assinar o ETP e dar seqüência no processo.

–

Rodrigo Nishimori
Administrador de Rede

Anexos:

ETP_2_.pdf

ESTUDO TÉCNICO PRELIMINAR

1) DESCRIÇÃO DA NECESSIDADE

1.1. Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

1.2. A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

1.3. Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

1.4. Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

1.5. Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

1.6. Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

1.7. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.

2) REQUISITOS DA CONTRATAÇÃO

Item	Descriçao	SKU	Quantidade
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160

3) LEVANTAMENTO DE MERCADO

Considerando que a Câmara Municipal de Foz do Iguaçu já dispõe de um sistema de antivírus, foram avaliadas duas alternativas sendo uma delas a renovação e upgrade de versão do sistema e a outra a aquisição de um sistema integrado com o nosso sistema de Firewall.

Mantendo os investimentos já realizados, tendo em vista de que além da aquisição do sistema, foi também realizado a contratação de uma empresa especializada para nos auxiliar na configuração recomendadas pelo fabricante, e com base nas pesquisa de preços e estudo entre outras soluções, optou-se pela renovação e upgrade da versão já utilizada do licenciamento da solução Kaspersky e aquisição de novas licenças para contemplar a necessidade do parque computacional da CMFI, levando em consideração a ampliação do nosso parque computacional que ocorreu nesses últimos anos.

4) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

As especificações do objeto desta licitação deverão estar detalhadas no termo de referência elaborado com base neste estudo técnico preliminar e de acordo com a solicitação elaborada pelo setor demandante.

5) ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

Item	Descrição	SKU	Quantidade	Valor
1	KASPERSKY NEXT EDR OPTIMUM 36 meses	KL4066KASTJ	160	R$64.820,80

Descrição Item 1

A solução deve incluir treinamento em segurança cibernética

Do módulo de proteção de endpoint

Compatibilidade com diferentes sistemas operacionais, MAC OS, Linux de 32 e 64 bits (CentOS, Red Hat Enterprise, Debian, Ubuntu, Oracle Linux), Windows 7, 8, 8.1, 10,11 para desktops, para servidores S.O Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022, Windows Small Business Server 2011, Servidores de terminal Microsoft (Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022).

Módulo de gerenciamento avançado

A solução deve suportar arquitetura cloud-native e on-premisse, a solução deve incluir suporte para implantação baseada em nuvem (Amazon Web Services e/ou Microsoft Azure. Integração nativa com as seguintes opções de SIEM (HP (Microfoco) ArcSight, IBM QRadar, Splunk, Kaspersky KUMA). 2.4.

A solução deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

A solução deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

A solução deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

A solução deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

O servidor de gerenciamento primário da solução deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.
A solução deve suportar os seguintes canais de entrega de notificação, E-mail, registro de sistema e SMS ou equivalente.
A solução deve ter a capacidade de etiquetar/marcar computadores com base em
Atributos de rede, Nome, Domínio e/ou Sufixo de Domínio, Endereço de IP, Endereço IP para servidor de gerenciamento, Localização no Active Directory, Unidade organizacional, Grupo, Sistema operacional, Número do pacote de serviço, Arquitetura Virtual, Registro de aplicativos, Nome da Aplicação, Versão do aplicativo, Fabricante, Tipo e versão, Arquitetura.
A solução deverá permitir especificamente o bloqueio dos seguintes dispositivos, Bluetooth, Dispositivos móveis, Modems externos, CD/DVD, Câmeras e scanners.
A solução deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.
A solução deve permitir realizar as seguintes ações para endpoints, verificação manual, verificação no acesso, verificação por demanda, verificação de arquivos compactados, verificação de arquivos individuais, pastas e unidades, bloqueio e verificação de scripts, proteção contra alteração de registros, proteção contra estouro de buffer, verificação em segundo plano/inativa.

A solução deverá suportar os seguintes servidores de banco de dados:
Windows,

- Microsoft SQL Server
- Microsoft Banco de dados SQL do Azure
- MySQL Standard e Enterprise
- MariaDB
- PostgreSQL

Linux:

- MySQL
- MariaDB
- PostgreSQL

A solução deverá suportar as seguintes plataformas virtuais:
Windows:

- VMware vSphere 6.7 e 7.0

- Estação de trabalho VMware 16 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Oracle VM VirtualBox 6.x

2.74.2. Linux:

- VMware vSphere 6.7, 7.0 e 8.0
- VMware Desktop 16 Pro e 17 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 e 8.x

Do módulo de gerenciamento simplificado

A solução deve suportar arquitetura cloud;

A solução deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

A solução deve permitir ao administrador gerar relatórios pré-definidos.

A solução deve incluir informações do endpoint, IP público de internet, IP interno do dispositivo, Versão do agente de proteção, ultima comunicação com a console, contendo data e hora, informações do sistema operacional;

Requisitos gerais

A solução deve ser capaz de detectar os seguintes tipos de ameaças:

Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

A solução deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
A solução deve ter capacidade de integração com a central de segurança do Windows Defender.
A solução deve suportar o subsistema Linux no Windows.
A solução deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

- Proteção contra ameaças sem arquivos (Fileless);
- Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

Do modulo de gerenciamento de dispositivos móveis

O modulo deve ser integrado a console de gerenciamento;
A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

- Android 5.0 ou posterior (incluindo Android 12L)

A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

- iOS 10–17 ou iPadOS 13–17

A solução deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

Do módulo de EDR

Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
A solução deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
Deve apresentar informações detalhadas contendo:

- Usuário que executou a ação;

- Informações acesso privilegiado;

A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.

O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único).

6) IMPACTOS AMBIENTAIS

Não foram identificados impactos ambientes nesta contratação

7) JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Não se aplica

8) CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

Não se identificou contratações interdependentes e/ou correlatas, sendo que a prestação dos serviços depende exclusivamente do presente procedimento.

9) ALINHAMENTO COM PAC – PLANO ANUAL DE CONTRATAÇÕES

A demanda em questão encontra-se prevista no plano anual de contratações.

10) RESULTADOS PRETENDIDOS

- Garantir um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;
- Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo estações de trabalho e notebooks comprometidos;
- Evitar, mitigar e conter a propagação de pragas digitais (vírus/malwares/spywares, spam, entre outros) com a administração centralizada da solução de proteção;
- Permitir o controle de acesso à rede por dispositivos computacionais, permitindo gerenciamento destes dispositivos;
- Possibilitar análise pormenorizada de arquivos, discos rígidos, unidades móveis, mensagens de e-mail e anexos, viabilizando detecção de ameaças, com intento de salvaguardar a estrutura tecnológica de ataques com teor e objetivo malicioso;

- Possibilitar o controle de acesso e tráfego de informações aos dispositivos e serviços operacionais na rede, através de gerenciamento centralizado, o que vem a complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;
- Aprimorar a segurança de TIC da CMFI frente a ameaças sofisticadas.

11) PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Tendo em vista que nosso ambiente de tecnologia já possui uma solução de firewall, não será necessária nenhuma providência prévia.

12) VIABILIDADE DA CONTRATAÇÃO

Esta equipe de TI declara viável esta contratação

13) TRATAMENTO DIFERENCIADO E FAVORECIDO A SER DISPENSADO ÀS MICROEMPRESAS, AS EMPRESAS DE PEQUENO PORTE E AOS MICROEMPREENDEDORES INDIVIDUAIS

A escolha deverá contemplar, preferencialmente, fornecedores deste município, nos termos previstos no art. 48, §3º da LC 123/2006 combinado com o art. 50-B, II da Lei Complementar 229/2014 do município de Foz do Iguaçu, com o objetivo de estímulo ao mercado local da cidade de Foz do Iguaçu, fixando, para este caso específico o limite percentual de 3 %.

14) RESPONSÁVEIS PELA ELABORAÇÃO DO ETP

_____
Responsável (nome, cargo, matrícula, setor)

_____
Responsável (nome, cargo, matrícula, setor)

_____
Responsável (nome, cargo, matrícula, setor)

Proc. Administrativo 6- 243/2024

De: Rodrigo N. - CMFI-DG-DIRTEC-EATI

Para: Envolvidos internos acompanhando

Data: 17/07/2024 às 11:06:35

Segue o Termo de referencia

_

Rodrigo Nishimori
Administrador de Rede

Anexos:

1_Termo_de_Referencia_Minuta.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Rodrigo Nishimori	17/07/2024 11:06:55	1Doc	RODRIGO NISHIMORI CPF 007.XXX.XXX-01

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **3143-813B-6840-7871**

TERMO DE REFERÊNCIA

1) DEFINIÇÃO DO OBJETO

Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento.

Item	Descrição	SKU	Quantidade	Valor
1	KASPERSKY NEXT EDR OPTIMUM 36 meses	KL4066KASTJ	160	R$64.820,80

2) FUNDAMENTAÇÃO DA CONTRATAÇÃO

Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos

meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".
Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.
Com a iminente expiração da licença, torna-se necessária a renovação e aquisição para assegurar a proteção atualizada contra as ameaças virtuais mais recentes.

3) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução de segurança deve atender a necessidade de evolução e adequação desta casa em relação a suas ferramentas de proteção, esta casa de leis possui dois contratos ativos de licença da ferramenta KESB Select da desenvolvedora Kaspersky Global, em um deles possui o quantitativo de 130 licenças a expirar em 22/09/2024 e o outro de 20 licenças a expirar em 01/10/2024. Sendo assim, a solução apresentada deve fornecer novas licenças em formato de renovação, adequada a nova linha de produtos das soluções de segurança com incremento de, no mínimo, EDR, bem como sua ativação.

Custo Inicial Reduzido: Ao optar pela renovação, a empresa evita os altos custos iniciais de compra e instalação de novas soluções, permitindo a alocação de recursos para outras áreas críticas do negócio.

- **Suporte e atualizações:** Fornecimento dos serviços de suporte técnico, bem como atualizações, asseguram o perfeito funcionamento da solução.
- **Gestão Simplificada:** Por se tratar de uma solução integrada a gestão centralizada, permite aos profissionais maior autonomia e melhor condição de adaptação, visto que a equipe é reduzida.

Os itens da presente solução devem ser contratados em conjunto tendo em vista a necessidade de completa compatibilidade para o correto funcionamento.

a) Proteção antivírus de Arquivos;

b) Proteção antivírus da Web;

c) Firewall local de cada máquina;

d) Bloqueador de Ataques da Rede;

e) Inspeção do Sistema;

f) Inspeção avançada de dispositivos portáteis (pen drive, cartão de memória, etc);

g) Monitoramento de Vulnerabilidades.

4) REQUISITOS DA CONTRATAÇÃO

4.1. Do módulo de proteção de endpoint

a. A solução proposta deverá proteger os sistemas operacionais abaixo:

i. Windows 7
ii. Windows 8
iii. Windows 8.1
iv. Windows 10
v. Windows 11

b. Servidores

i. Windows Small Business Server 2011
ii. Windows MultiPoint Server 2011
iii. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

c. Servidores de terminal Microsoft

i. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

d. Sistemas operacionais Linux de 32 bits:

i. CentOS 6.7 e posterior
ii. Debian GNU/Linux 11.0 e posterior
iii. Debian GNU/Linux 12.0 e posterior
iv. Red Hat Enterprise Linux 6.7 e posterior

e. Sistemas operacionais Linux de 64 bits:

i. Amazon Linux 2.
ii. CentOS 6.7 e mais tarde
iii. CentOS 7.2 e posterior.
iv. CentOS Stream 8.
v. CentOS Stream 9.
vi. Debian GNU/Linux 11.0 e posterior.
vii. Debian GNU/Linux 12.0 e posterior.
viii. Linux Mint 20.3 e superior.
ix. Linux Mint 21.1 e posterior.
x. openSUSE Leap 15.0 e posterior.
xi. Oracle Linux 7.3 e posterior.
xii. Oracle Linux 8.0 e posterior.
xiii. Oracle Linux 9.0 e posterior.
xiv. Red Hat Enterprise Linux 6.7 e posterior
xv. Red Hat Enterprise Linux 7.2 e posterior.
xvi. Red Hat Enterprise Linux 8.0 e posterior.
xvii. Red Hat Enterprise Linux 9.0 e posterior.
xviii. Rocky Linux 8.5 e posterior.
xix. Rocky Linux 9.1.
xx. SUSE Linux Enterprise Server 12.5 ou posterior.
xxi. SUSE Linux Enterprise Server 15 ou posterior.
xxii. Ubuntu 20.04 LTS.
xxiii. Ubuntu 22.04 LTS.
xxiv. Sistemas operacionais Arm de 64 bits:

xxv. CentOS Stream 9.
xxvi. SUSE Linux Enterprise Server 15.
xxvii. Ubuntu 22.04 LTS.

f. Sistemas operacionais MAC OS:
i. macOS 12 – 14

g. Ferramentas de virtualização MAC OS:
i. Parallels Desktop 16 para Mac Business Edition
ii. VMware Fusion 11.5 Profissional
iii. VMware Fusion 12 Profissional

h. A solução proposta deverá suportar as seguintes plataformas virtuais:
i. VMware Workstation 17.0.2 Pro
ii. VMware ESXi 8.0 Update 2
iii. Microsoft Hyper-V Server 2019
iv. Citrix Virtual Apps e Desktop 7 2308
v. Citrix Provisioning 2308
vi. Citrix Hypervisor 8.2 Update 1

4.2. Do módulo de gerenciamento avançado

a. A solução proposta deve suportar arquitetura cloud-native e on-premisse;
b. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
i. Amazon Web Services
ii. Microsoft Azure
c. A solução proposta deve incluir as seguintes opções de integração SIEM:
i. HP (Microfoco) ArcSight
ii. IBM QRadar
iii. Splunk
iv. Kaspersky KUMA
d. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.
e. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;
f. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.
g. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.
h. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.
i. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.
j. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.
k. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.
l. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.

m. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

n. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:

i. Status do dispositivo
ii. Tag
iii. Diretório ativo
iv. Proprietários de dispositivos
v. Hardware

o. A solução proposta deve suportar os seguintes canais de entrega de notificação:

i. E-mail
ii. Registro de sistema
iii. SMS

p. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:

i. Atributos de rede
ii. Nome
iii. Domínio e/ou Sufixo de Domínio
iv. Endereço de IP
v. Endereço IP para servidor de gerenciamento
vi. Localização no Active Directory
vii. Unidade organizacional
viii. Grupo
ix. Sistema operacional
x. Número do pacote de serviço
xi. Arquitetura Virtual
xii. Registro de aplicativos
xiii. Nome da Aplicação
xiv. Versão do aplicativo
xv. Fabricante
xvi. Tipo e versão
xvii. Arquitetura

q. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

r. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

s. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

i. Dispositivos Desktop/Servidores
ii. Dispositivos móveis
iii. Dispositivos de rede
iv. Dispositivos virtuais
v. Componentes OEM
vi. Periféricos de computador
vii. Dispositivos IoT conectados
viii. Telefones VoIP

ix. Repositórios de rede

t. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

i. Nome da Aplicação
ii. Caminho do aplicativo
iii. Metadados do aplicativo
iv. Aplicativo Certificado digital
v. Categorias de aplicativos predefinidas pelo fornecedor
vi. SHA256 e MD5

u. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

i. Bluetooth
ii. Dispositivos móveis
iii. Modems externos
iv. CD/DVD
v. Câmeras e scanners
vi. MTPs
vii. E a transferência de dados para dispositivos móveis

v. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

w. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

x. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

i. Estruturas de domínios e grupos de trabalho do Windows
ii. Estruturas de grupos do Active Directory
iii. Conteúdo de um arquivo de texto criado manualmente pelo administrador

y. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

z. A solução proposta deve permitir realizar as seguintes ações para endpoints:

i. Verificação manual;
ii. Verificação no acesso;
iii. Verificação por demanda;
iv. Verificação de arquivos compactados
v. Verificação de arquivos individuais, pastas e unidades;
vi. Bloqueio e verificação de scripts
vii. Proteção contra alteração de registros;
viii. Proteção contra estouro de buffer;
ix. Verificação em segundo plano/inativa

1.1. Verificação de unidade removível na conexão com o sistema;

1.2. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.

1.3. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.

1.4. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.
1.5. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.
1.6. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.
1.7. A solução proposta deve suportar Windows Failover Cluster.
1.8. A solução proposta deve ter um recurso de clustering integrado.
1.9. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.
1.10. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.
1.11. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.
1.12. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.
1.13. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.
1.14. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.
1.15. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.
1.16. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.
1.17. A solução proposta deverá possuir controles para download de DLL e drivers.
1.18. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão.
1.19. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.
1.20. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).
1.21. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.
1.22. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.
1.23. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.
1.24. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.

1.25. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.
1.26. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.
1.27. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.
1.28. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.
1.29. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.
1.30. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.
1.31. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. .
1.32. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.
1.33. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.
1.34. A solução proposta deve permitir ao administrador personalizar relatórios.
1.35. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.
1.36. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.
1.37. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.
1.38. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.
1.39. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.
1.40. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.
1.41. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;
1.42. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.
1.43. A solução proposta deve suportar integração com solução APT.

1.44. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.
1.45. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:
1.45.1. Windows
1.45.2. Linux
1.46. A solução proposta deverá suportar os seguintes servidores de banco de dados:
1.46.1.1. Windows:
1.46.1.2. Microsoft SQL Server
1.46.1.3. Microsoft Banco de dados SQL do Azure
1.46.1.4. MySQL Standard e Enterprise
1.46.1.5. MariaDB
1.46.1.6. PostgreSQL
1.46.2. Linux:
1.46.2.1. MySQL
1.46.2.2. MariaDB
1.46.2.3. PostgreSQL
1.47. A solução proposta deverá suportar as seguintes plataformas virtuais:
1.47.1.1. Windows:
1.47.1.2. VMware vSphere 6.7 e 7.0
1.47.1.3. Estação de trabalho VMware 16 Pro
1.47.1.4. Servidor Microsoft Hyper-V 2012 de 64 bits
1.47.1.5. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
1.47.1.6. Microsoft Servidor Hyper -V 2016 de 64 bits
1.47.1.7. Servidor Microsoft Hyper-V 2019 de 64 bits
1.47.1.8. Servidor Microsoft Hyper-V 2022 de 64 bits
1.47.1.9. Citrix XenServer 7.1 LTSR
1.47.1.10. Citrix XenServer 8.x
1.47.1.11. Oracle VM VirtualBox 6.x
1.47.2. Linux:
1.47.2.1. VMware vSphere 6.7, 7.0 e 8.0
1.47.2.2. VMware Desktop 16 Pro e 17 Pro
1.47.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits
1.47.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
1.47.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits
1.47.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits
1.47.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits
1.47.2.8. Citrix XenServer 7.1 e 8.x
1.47.2.9. Oracle VM VirtualBox 6.x e7.x
1.48. A solução proposta deve suportar criptografia em vários níveis:
1.48.1. Criptografia completa do disco – incluindo disco do sistema
1.48.2. Criptografia de arquivos e pastas
1.48.3. Criptografia de mídia removível
1.48.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2
1.49. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:
1.49.1. A criptografia de arquivos em unidades de computador locais.

1.49.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.
1.49.3. A criação de listas criptografadas de pastas em unidades de computador locais.
1.50. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:
1.50.1. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.
1.50.2. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.
1.51. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:
1.51.1. A criptografia de todos os arquivos armazenados em unidades removíveis.
1.51.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.
1.52. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia
1.53. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.
1.54. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.
1.55. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.
1.56. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.
1.57. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.
1.58. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.
1.59. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.
1.60. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.
1.61. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.

1.62. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.
1.63. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.
1.64. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.
1.65. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário.
1.66. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.
1.67. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.
1.68. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:
1.68.1. Uso do Trusted Platform Module e configurações de senha.
1.68.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.
1.69. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).
1.70. A solução proposta deve suportar criptografia em Microsoft Surface Tablets.
1.71. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
1.71.1. Instalação remota de software de terceiros
1.71.2. Relatórios sobre software e hardware existentes
1.71.3. Monitoramento para instalação de software não autorizado
1.71.4. Remoção de software não autorizado
1.72. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.
1.73. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.
1.74. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.
1.75. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.
1.76. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.
1.77. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.
1.78. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.
1.79. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança
1.80. A solução proposta deve permitir ao administrador aprovar atualizações.

1.81. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.
1.82. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.
1.83. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.
1.84. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.
1.85. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.
1.86. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).
1.87. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.
1.88. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.
1.89. A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’.
1.90. A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”.
1.91. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.
1.92. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.
1.93. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.
1.94. A solução proposta deve apoiar a implantação do sistema operacional.
1.95. A solução proposta deve suportar Wake-on LAN e UEFI.
1.96. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.
1.97. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.
1.98. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.
1.99. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.
1.100. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.
1.101. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.
1.102. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.
1.103. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.

1.104. A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.
1.105. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:
1.105.1. Inicie a instalação ao reiniciar ou desligar o computador.
1.105.2. Instale o gerador necessário todos os pré-requisitos do sistema.
1.105.3. Permitir a instalação de novas versões de aplicativos durante as atualizações.
1.105.4. Baixe atualizações para o dispositivo sem instalá-las.
1.106. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.
1.107. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.
1.108. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:
1.108.1. CEF;
1.108.2. LEEF;
1.109. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.
1.110. O relatório da solução proposta deve conter informações CVE.
1.111. A solução proposta deve suportar instalação de aplicações e software de terceiros;

4.3. Do módulo de gerenciamento simplificado
1.112. A solução proposta deve suportar arquitetura cloud;
1.113. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.
1.114. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.
1.115. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.
1.116. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.
1.117. A solução proposta deve atender as condições apontadas no item e subintes 6.
1.118. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.
1.119. A solução proposta deve incluir informações do endpoint:
1.119.1. IP público de internet;
1.119.2. IP interno do dispositivo;
1.119.3. Versão do agente de proteção;
1.119.4. Ultima comunicação com a console, contendo data e hora;
1.119.5. Informações do sistema operacional;
1.120. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.
1.121. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.
1.122. A solução proposta deve incluir treinamento em segurança cibernética.

4.4. Requisitos gerais

1.123. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:

1.123.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

1.124. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.

1.125. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).

1.126. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.

1.127. A solução proposta deve suportar o subsistema Linux no Windows.

1.128. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

1.128.1. Proteção contra ameaças sem arquivos (Fileless);

1.128.2. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

1.129. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;

1.130. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.

1.131. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.

1.132. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.

1.133. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.

1.134. A solução proposta deve fornecer análise comportamental baseada em machine learning.

1.135. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.

1.136. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:

1.136.1. Controles de aplicativos,

1.136.2. Controle web e dispositivos

1.136.3. HIPS e Firewall

1.136.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;

1.136.5. Gerenciamento de criptografia de arquivos e discos;

1.136.6. Controle adaptativo para detecção de anomalias;

1.137. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.

1.138. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.

1.139. A solução proposta deve ter bancos de dados de reputação locais e globais.
1.140. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.
1.141. A solução proposta deve incluir um módulo capaz, no mínimo, de:
1.141.1. Bloqueio de aplicativos com base em sua categorização.
1.141.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.
1.141.3. A adição de sub-redes e a modificação de permissões de atividade.
1.142. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.
1.143. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.
1.144. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.
1.145. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
1.145.1. Modo silencioso;
1.145.2. Discos rígidos e dispositivos removíveis;
1.145.3. De todos as contas de usuários do dispositivo.
1.146. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:
1.146.1. Exclusão imediata de dados;
1.146.2. Exclusão de dados adiada.
1.147. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:
1.147.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
1.147.2. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.
1.148. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.
1.149. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.
1.150. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.
1.151. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.
1.152. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.
1.153. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.
1.154. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.

1.155. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;
1.156. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;
1.157. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.
1.158. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.
1.159. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.
1.160. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.
1.161. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.
1.162. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.
1.163. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.
1.164. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.
1.165. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.
1.166. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.
1.167. A solução proposta deve ter categoria de detecção para bloquear banners de sites.
1.168. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;
1.169. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.
1.170. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.
1.171. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.
1.172. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;
1.173. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.
1.174. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.
1.175. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.

1.176. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.
1.177. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.
1.178. A solução proposta deve suportar o controle de scripts executados em PowerShell.
1.179. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.
1.180. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.
1.181. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.
1.182. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.
1.183. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.
1.184. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.
1.185. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
1.185.1. Filtro de anexos.
1.185.2. Verificação de mensagens de email ao receber, ler e enviar.
1.186. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.
1.187. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;
1.188. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);
1.189. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.
1.190. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.
1.191. A solução proposta deve incluir suporte ao protocolo IPv6.
1.192. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.
1.193. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
1.194. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.
1.195. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.
1.196. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.
1.197. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.

1.198. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.
1.199. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.
1.200. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.
1.201. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.
1.202. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.
1.203. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.
1.204. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.
1.205. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.
1.206. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.
1.207. A solução proposta deve suportar endereços IPv6.
1.208. A solução proposta deve suportar verificação em duas etapas (autenticação).
1.209. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.
1.210. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.
1.211. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.
1.212. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.
1.213. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.
1.214. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.
1.215. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.
1.216. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.
1.217. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.
1.218. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.
1.219. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.

1.220. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.
1.221. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.
1.222. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.
1.223. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.
1.224. A solução proposta deve ter a capacidade de excluir atualizações baixadas.
1.225. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.
1.226. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.
1.227. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.
1.228. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.
1.229. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.
1.230. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.
1.231. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.
1.232. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.
1.233. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
1.233.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.
1.233.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.
1.234. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.
1.235. A solução proposta deve gerar relatoiros de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

4.5. Do modulo de gerenciamento de dispositivos móveis
1.236. O modulo deve ser integrado a console de gerenciamento;
1.237. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
1.237.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)
1.238. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
1.238.1. iOS 10–17 ou iPadOS 13–17
1.239. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.
1.240. A solução proposta deve suportar dispositivos iOS supervisionados.
1.241. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio

(porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.
1.242. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.
1.243. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.
1.244. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).
1.245. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.
1.246. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.
1.247. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.
1.248. A solução proposta deve ter recursos de conteinerização para dispositivos Android.
1.249. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:
1.249.1. Dados em contêineres
1.249.2. Contas de e-mail corporativo
1.249.3. Configurações para conexão à rede Wi-Fi corporativa e VPN
1.249.4. Nome do ponto de acesso (APN)
1.249.5. Perfil do Android for Work
1.249.6. Recipiente KNOX
1.249.7. Chave do gerenciador de licença KNOX
1.250. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
1.250.1. Todos os perfis de configuração instalados
1.250.2. Todos os perfis de provisionamento
1.250.3. O perfil iOS MDM
1.251. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas
1.252. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo .
1.253. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:
1.253.1. Critérios de verificação do dispositivo;
1.253.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;
1.254. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.
1.255. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:

1.255.1. Cartões de memória e outras unidades removíveis
1.255.2. Câmera do dispositivo
1.255.3. Conexões Wi-Fi
1.255.4. Conexões Bluetooth
1.255.5. Porta de conexão infravermelha
1.255.6. Ativação do ponto de acesso Wi-Fi
1.255.7. Conexão de área de trabalho remota
1.255.8. Sincronização de área de trabalho
1.255.9. Definir configurações da caixa de correio do Exchange
1.255.10. Configurar caixa de e-mail em dispositivos iOS MDM
1.255.11. Configure contêineres Samsung KNOX.
1.255.12. Definir as configurações do perfil do Android for Work
1.255.13. Configurar e-mail/calendário/contatos
1.255.14. Defina as configurações de restrição de conteúdo de mídia.
1.255.15. Definir configurações de proxy no dispositivo móvel
1.255.16. Configurar certificados e SCEP
1.256. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay .
1.257. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:
1.257.1. Google Play, Huawei App Gallery e Apple App Store
1.257.2. Portal de inscrição móvel KNOX
1.257.3. Pacotes de instalação pré-configurados independentes
1.258. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.
1.259. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.
1.260. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
1.260.1. VMware AirWatch 9.3 ou posterior
1.260.2. MobileIron 10.0 ou posterior
1.260.3. IBM MaaS360 10.68 ou posterior
1.260.4. Microsoft Intune 1908 ou posterior
1.260.5. SOTI MobiControl 14.1.4 (1693) ou posterior
1.261. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.
1.262. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:
1.262.1. Google Play
1.262.2. Galeria de aplicativos Huawei
1.262.3. Loja de aplicativos da Apple
1.263. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.
1.264. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.

1.265. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.
1.266. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.
1.267. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.
1.268. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.
1.269. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.
1.270. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.
1.271. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.
1.272. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.
1.273. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.
1.274. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.
1.275. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
1.276. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

4.6. Do módulo de EDR

4.6.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
4.6.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
4.6.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
4.6.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
4.6.5. Deve apresentar informações detalhadas contendo:
4.6.5.1. Usuário que executou a ação;
4.6.5.2. Informações acesso privilegiado;
4.6.6. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.
4.6.7. A solução proposta deve suportar integração com serviço de reputação em nuvem.
4.6.8. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)
4.6.9. O agente EDR deve ter integração com o aplicativo de proteção de endpoint(agente único).
4.6.10. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;

4.6.11. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.
4.6.12. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.
4.6.13. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.
4.6.14. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.
4.6.15. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.
4.6.16. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.
4.6.17. A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.
4.6.18. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.
4.6.19. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.
4.6.20. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:
4.6.21. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).
4.6.22. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.
4.6.23. Informações gerais sobre a detecção, incluindo modo de detecção.
4.6.24. Alterações no registro associadas à detecção.
4.6.25. Histórico da presença de arquivos no dispositivo.
4.6.26. Ações de resposta executadas pela aplicação.
4.6.27. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.
4.6.28. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:
4.6.29. Processo
4.6.30. Conexões de rede
4.6.31. Alterações no registro
4.6.32. Detalhes do download de objeto
4.6.33. A solução proposta deve fornecer orientação de resposta (resposta guiada).
4.6.34. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente
4.6.35. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
4.6.36. Impedir a execução de objetos
4.6.37. Isolamento de host

4.6.38. Excluir objeto do host ou grupo de hosts
4.6.39. Encerrar um processo no dispositivo
4.6.40. Colocar um objeto em quarentena
4.6.41. Execute a verificação do sistema
4.6.42. Execução remota de programa/processo/comando
4.6.43. Iniciar a varredura IoC para um grupo de hosts.

4.7. Requisitos para documentação da solução.

4.7.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:
4.7.2. Ajuda on-line para administradores
4.7.3. Ajuda on-line para melhores práticas de implementação
4.7.4. Ajuda on-line para proteção de servidores de administração
4.7.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.
4.8. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

5. MODELO DE EXECUÇÃO DO OBJETO

Em até, 30 dias, a contar da assinatura do contrato, as novas licenças deverão ser fornecidas e registradas em nome de CÂMARA MUNICIPAL DE FOZ DO IGUAÇU, nome fantasia PODER LEGISLATIVO, CNPJ 75.914.051/0001-28, atreladas a conta suporte@fozdoiguacu.pr.leg.br , dentro da plataforma da desenvolvedora Kaspersky Global.
Quando que realizada a disponibilização da licença, notificar via e-mail os responsáveis técnicos, sanches@fozdoiguacu.pr.leg.br e rodrigo@fozdoiguacu.pr.leg.br com detalhes do acesso.

6. MODELO DE GESTÃO DO CONTRATO E CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

A execução do objeto seguirá a seguinte dinâmica:

6.1 A contratante indicará Fiscal de contratos que irá acompanhar a execução do contrato em conformidade com este termo de referência.

6.2 O Contrato terá o prazo de 3 (três) anos, podendo ser prorrogado.

6.3 A Contratada formalizará a designação do preposto da empresa, especificando os poderes e responsabilidades relacionados à execução do objeto contratado.

6.4 Toda comunicação entre a Contratante e a Contratada deverá ser formalizada por escrito, especialmente quando exigido por lei, podendo ser realizada por meio de mensagem eletrônica, quando aplicável.

6.5 A execução será realizada de forma parcelada formalizada pelo envio da ordem de compra.

6.6 Os prazos e critérios para recebimento e pagamento estão detalhados nos itens 7.3 a 7.4.

6.7 Considera-se ocorrido o recebimento da nota fiscal quando a Gestão de contratos atestar a execução do objeto do contrato através do termo de recebimento definitivo.

6.8 Não haverá exigência de garantia contratual da execução, devido às características da contratação.

6.9 A apresentação da Nota Fiscal/fatura é indispensável a cada fornecimento de bem ou serviço, para fins de liquidação e pagamento da despesa, emitida ao destinatário: Razão social: CÂMARA MUNICIPAL DE FOZ DO IGUACU; CNPJ: 75.914.051/0001-28; Endereço: Travessa Oscar Muxfeldt, nº 81, Centro, na cidade de Foz do Iguaçu-Paraná, CEP 85.851-490. Telefone: (45) 3521-8100.

6.10 Antes de cada pagamento à Contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

6.11 Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se- á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

6.12 Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

6.13 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

6.14 Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 20 (vinte) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da Contratante.

6.15 Persistindo a irregularidade, a Contratante deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa.

6.16 Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso a Contratada não regularize sua situação junto ao SICAF.

6.17 O prazo desta contratação será de 36 meses, contados da assinatura do contrato.

6.18 Pagamento:

6.18.1 Os pagamentos serão efetuados até o 10° (décimo) dia após o recebimento definitivo dos

bens, condicionado a apresentação da Nota Fiscal/Fatura, bem como os documentos de regularidade fiscal, social e trabalhista exigidos pelo art. 68 da Lei n° 14.133/2021

6.18.2 Na eventualidade de ocorrer atraso no pagamento, o valor será atualizado pela variação acumulada do IPCA/IBGE, ocorrida entre a data de seu adimplemento e a do efetivo pagamento, calculada pro rata tempore.

7 Sanções:

7.1 Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei n° 14.133, de 2021, quais sejam:

7.2 Dar causa à inexecução parcial do contrato;

7.3 Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

7.4 Dar causa à inexecução total do contrato;

7.5 Deixar de entregar a documentação exigida para o certame;

7.6 Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

7.7 Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

7.8 Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

7.9 Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

7.10 Fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

7.11 Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

7.12 Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

7.13 Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;

7.14 O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Advertência pela falta do subitem 8.2 deste Aviso de Contratação Direta, quando não se justificar a imposição de

b) penalidade mais grave;

c) Multa de até 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor,

d) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver

e) aplicado a sanção, pelo prazo máximo de 3 (três) anos.

f) Direta, quando não se justificar a imposição de penalidade mais grave;

g) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 8.9 a bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

8 A fiscalização do contrato será realizada pelo servidor(a) designado:

9 A gestão do contrato será realizada pelo servidor (a) designado:

7. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

O fornecedor será selecionado por meio de DISPENSA DE LICITAÇÃO, com a interpretação mais flexível, e considerado o atual limite de R$59.906,02 para serviços e fornecimentos, conforme art. 75, inc. II, da Lei º 14.133/21 c/c Decreto nº 11.871/2023.

8. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

As quantidades previstas a serem adquiridas, conforme os itens descritos, são:

Item	Descrição	SKU	Quantidade	Valor
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160	R$64.820,80

A pesquisa de preço foi realizada considerando os parâmetros dispostos da Lei 14.133 no art. 23 § inciso IV – *"pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital".* Do qual optou-se pelo preço médio ofertado.

Quanto à não utilização dos parâmetros dos § Incisos I e II do Art. 23, consultas no portal PNCP (Inciso I) e contratações similares feitas pela Administração Pública (II), conforme descrito no parágrafo anterior, torna-se ineficaz e escassa a busca por contratações similares em outros órgãos. Regendo-se pela economicidade, melhor tecnologia e melhores resultados pretendidos pelo órgão, a consulta aos fornecedores torna-se mais eficaz.

9. TRATAMENTO DIFERENCIADO E FAVORECIDO A SER DISPENSADO ÀS MICROEMPRESAS, ÀS EMPRESAS DE PEQUENO PORTE E AOS MICROEMPREENDEDORES INDIVIDUAIS

Após diversas tentativas de localização e contato com empresas qualificadas como microempresas (ME) e empresas de pequeno porte (EPP) na região de Foz do Iguaçu para fornecimento das licenças, constatou-se a inexistência, inclusive pelo embasamento da pesquisa na base de de empresas credenciadas junto ao portal do desenvolvedor, acessado na data de 10/07/2024 às 13:35.

Durante o processo de prospecção, entramos em contato direto com diversas empresas locais, incluindo aquelas registradas como ME e EPP, para verificar a capacidade técnica e a disponibilidade para fornecimento do serviço requerido. Nenhuma das ME/EPP contactadas demonstrou capacidade técnica ou interesse em participar do certame.

Diante dessas circunstâncias, a manutenção da exclusividade do certame para ME e EPP pode inviabilizar a contratação, comprometendo a eficiência e a continuidade dos serviços públicos dependentes de uma conexão estável e de alta velocidade, eis que há sério risco da licitação ser

deserta.

Ressalta-se, porém, que as ME/EPP ainda poderão participar do certame com vantagens sobre os demais concorrentes conforme versa a legislação pátria.

Portanto, justifica-se o afastamento da exclusividade de participação de microempresas e empresas de pequeno porte neste certame específico, com base na inexistência de fornecedores locais qualificados e na necessidade imperiosa de garantir a prestação adequada e contínua dos serviços públicos.

10. ADEQUAÇÃO ORÇAMENTÁRIA

ITEM	DOTAÇÃO
1	01.01.01.031.0001.2002.3.3.90.40.99.05 - AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE

Proc. Administrativo 7- 243/2024

De: Rodrigo N. - CMFI-DG-DIRTEC-EATI

Para: Envolvidos internos acompanhando

Data: 17/07/2024 às 11:10:06

Segue o Relatório de Pesquisa de Preço.

_

Rodrigo Nishimori
Administrador de Rede

Anexos:

RELATORIA_PESQUISA_DE_PRECOS.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Rafael Sanches Alencar	17/07/2024 12:07:51	1Doc	RAFAEL SANCHES ALENCAR CPF 006.XXX.XXX-96

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **7AF8-4761-6504-0616**

RELATÓRIO DE PESQUISA DE PREÇOS, PLANILHA COMPARATIVA E DOCUMENTAÇÃO COMPROBATÓRIA

INTRODUÇÃO

O presente relatório é resultado da pesquisa de preços abaixo discriminada em cumprimento ao determinado na Lei nº 14.133/2021 em conformidade com o Ato da Presidência nº 136/2023.

AGENTE RESPONSÁVEL PELA PESQUISA: Rafael Sanches Alencar

OBJETO: Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses

MÉTODO ESTATÍSTICO APLICADO COM JUSTIFICATIVAS PARA A METODOLOGIA UTILIZADA, EM ESPECIAL PARA A DESCONSIDERAÇÃO DE VALORES INCONSISTENTES, INEXEQUÍVEIS OU EXCESSIVAMENTE ELEVADOS, SE APLICÁVEL: Os valores foram com base em orçamentos obtidos em mercado, no qual se optou pelo preço médio, afim de satisfazer as demandas desta casa de leis.

CARACTERIZAÇÃO DAS FONTES DE PESQUISA CONSULTADAS: Foram realizadas pesquisas de preços utilizando-se dos seguintes parâmetros *estabelecidos no Ato da Presidência nº 136/2023, no qual Art. 6º "A pesquisa* de preços para fins de determinação do preço estimado na contratação direta para a aquisição de bens e contratação de serviços em geral, consolidada em mapa comparativo, terá prazo de validade de 6 (seis) meses e será realizada mediante a utilização dos seguintes parâmetros, **de forma combinada ou não"**. No qual foi utilizada IV – pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos orçamentos com mais de 6 (seis) meses de antecedência da data da pesquisa de preço;

JUSTIFICATIVA DAS FONTES CONSULTADAS: Foi consultado várias empresas, porém somente uma apresentou a proposta e editais citados no ETP, conforme os documentos juntados a este processo, e ainda devido a

especificidade da contração, bem como a necessidade do contrato de todos os itens, por terem interdependência entre si.

PERÍODO DE REALIZAÇÃO DA PESQUISA DE PREÇOS: Junho de 2024.

Abaixo relatório detalhado identificando cada um dos itens e seus valores obtidos:

PESQUISA DE MERCADO						
LOTE I - ITEM 1 - Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License						
FORNECEDOR	**MARCA**	**C/D**	**ART. 7º §4º**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL**
OPTIMUS DATA TECHNOLOGY LTDA		C	Exequível	160	R$ 358,19	R$ 57.310,40
Avant		C	Exequível	160	R$ 445,94	R$ 71.350,40
Solo Network		C	Exequível	160	R$ 411,26	R$ 65.801,60
		C		0		R$ 0,00
	-	C		1		R$ 0,00
	-	C		1		R$ 0,00
	-	C		1		R$ 0,00
Média PREÇO/FORNECEDOR					**R$ 64.820,80**	**#N/D**

VALOR TOTAL R$ 64.820,80 (Sessenta e quatro mil oitocentos e vinte reais e vinte e oitenta centavos).

Eu, Rafael Sanches Alencar, declaro que efetuei a pesquisa de preços, na forma dos incisos I do artigo 23° da Lei n° 14.133/2021, em conformidade com o Ato da Presidência nº 136/2023 e que os preços aqui apresentados condizem com os praticados no mercado.

Proc. Administrativo 8- 243/2024

De: Rodrigo N. - CMFI-DG-DIRTEC-EATI

Para: Envolvidos internos acompanhando

Data: 17/07/2024 às 12:51:46

Segue em anexo o ETP para assinatura

_

Rodrigo Nishimori
Administrador de Rede

Anexos:

ETP_2_.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Jeverson Siqueira	17/07/2024 12:57:23	1Doc	JEVERSON SIQUEIRA CPF 080.XXX.XXX-74

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **8FC5-AE07-00DA-9371**

ESTUDO TÉCNICO PRELIMINAR

1) DESCRIÇÃO DA NECESSIDADE

1.1. Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

1.2. A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

1.3. Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

1.4. Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

1.5. Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

1.6. Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

1.7. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.

2) REQUISITOS DA CONTRATAÇÃO

Item	Descriçao	SKU	Quantidade
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160

3) LEVANTAMENTO DE MERCADO

Considerando que a Câmara Municipal de Foz do Iguaçu já dispõe de um sistema de antivírus, foram avaliadas duas alternativas sendo uma delas a renovação e upgrade de versão do sistema e a outra a aquisição de um sistema integrado com o nosso sistema de Firewall.

Mantendo os investimentos já realizados, tendo em vista de que além da aquisição do sistema, foi também realizado a contratação de uma empresa especializada para nos auxiliar na configuração recomendadas pelo fabricante, e com base nas pesquisa de preços e estudo entre outras soluções, optou-se pela renovação e upgrade da versão já utilizada do licenciamento da solução Kaspersky e aquisição de novas licenças para contemplar a necessidade do parque computacional da CMFI, levando em consideração a ampliação do nosso parque computacional que ocorreu nesses últimos anos.

4) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

As especificações do objeto desta licitação deverão estar detalhadas no termo de referência elaborado com base neste estudo técnico preliminar e de acordo com a solicitação elaborada pelo setor demandante.

5) ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

Item	Descrição	SKU	Quantidade	Valor
1	KASPERSKY NEXT EDR OPTIMUM 36 meses	KL4066KASTJ	160	R$64.820,80

Descrição Item 1

A solução deve incluir treinamento em segurança cibernética

Do módulo de proteção de endpoint

Compatibilidade com diferentes sistemas operacionais, MAC OS, Linux de 32 e 64 bits (CentOS, Red Hat Enterprise, Debian, Ubuntu, Oracle Linux), Windows 7, 8, 8.1, 10,11 para desktops, para servidores S.O Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022, Windows Small Business Server 2011, Servidores de terminal Microsoft (Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022).

Módulo de gerenciamento avançado

A solução deve suportar arquitetura cloud-native e on-premisse, a solução deve incluir suporte para implantação baseada em nuvem (Amazon Web Services e/ou Microsoft Azure. Integração nativa com as seguintes opções de SIEM (HP (Microfoco) ArcSight, IBM QRadar, Splunk, Kaspersky KUMA). 2.4.

A solução deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

A solução deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

A solução deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

A solução deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

O servidor de gerenciamento primário da solução deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.
A solução deve suportar os seguintes canais de entrega de notificação, E-mail, registro de sistema e SMS ou equivalente.
A solução deve ter a capacidade de etiquetar/marcar computadores com base em
Atributos de rede, Nome, Domínio e/ou Sufixo de Domínio, Endereço de IP, Endereço IP para servidor de gerenciamento, Localização no Active Directory, Unidade organizacional, Grupo, Sistema operacional, Número do pacote de serviço, Arquitetura Virtual, Registro de aplicativos, Nome da Aplicação, Versão do aplicativo, Fabricante, Tipo e versão, Arquitetura.
A solução deverá permitir especificamente o bloqueio dos seguintes dispositivos, Bluetooth, Dispositivos móveis, Modems externos, CD/DVD, Câmeras e scanners.
A solução deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.
A solução deve permitir realizar as seguintes ações para endpoints, verificação manual, verificação no acesso, verificação por demanda, verificação de arquivos compactados, verificação de arquivos individuais, pastas e unidades, bloqueio e verificação de scripts, proteção contra alteração de registros, proteção contra estouro de buffer, verificação em segundo plano/inativa.

A solução deverá suportar os seguintes servidores de banco de dados:
Windows,

- Microsoft SQL Server
- Microsoft Banco de dados SQL do Azure
- MySQL Standard e Enterprise
- MariaDB
- PostgreSQL

Linux:

- MySQL
- MariaDB
- PostgreSQL

A solução deverá suportar as seguintes plataformas virtuais:
Windows:

- VMware vSphere 6.7 e 7.0

- Estação de trabalho VMware 16 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Oracle VM VirtualBox 6.x

2.74.2. Linux:

- VMware vSphere 6.7, 7.0 e 8.0
- VMware Desktop 16 Pro e 17 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 e 8.x

Do módulo de gerenciamento simplificado

A solução deve suportar arquitetura cloud;

A solução deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

A solução deve permitir ao administrador gerar relatórios pré-definidos.

A solução deve incluir informações do endpoint, IP público de internet, IP interno do dispositivo, Versão do agente de proteção, ultima comunicação com a console, contendo data e hora, informações do sistema operacional;

Requisitos gerais

A solução deve ser capaz de detectar os seguintes tipos de ameaças:

Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

A solução deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
A solução deve ter capacidade de integração com a central de segurança do Windows Defender.
A solução deve suportar o subsistema Linux no Windows.
A solução deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

- Proteção contra ameaças sem arquivos (Fileless);
- Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

Do modulo de gerenciamento de dispositivos móveis

O modulo deve ser integrado a console de gerenciamento;
A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

- Android 5.0 ou posterior (incluindo Android 12L)

A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

- iOS 10–17 ou iPadOS 13–17

A solução deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

Do módulo de EDR

Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
A solução deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
Deve apresentar informações detalhadas contendo:

- Usuário que executou a ação;

- Informações acesso privilegiado;

A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.

O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único).

6) IMPACTOS AMBIENTAIS

Não foram identificados impactos ambientes nesta contratação

7) JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Não se aplica

8) CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

Não se identificou contratações interdependentes e/ou correlatas, sendo que a prestação dos serviços depende exclusivamente do presente procedimento.

9) ALINHAMENTO COM PAC – PLANO ANUAL DE CONTRATAÇÕES

A demanda em questão encontra-se prevista no plano anual de contratações.

10) RESULTADOS PRETENDIDOS

- Garantir um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;
- Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo estações de trabalho e notebooks comprometidos;
- Evitar, mitigar e conter a propagação de pragas digitais (vírus/malwares/spywares, spam, entre outros) com a administração centralizada da solução de proteção;
- Permitir o controle de acesso à rede por dispositivos computacionais, permitindo gerenciamento destes dispositivos;
- Possibilitar análise pormenorizada de arquivos, discos rígidos, unidades móveis, mensagens de e-mail e anexos, viabilizando detecção de ameaças, com intento de salvaguardar a estrutura tecnológica de ataques com teor e objetivo malicioso;

- Possibilitar o controle de acesso e tráfego de informações aos dispositivos e serviços operacionais na rede, através de gerenciamento centralizado, o que vem a complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;
- Aprimorar a segurança de TIC da CMFI frente a ameaças sofisticadas.

11) PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Tendo em vista que nosso ambiente de tecnologia já possui uma solução de firewall, não será necessária nenhuma providência prévia.

12) VIABILIDADE DA CONTRATAÇÃO

Esta equipe de TI declara viável esta contratação

13) TRATAMENTO DIFERENCIADO E FAVORECIDO A SER DISPENSADO ÀS MICROEMPRESAS, AS EMPRESAS DE PEQUENO PORTE E AOS MICROEMPREENDEDORES INDIVIDUAIS

A escolha deverá contemplar, preferencialmente, fornecedores deste município, nos termos previstos no art. 48, §3º da LC 123/2006 combinado com o art. 50-B, II da Lei Complementar 229/2014 do município de Foz do Iguaçu, com o objetivo de estímulo ao mercado local da cidade de Foz do Iguaçu, fixando, para este caso específico o limite percentual de 3 %.

14) RESPONSÁVEIS PELA ELABORAÇÃO DO ETP

_____
Responsável (nome, cargo, matrícula, setor)

_____
Responsável (nome, cargo, matrícula, setor)

_____
Responsável (nome, cargo, matrícula, setor)

Proc. Administrativo 9- 243/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: CMFI-PRESID-DG-DIRFIN-COM - Chefia Compras

Data: 17/07/2024 às 14:05:53

Considerando os documentos anexados, segue para próxima fase.

–

Rafael Sanches
Diretoria de Tecnologia

Proc. Administrativo 10- 243/2024

De: Débora R. - CMFI-PRESID-DG-DIRFIN-COM-EC

Para: Envolvidos internos acompanhando

Data: 30/07/2024 às 09:36:56

Em anexo alguns apontamentos ao Termo de Referência elaborado pelo setor demandante. Necessária adequação.

–

Débora Borges Rengel
Analista Legislativo

Anexos:

5_Termo_de_Referencia_Minuta_APONTAMENTOS.docx

Proc. Administrativo 11- 243/2024

De: Rodrigo N. - CMFI-DG-DIRTEC-EATI

Para: Envolvidos internos acompanhando

Data: 05/08/2024 às 12:43:49

ETP

–

Rodrigo Nishimori
Administrador de Rede

Anexos:

ETP.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Jeverson Siqueira	05/08/2024 12:51:21	1Doc	JEVERSON SIQUEIRA CPF 080.XXX.XXX-74

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **702B-A398-1642-7D93**

ESTUDO TÉCNICO PRELIMINAR

1) DESCRIÇÃO DA NECESSIDADE

1.1. Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

1.2. A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

1.3. Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

1.4. Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

1.5. Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

1.6. Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

1.7. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.

2) REQUISITOS DA CONTRATAÇÃO

Item	Descriçao	SKU	Quantidade
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160

3) LEVANTAMENTO DE MERCADO

Considerando que a Câmara Municipal de Foz do Iguaçu já dispõe de um sistema de antivírus, foram avaliadas duas alternativas sendo uma delas a renovação e upgrade de versão do sistema e a outra a aquisição de um sistema integrado com o nosso sistema de Firewall.

Mantendo os investimentos já realizados, tendo em vista de que além da aquisição do sistema, foi também realizado a contratação de uma empresa especializada para nos auxiliar na configuração recomendadas pelo fabricante, e com base nas pesquisa de preços e estudo entre outras soluções, optou-se pela renovação e upgrade da versão já utilizada do licenciamento da solução Kaspersky e aquisição de novas licenças para contemplar a necessidade do parque computacional da CMFI, levando em consideração a ampliação do nosso parque computacional que ocorreu nesses últimos anos.

4) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

As especificações do objeto desta licitação deverão estar detalhadas no termo de referência elaborado com base neste estudo técnico preliminar e de acordo com a solicitação elaborada pelo setor demandante.

5) ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

Item	Descrição	SKU	Quantidade	Valor
1	KASPERSKY NEXT EDR OPTIMUM 36 meses	KL4066KASTJ	160	R$ 57.310,40

Descrição Item 1

A solução deve incluir treinamento em segurança cibernética

Do módulo de proteção de endpoint

Compatibilidade com diferentes sistemas operacionais, MAC OS, Linux de 32 e 64 bits (CentOS, Red Hat Enterprise, Debian, Ubuntu, Oracle Linux), Windows 7, 8, 8.1, 10,11 para desktops, para servidores S.O Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022, Windows Small Business Server 2011, Servidores de terminal Microsoft (Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022).

Módulo de gerenciamento avançado

A solução deve suportar arquitetura cloud-native e on-premisse, a solução deve incluir suporte para implantação baseada em nuvem (Amazon Web Services e/ou Microsoft Azure. Integração nativa com as seguintes opções de SIEM (HP (Microfoco) ArcSight, IBM QRadar, Splunk, Kaspersky KUMA). 2.4.

A solução deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

A solução deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

A solução deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

A solução deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

O servidor de gerenciamento primário da solução deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.
A solução deve suportar os seguintes canais de entrega de notificação, E-mail, registro de sistema e SMS ou equivalente.
A solução deve ter a capacidade de etiquetar/marcar computadores com base em
Atributos de rede, Nome, Domínio e/ou Sufixo de Domínio, Endereço de IP, Endereço IP para servidor de gerenciamento, Localização no Active Directory, Unidade organizacional, Grupo, Sistema operacional, Número do pacote de serviço, Arquitetura Virtual, Registro de aplicativos, Nome da Aplicação, Versão do aplicativo, Fabricante, Tipo e versão, Arquitetura.
A solução deverá permitir especificamente o bloqueio dos seguintes dispositivos, Bluetooth, Dispositivos móveis, Modems externos, CD/DVD, Câmeras e scanners.
A solução deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.
A solução deve permitir realizar as seguintes ações para endpoints, verificação manual, verificação no acesso, verificação por demanda, verificação de arquivos compactados, verificação de arquivos individuais, pastas e unidades, bloqueio e verificação de scripts, proteção contra alteração de registros, proteção contra estouro de buffer, verificação em segundo plano/inativa.

A solução deverá suportar os seguintes servidores de banco de dados:
Windows,

- Microsoft SQL Server
- Microsoft Banco de dados SQL do Azure
- MySQL Standard e Enterprise
- MariaDB
- PostgreSQL

Linux:

- MySQL
- MariaDB
- PostgreSQL

A solução deverá suportar as seguintes plataformas virtuais:
Windows:

- VMware vSphere 6.7 e 7.0

- Estação de trabalho VMware 16 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Oracle VM VirtualBox 6.x

2.74.2. Linux:

- VMware vSphere 6.7, 7.0 e 8.0
- VMware Desktop 16 Pro e 17 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 e 8.x

Do módulo de gerenciamento simplificado

A solução deve suportar arquitetura cloud;

A solução deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

A solução deve permitir ao administrador gerar relatórios pré-definidos.

A solução deve incluir informações do endpoint, IP público de internet, IP interno do dispositivo, Versão do agente de proteção, ultima comunicação com a console, contendo data e hora, informações do sistema operacional;

Requisitos gerais

A solução deve ser capaz de detectar os seguintes tipos de ameaças:

Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

A solução deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
A solução deve ter capacidade de integração com a central de segurança do Windows Defender.
A solução deve suportar o subsistema Linux no Windows.
A solução deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

- Proteção contra ameaças sem arquivos (Fileless);
- Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

Do modulo de gerenciamento de dispositivos móveis

O modulo deve ser integrado a console de gerenciamento;
A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

- Android 5.0 ou posterior (incluindo Android 12L)

A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

- iOS 10–17 ou iPadOS 13–17

A solução deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

Do módulo de EDR

Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
A solução deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
Deve apresentar informações detalhadas contendo:

- Usuário que executou a ação;
- Informações acesso privilegiado;

A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas. O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único).

6) IMPACTOS AMBIENTAIS

Não foram identificados impactos ambientes nesta contratação

7) JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Não se aplica

8) CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

Não se identificou contratações interdependentes e/ou correlatas, sendo que a prestação dos serviços depende exclusivamente do presente procedimento.

9) ALINHAMENTO COM PAC – PLANO ANUAL DE CONTRATAÇÕES

A demanda em questão encontra-se prevista no plano anual de contratações.

10) RESULTADOS PRETENDIDOS

- Garantir um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;
- Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo estações de trabalho e notebooks comprometidos;
- Evitar, mitigar e conter a propagação de pragas digitais (vírus/malwares/spywares, spam, entre outros) com a administração centralizada da solução de proteção;
- Permitir o controle de acesso à rede por dispositivos computacionais, permitindo gerenciamento destes dispositivos;
- Possibilitar análise pormenorizada de arquivos, discos rígidos, unidades móveis, mensagens de e-mail e anexos, viabilizando detecção de ameaças, com intento de salvaguardar a estrutura tecnológica de ataques com teor e objetivo malicioso;
- Possibilitar o controle de acesso e tráfego de informações aos dispositivos e serviços operacionais na rede, através de gerenciamento centralizado, o que vem

a complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;

- Aprimorar a segurança de TIC da CMFI frente a ameaças sofisticadas.

11) PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Tendo em vista que nosso ambiente de tecnologia já possui uma solução de firewall, não será necessária nenhuma providência prévia.

12) VIABILIDADE DA CONTRATAÇÃO

Esta equipe de TI declara viável esta contratação

13) TRATAMENTO DIFERENCIADO E FAVORECIDO A SER DISPENSADO ÀS MICROEMPRESAS, ÀS EMPRESAS DE PEQUENO PORTE E AOS MICROEMPREENDEDORES INDIVIDUAIS

Após diversas tentativas de localização e contato com empresas qualificadas como microempresas (ME) e empresas de pequeno porte (EPP) na região de Foz do Iguaçu para fornecimento das licenças, constatou-se a inexistência, inclusive pelo embasamento da pesquisa na base de de empresas credenciadas junto ao portal do desenvolvedor, acessado na data de 10/06/2024 às 09:38. Durante o processo de prospecção, entramos em contato direto com diversas empresas locais, incluindo aquelas registradas como ME e EPP, para verificar a capacidade técnica e a disponibilidade para fornecimento do serviço requerido. Nenhuma das ME/EPP contactadas demonstrou capacidade técnica ou interesse em participar do certame.

Diante dessas circunstâncias, a manutenção da exclusividade do certame para ME e EPP pode inviabilizar a contratação, comprometendo a eficiência e a continuidade dos serviços públicos dependentes de uma conexão estável e de alta velocidade, eis que há sério risco da licitação ser deserta. Ressalta-se, porém, que as ME/EPP ainda poderão participar do certame com vantagens sobre os demais concorrentes conforme versa a legislação pátria.

Portanto, justifica-se o afastamento da exclusividade de participação de microempresas e empresas de pequeno porte neste certame específico, com base na inexistência de fornecedores locais qualificados e na necessidade imperiosa de garantir a prestação adequada e contínua dos serviços públicos.

14) RESPONSÁVEIS PELA ELABORAÇÃO DO ETP

Proc. Administrativo 12- 243/2024

De: Rodrigo N. - CMFI-DG-DIRTEC-EATI

Para: Envolvidos internos acompanhando

Data: 05/08/2024 às 12:44:19

TR

_

Rodrigo Nishimori
Administrador de Rede

Anexos:

1_Termo_de_Referencia_Minuta.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Rodrigo Nishimori	05/08/2024 12:44:39	1Doc	RODRIGO NISHIMORI CPF 007.XXX.XXX-01

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **4ABC-2F9E-FB05-4B66**

TERMO DE REFERÊNCIA

1) DEFINIÇÃO DO OBJETO

Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

Item	CAT/MAT	Descrição	Prazo	SKU	Quantidade	Valor
1	350949	KASPERSKY NEXT EDR OPTIMUM 36 meses	36 meses	KL4066KASTJ	160	R$ 57.310,40

2) FUNDAMENTAÇÃO DA CONTRATAÇÃO

Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".
Considerando que esta casa de leis realiza a utilização da solução de segurança, sem ressalvas e visa proteger seu investimento, assegurar a padronização e compatibilidade com o ambiente computacional. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para, no mínimo, manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.
Com a iminente expiração da licença, torna-se necessária a renovação e aquisição para assegurar a proteção atualizada contra as ameaças virtuais mais recentes.
Sendo a demanda prevista no PAC, conforme documento de estudo técnico preliminar - ETP.

3) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução de segurança deve atender a necessidade de evolução e adequação desta casa em relação a suas ferramentas de proteção, esta casa de leis possui dois contratos ativos de licença da ferramenta KESB Select da desenvolvedora Kaspersky Global, em um deles possui o quantitativo de 130 licenças a expirar em 22/09/2024 e o outro de 20 licenças a expirar em 01/10/2024. Sendo assim, a solução apresentada deve fornecer 10 novas licenças e 150 em formato de renovação, adequada à nova linha de produtos das soluções de segurança com incremento de, no mínimo, EDR, bem como sua ativação. Referente a possibilidade de parcelamento, deve seguir de acordo com o ETP, por se tratar de uma solução integrada.

Custo Inicial Reduzido: Ao optar pela renovação, a empresa evita os altos custos iniciais de compra e instalação de novas soluções, permitindo a alocação de recursos para outras áreas críticas do negócio.

- **Suporte e atualizações:** Fornecimento dos serviços de suporte técnico, bem como atualizações, asseguram o perfeito funcionamento da solução.
- **Gestão Simplificada:** Por se tratar de uma solução integrada a gestão centralizada, permite aos profissionais maior autonomia e melhor condição de adaptação, visto que a equipe é reduzida.

Os itens da presente solução devem ser contratados em conjunto tendo em vista a necessidade de completa compatibilidade para o correto funcionamento.

a) Proteção antivírus de Arquivos;

b) Proteção antivírus da Web;

c) Firewall local de cada máquina;

d) Bloqueador de Ataques da Rede;

e) Inspeção do Sistema;

f) Inspeção avançada de dispositivos portáteis (pen drive, cartão de memória, etc);

g) Monitoramento de Vulnerabilidades.

4) REQUISITOS DA CONTRATAÇÃO

4.1. Do módulo de proteção de endpoint

a. A solução proposta deverá proteger os sistemas operacionais abaixo:

i. Windows 7
ii. Windows 8
iii. Windows 8.1
iv. Windows 10
v. Windows 11

b. Servidores

i. Windows Small Business Server 2011
ii. Windows MultiPoint Server 2011
iii. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

c. Servidores de terminal Microsoft

i. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

d. Sistemas operacionais Linux de 32 bits:

i. CentOS 6.7 e posterior
ii. Debian GNU/Linux 11.0 e posterior
iii. Debian GNU/Linux 12.0 e posterior
iv. Red Hat Enterprise Linux 6.7 e posterior

e. Sistemas operacionais Linux de 64 bits:

i. Amazon Linux 2.
ii. CentOS 6.7 e mais tarde
iii. CentOS 7.2 e posterior.
iv. CentOS Stream 8.
v. CentOS Stream 9.
vi. Debian GNU/Linux 11.0 e posterior.
vii. Debian GNU/Linux 12.0 e posterior.
viii. Linux Mint 20.3 e superior.
ix. Linux Mint 21.1 e posterior.
x. openSUSE Leap 15.0 e posterior.
xi. Oracle Linux 7.3 e posterior.
xii. Oracle Linux 8.0 e posterior.
xiii. Oracle Linux 9.0 e posterior.
xiv. Red Hat Enterprise Linux 6.7 e posterior
xv. Red Hat Enterprise Linux 7.2 e posterior.

xvi. Red Hat Enterprise Linux 8.0 e posterior.
xvii. Red Hat Enterprise Linux 9.0 e posterior.
xviii. Rocky Linux 8.5 e posterior.
xix. Rocky Linux 9.1.
xx. SUSE Linux Enterprise Server 12.5 ou posterior.
xxi. SUSE Linux Enterprise Server 15 ou posterior.
xxii. Ubuntu 20.04 LTS.
xxiii. Ubuntu 22.04 LTS.
xxiv. Sistemas operacionais Arm de 64 bits:
xxv. CentOS Stream 9.
xxvi. SUSE Linux Enterprise Server 15.
xxvii. Ubuntu 22.04 LTS.

f. Sistemas operacionais MAC OS:
i. macOS 12 – 14

g. Ferramentas de virtualização MAC OS:
i. Parallels Desktop 16 para Mac Business Edition
ii. VMware Fusion 11.5 Profissional
iii. VMware Fusion 12 Profissional

h. A solução proposta deverá suportar as seguintes plataformas virtuais:
i. VMware Workstation 17.0.2 Pro
ii. VMware ESXi 8.0 Update 2
iii. Microsoft Hyper-V Server 2019
iv. Citrix Virtual Apps e Desktop 7 2308
v. Citrix Provisioning 2308
vi. Citrix Hypervisor 8.2 Update 1

4.2. Do módulo de gerenciamento avançado

a. A solução proposta deve suportar arquitetura cloud-native e on-premisse;
b. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
i. Amazon Web Services
ii. Microsoft Azure
c. A solução proposta deve incluir as seguintes opções de integração SIEM:
i. HP (Microfoco) ArcSight
ii. IBM QRadar
iii. Splunk
iv. Kaspersky KUMA
d. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.
e. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;
f. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.
g. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.
h. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

i. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

j. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

k. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

l. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.

m. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

n. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:

i. Status do dispositivo
ii. Tag
iii. Diretório ativo
iv. Proprietários de dispositivos
v. Hardware

o. A solução proposta deve suportar os seguintes canais de entrega de notificação:

i. E-mail
ii. Registro de sistema
iii. SMS

p. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:

i. Atributos de rede
ii. Nome
iii. Domínio e/ou Sufixo de Domínio
iv. Endereço de IP
v. Endereço IP para servidor de gerenciamento
vi. Localização no Active Directory
vii. Unidade organizacional
viii. Grupo
ix. Sistema operacional
x. Número do pacote de serviço
xi. Arquitetura Virtual
xii. Registro de aplicativos
xiii. Nome da Aplicação
xiv. Versão do aplicativo
xv. Fabricante
xvi. Tipo e versão
xvii. Arquitetura

q. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

r. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

s. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

i. Dispositivos Desktop/Servidores
ii. Dispositivos móveis
iii. Dispositivos de rede
iv. Dispositivos virtuais
v. Componentes OEM
vi. Periféricos de computador
vii. Dispositivos IoT conectados
viii. Telefones VoIP
ix. Repositórios de rede

t. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

i. Nome da Aplicação
ii. Caminho do aplicativo
iii. Metadados do aplicativo
iv. Aplicativo Certificado digital
v. Categorias de aplicativos predefinidas pelo fornecedor
vi. SHA256 e MD5

u. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

i. Bluetooth
ii. Dispositivos móveis
iii. Modems externos
iv. CD/DVD
v. Câmeras e scanners
vi. MTPs
vii. E a transferência de dados para dispositivos móveis

v. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

w. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

x. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

i. Estruturas de domínios e grupos de trabalho do Windows
ii. Estruturas de grupos do Active Directory
iii. Conteúdo de um arquivo de texto criado manualmente pelo administrador

y. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

z. A solução proposta deve permitir realizar as seguintes ações para endpoints:

i. Verificação manual;
ii. Verificação no acesso;
iii. Verificação por demanda;
iv. Verificação de arquivos compactados
v. Verificação de arquivos individuais, pastas e unidades;
vi. Bloqueio e verificação de scripts

vii. Proteção contra alteração de registros;
viii. Proteção contra estouro de buffer;
ix. Verificação em segundo plano/inativa

1.1. Verificação de unidade removível na conexão com o sistema;
1.2. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.
1.3. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.
1.4. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.
1.5. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.
1.6. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.
1.7. A solução proposta deve suportar Windows Failover Cluster.
1.8. A solução proposta deve ter um recurso de clustering integrado.
1.9. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.
1.10. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.
1.11. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.
1.12. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.
1.13. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.
1.14. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.
1.15. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.
1.16. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.
1.17. A solução proposta deverá possuir controles para download de DLL e drivers.
1.18. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão.
1.19. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.
1.20. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).
1.21. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.
1.22. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir

as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.
1.23. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.
1.24. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.
1.25. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.
1.26. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.
1.27. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.
1.28. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.
1.29. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.
1.30. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.
1.31. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. .
1.32. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.
1.33. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.
1.34. A solução proposta deve permitir ao administrador personalizar relatórios.
1.35. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.
1.36. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.
1.37. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.
1.38. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.
1.39. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.

1.40. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.
1.41. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;
1.42. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.
1.43. A solução proposta deve suportar integração com solução APT.
1.44. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.
1.45. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:
1.45.1. Windows
1.45.2. Linux
1.46. A solução proposta deverá suportar os seguintes servidores de banco de dados:
1.46.1.1. Windows:
1.46.1.2. Microsoft SQL Server
1.46.1.3. Microsoft Banco de dados SQL do Azure
1.46.1.4. MySQL Standard e Enterprise
1.46.1.5. MariaDB
1.46.1.6. PostgreSQL
1.46.2. Linux:
1.46.2.1. MySQL
1.46.2.2. MariaDB
1.46.2.3. PostgreSQL
1.47. A solução proposta deverá suportar as seguintes plataformas virtuais:
1.47.1.1. Windows:
1.47.1.2. VMware vSphere 6.7 e 7.0
1.47.1.3. Estação de trabalho VMware 16 Pro
1.47.1.4. Servidor Microsoft Hyper-V 2012 de 64 bits
1.47.1.5. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
1.47.1.6. Microsoft Servidor Hyper -V 2016 de 64 bits
1.47.1.7. Servidor Microsoft Hyper-V 2019 de 64 bits
1.47.1.8. Servidor Microsoft Hyper-V 2022 de 64 bits
1.47.1.9. Citrix XenServer 7.1 LTSR
1.47.1.10. Citrix XenServer 8.x
1.47.1.11. Oracle VM VirtualBox 6.x
1.47.2. Linux:
1.47.2.1. VMware vSphere 6.7, 7.0 e 8.0
1.47.2.2. VMware Desktop 16 Pro e 17 Pro
1.47.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits
1.47.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
1.47.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits
1.47.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits
1.47.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits
1.47.2.8. Citrix XenServer 7.1 e 8.x

1.47.2.9. Oracle VM VirtualBox 6.x e7.x
1.48. A solução proposta deve suportar criptografia em vários níveis:
1.48.1. Criptografia completa do disco – incluindo disco do sistema
1.48.2. Criptografia de arquivos e pastas
1.48.3. Criptografia de mídia removível
1.48.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2
1.49. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:
1.49.1. A criptografia de arquivos em unidades de computador locais.
1.49.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.
1.49.3. A criação de listas criptografadas de pastas em unidades de computador locais.
1.50. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:
1.50.1. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.
1.50.2. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.
1.51. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:
1.51.1. A criptografia de todos os arquivos armazenados em unidades removíveis.
1.51.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.
1.52. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia
1.53. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.
1.54. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.
1.55. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.
1.56. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.
1.57. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.
1.58. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.

1.59. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.
1.60. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.
1.61. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.
1.62. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.
1.63. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.
1.64. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.
1.65. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário.
1.66. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.
1.67. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.
1.68. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:
1.68.1. Uso do Trusted Platform Module e configurações de senha.
1.68.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.
1.69. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).
1.70. A solução proposta deve suportar criptografia em Microsoft Surface Tablets.
1.71. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
1.71.1. Instalação remota de software de terceiros
1.71.2. Relatórios sobre software e hardware existentes
1.71.3. Monitoramento para instalação de software não autorizado
1.71.4. Remoção de software não autorizado
1.72. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.
1.73. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.
1.74. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.
1.75. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.
1.76. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.

1.77. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.
1.78. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.
1.79. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança
1.80. A solução proposta deve permitir ao administrador aprovar atualizações.
1.81. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.
1.82. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.
1.83. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.
1.84. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.
1.85. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.
1.86. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).
1.87. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.
1.88. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.
1.89. A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’.
1.90. A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”.
1.91. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.
1.92. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.
1.93. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.
1.94. A solução proposta deve apoiar a implantação do sistema operacional.
1.95. A solução proposta deve suportar Wake-on LAN e UEFI.
1.96. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.
1.97. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.
1.98. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.
1.99. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.
1.100. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.

1.101. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.
1.102. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.
1.103. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.
1.104. A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.
1.105. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:
1.105.1. Inicie a instalação ao reiniciar ou desligar o computador.
1.105.2. Instale o gerador necessário todos os pré-requisitos do sistema.
1.105.3. Permitir a instalação de novas versões de aplicativos durante as atualizações.
1.105.4. Baixe atualizações para o dispositivo sem instalá-las.
1.106. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.
1.107. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.
1.108. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:
1.108.1. CEF;
1.108.2. LEEF;
1.109. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.
1.110. O relatório da solução proposta deve conter informações CVE.
1.111. A solução proposta deve suportar instalação de aplicações e software de terceiros;

4.3. Do módulo de gerenciamento simplificado
1.112. A solução proposta deve suportar arquitetura cloud;
1.113. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.
1.114. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.
1.115. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.
1.116. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.
1.117. A solução proposta deve atender as condições apontadas no item e subintes 6.
1.118. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.
1.119. A solução proposta deve incluir informações do endpoint:
1.119.1. IP público de internet;
1.119.2. IP interno do dispositivo;
1.119.3. Versão do agente de proteção;

1.119.4. Ultima comunicação com a console, contendo data e hora;
1.119.5. Informações do sistema operacional;
1.120. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.
1.121. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.
1.122. A solução proposta deve incluir treinamento em segurança cibernética.

4.4. Requisitos gerais

1.123. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
1.123.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.
1.124. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
1.125. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).
1.126. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.
1.127. A solução proposta deve suportar o subsistema Linux no Windows.
1.128. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
1.128.1. Proteção contra ameaças sem arquivos (Fileless);
1.128.2. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;
1.129. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;
1.130. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.
1.131. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.
1.132. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.
1.133. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.
1.134. A solução proposta deve fornecer análise comportamental baseada em machine learning.
1.135. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.
1.136. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
1.136.1. Controles de aplicativos,
1.136.2. Controle web e dispositivos
1.136.3. HIPS e Firewall
1.136.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;

1.136.5. Gerenciamento de criptografia de arquivos e discos;
1.136.6. Controle adaptativo para detecção de anomalias;
1.137. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.
1.138. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.
1.139. A solução proposta deve ter bancos de dados de reputação locais e globais.
1.140. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.
1.141. A solução proposta deve incluir um módulo capaz, no mínimo, de:
1.141.1. Bloqueio de aplicativos com base em sua categorização.
1.141.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.
1.141.3. A adição de sub-redes e a modificação de permissões de atividade.
1.142. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.
1.143. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.
1.144. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.
1.145. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
1.145.1. Modo silencioso;
1.145.2. Discos rígidos e dispositivos removíveis;
1.145.3. De todos as contas de usuários do dispositivo.
1.146. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:
1.146.1. Exclusão imediata de dados;
1.146.2. Exclusão de dados adiada.
1.147. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:
1.147.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
1.147.2. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.
1.148. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.
1.149. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.
1.150. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.
1.151. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

1.152. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.
1.153. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.
1.154. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.
1.155. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;
1.156. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;
1.157. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.
1.158. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.
1.159. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.
1.160. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.
1.161. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.
1.162. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.
1.163. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.
1.164. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.
1.165. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.
1.166. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.
1.167. A solução proposta deve ter categoria de detecção para bloquear banners de sites.
1.168. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;
1.169. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.
1.170. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.
1.171. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.
1.172. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

1.173. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.
1.174. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.
1.175. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.
1.176. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.
1.177. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.
1.178. A solução proposta deve suportar o controle de scripts executados em PowerShell.
1.179. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.
1.180. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.
1.181. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.
1.182. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.
1.183. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.
1.184. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.
1.185. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
1.185.1. Filtro de anexos.
1.185.2. Verificação de mensagens de email ao receber, ler e enviar.
1.186. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.
1.187. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;
1.188. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);
1.189. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.
1.190. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.
1.191. A solução proposta deve incluir suporte ao protocolo IPv6.
1.192. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.
1.193. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
1.194. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.

1.195. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.
1.196. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.
1.197. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.
1.198. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.
1.199. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.
1.200. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.
1.201. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.
1.202. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.
1.203. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.
1.204. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.
1.205. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.
1.206. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.
1.207. A solução proposta deve suportar endereços IPv6.
1.208. A solução proposta deve suportar verificação em duas etapas (autenticação).
1.209. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.
1.210. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.
1.211. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.
1.212. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.
1.213. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.
1.214. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.
1.215. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.
1.216. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.

1.217. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.
1.218. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.
1.219. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.
1.220. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.
1.221. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.
1.222. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.
1.223. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.
1.224. A solução proposta deve ter a capacidade de excluir atualizações baixadas.
1.225. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.
1.226. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.
1.227. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.
1.228. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.
1.229. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.
1.230. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.
1.231. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.
1.232. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.
1.233. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
1.233.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.
1.233.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.
1.234. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.
1.235. A solução proposta deve gerar relatoiros de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

4.5. Do modulo de gerenciamento de dispositivos móveis

1.236. O modulo deve ser integrado a console de gerenciamento;
1.237. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
1.237.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)

1.238. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
1.238.1. iOS 10–17 ou iPadOS 13–17
1.239. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.
1.240. A solução proposta deve suportar dispositivos iOS supervisionados.
1.241. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.
1.242. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.
1.243. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.
1.244. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).
1.245. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.
1.246. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.
1.247. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.
1.248. A solução proposta deve ter recursos de conteinerização para dispositivos Android.
1.249. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:
1.249.1. Dados em contêineres
1.249.2. Contas de e-mail corporativo
1.249.3. Configurações para conexão à rede Wi-Fi corporativa e VPN
1.249.4. Nome do ponto de acesso (APN)
1.249.5. Perfil do Android for Work
1.249.6. Recipiente KNOX
1.249.7. Chave do gerenciador de licença KNOX
1.250. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
1.250.1. Todos os perfis de configuração instalados
1.250.2. Todos os perfis de provisionamento
1.250.3. O perfil iOS MDM
1.251. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas
1.252. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo .
1.253. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:
1.253.1. Critérios de verificação do dispositivo;

1.253.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;
1.254. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.
1.255. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:
1.255.1. Cartões de memória e outras unidades removíveis
1.255.2. Câmera do dispositivo
1.255.3. Conexões Wi-Fi
1.255.4. Conexões Bluetooth
1.255.5. Porta de conexão infravermelha
1.255.6. Ativação do ponto de acesso Wi-Fi
1.255.7. Conexão de área de trabalho remota
1.255.8. Sincronização de área de trabalho
1.255.9. Definir configurações da caixa de correio do Exchange
1.255.10. Configurar caixa de e-mail em dispositivos iOS MDM
1.255.11. Configure contêineres Samsung KNOX.
1.255.12. Definir as configurações do perfil do Android for Work
1.255.13. Configurar e-mail/calendário/contatos
1.255.14. Defina as configurações de restrição de conteúdo de mídia.
1.255.15. Definir configurações de proxy no dispositivo móvel
1.255.16. Configurar certificados e SCEP
1.256. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay .
1.257. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:
1.257.1. Google Play, Huawei App Gallery e Apple App Store
1.257.2. Portal de inscrição móvel KNOX
1.257.3. Pacotes de instalação pré-configurados independentes
1.258. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.
1.259. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.
1.260. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
1.260.1. VMware AirWatch 9.3 ou posterior
1.260.2. MobileIron 10.0 ou posterior
1.260.3. IBM MaaS360 10.68 ou posterior
1.260.4. Microsoft Intune 1908 ou posterior
1.260.5. SOTI MobiControl 14.1.4 (1693) ou posterior
1.261. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.
1.262. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:
1.262.1. Google Play
1.262.2. Galeria de aplicativos Huawei

1.262.3. Loja de aplicativos da Apple
1.263. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.
1.264. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.
1.265. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.
1.266. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.
1.267. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.
1.268. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.
1.269. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.
1.270. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.
1.271. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.
1.272. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.
1.273. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.
1.274. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.
1.275. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
1.276. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

4.6. Do módulo de EDR

4.6.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
4.6.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
4.6.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
4.6.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
4.6.5. Deve apresentar informações detalhadas contendo:
4.6.5.1.Usuário que executou a ação;
4.6.5.2.Informações acesso privilegiado;
4.6.6. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.
4.6.7. A solução proposta deve suportar integração com serviço de reputação em nuvem.
4.6.8. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)

4.6.9. O agente EDR deve ter integração com o aplicativo de proteção de endpoint(agente único).
4.6.10. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;
4.6.11. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.
4.6.12. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.
4.6.13. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.
4.6.14. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.
4.6.15. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.
4.6.16. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.
4.6.17. A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.
4.6.18. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.
4.6.19. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.
4.6.20. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:
4.6.21. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).
4.6.22. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.
4.6.23. Informações gerais sobre a detecção, incluindo modo de detecção.
4.6.24. Alterações no registro associadas à detecção.
4.6.25. Histórico da presença de arquivos no dispositivo.
4.6.26. Ações de resposta executadas pela aplicação.
4.6.27. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.
4.6.28. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:
4.6.29. Processo
4.6.30. Conexões de rede
4.6.31. Alterações no registro
4.6.32. Detalhes do download de objeto
4.6.33. A solução proposta deve fornecer orientação de resposta (resposta guiada).
4.6.34. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente

4.6.35. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
4.6.36. Impedir a execução de objetos
4.6.37. Isolamento de host
4.6.38. Excluir objeto do host ou grupo de hosts
4.6.39. Encerrar um processo no dispositivo
4.6.40. Colocar um objeto em quarentena
4.6.41. Execute a verificação do sistema
4.6.42. Execução remota de programa/processo/comando
4.6.43. Iniciar a varredura IoC para um grupo de hosts.

4.1. Requisitos para documentação da solução.
4.1.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:
4.1.2. Ajuda on-line para administradores
4.1.3. Ajuda on-line para melhores práticas de implementação
4.1.4. Ajuda on-line para proteção de servidores de administração
4.1.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.
4.2. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

5. PRAZO DE GARANTIA

5.1. As empresas licitantes deverão indicar o prazo da garantia do Software ou licença, que deverá ser de 36 meses oferecido diretamente ou com a autorização e responsabilidade do fabricante, sendo este o período em que se obrigam a prestar a manutenção e assistência técnica gratuita, nos termos regulados na minuta do contrato.

5.2. Serão desclassificadas as propostas que não ofereçam prazo de garantia ou abaixo do mínimo estipulado. As empresas licitantes indicarão, SOB PENA DE DESCLASSIFICAÇÃO, informações relacionadas à PADRONIZAÇÃO e COMPATIBILIDADE da solução, conforme detalhamento no ETP.

6. OBRIGAÇÕES DA CONTRATANTE

6.1. Comunicar à Contratada quaisquer irregularidades nos equipamentos, para adoção das providências cabíveis;

6.2. Designar funcionário para acompanhar/fiscalizar a entrega;

6.3. Efetuar os pagamentos relativos ao presente contrato em moeda corrente quando da apresentação da fatura de serviços executados respeitando os prazos de vencimentos;

6.4. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;

6.5. Qualquer alteração deste, somente deverá ser com o aval dos gestores do contrato;

6.6. Aplicar a contratada as sanções administrativas regulamentares e contratuais cabíveis;

7. OBRIGAÇÕES DA CONTRATADA

7.1. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

7.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do contrato, inerentes à execução do objeto contratual;

7.3. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

7.4. É de responsabilidade da CONTRATADA, manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

8. DA SUBCONTRATAÇÃO

8.1. Não será admitida a subcontratação do objeto.

9. MODELO DE EXECUÇÃO DO OBJETO

Em até, 30 dias, a contar da assinatura do contrato, as novas licenças deverão ser fornecidas e registradas em nome de CÂMARA MUNICIPAL DE FOZ DO IGUAÇU, nome fantasia PODER LEGISLATIVO, CNPJ 75.914.051/0001-28, atreladas a conta suporte@fozdoiguacu.pr.leg.br , dentro da plataforma da desenvolvedora Kaspersky Global.
Quando que realizada a disponibilização da licença, notificar via e-mail os responsáveis técnicos, sanches@fozdoiguacu.pr.leg.br e rodrigo@fozdoiguacu.pr.leg.br com detalhes do acesso.

10. MODELO DE GESTÃO DO CONTRATO E CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

A execução do objeto seguirá a seguinte dinâmica:

6.1 A contratante indicará Fiscal de contratos que irá acompanhar a execução do contrato em conformidade com este termo de referência.

6.2 O Contrato terá o prazo de 3 (três) anos, podendo ser prorrogado.

6.3 A Contratada formalizará a designação do preposto da empresa, especificando os poderes e responsabilidades relacionados à execução do objeto contratado.

6.4 Toda comunicação entre a Contratante e a Contratada deverá ser formalizada por escrito, especialmente quando exigido por lei, podendo ser realizada por meio de mensagem eletrônica, quando aplicável.

6.5 A execução será realizada de forma parcelada formalizada pelo envio da ordem de compra.

6.6 Os prazos e critérios para recebimento e pagamento estão detalhados nos itens 7.3 a 7.4.

6.7 Considera-se ocorrido o recebimento da nota fiscal quando a Gestão de contratos atestar a execução do objeto do contrato através do termo de recebimento definitivo.

6.8 Não haverá exigência de garantia contratual da execução, devido às características da

contratação.

6.9 A apresentação da Nota Fiscal/fatura é indispensável a cada fornecimento de bem ou serviço, para fins de liquidação e pagamento da despesa, emitida ao destinatário: Razão social: CÂMARA MUNICIPAL DE FOZ DO IGUACU; CNPJ: 75.914.051/0001-28; Endereço: Travessa Oscar Muxfeldt, nº 81, Centro, na cidade de Foz do Iguaçu-Paraná, CEP 85.851-490. Telefone: (45) 3521-8100.

6.10 Antes de cada pagamento à Contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

6.11 Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se- á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

6.12 Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

6.13 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

6.14 Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 20 (vinte) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da Contratante.

6.15 Persistindo a irregularidade, a Contratante deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa.

6.16 Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso a Contratada não regularize sua situação junto ao SICAF.

6.17 O prazo desta contratação será de 36 meses, contados da assinatura do contrato.

6.18 Pagamento:

6.18.1 Os pagamentos serão efetuados até o 10° (décimo) dia após o recebimento definitivo dos bens, condicionado a apresentação da Nota Fiscal/Fatura, bem como os documentos de regularidade

fiscal, social e trabalhista exigidos pelo art. 68 da Lei n° 14.133/2021
6.18.2 Na eventualidade de ocorrer atraso no pagamento, o valor será atualizado pela variação acumulada do IPCA/IBGE, ocorrida entre a data de seu adimplemento e a do efetivo pagamento, calculada pro rata tempore.
7 Sanções:
7.1 Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei n° 14.133, de 2021, quais sejam:
7.2 Dar causa à inexecução parcial do contrato;
7.3 Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;
7.4 Dar causa à inexecução total do contrato;
7.5 Deixar de entregar a documentação exigida para o certame;
7.6 Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
7.7 Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
7.8 Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;
7.9 Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;
7.10 Fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;
7.11 Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
7.12 Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.
7.13 Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;
7.14 O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:
a) Multa de até 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor,
b) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver
c) aplicado a sanção, pelo prazo máximo de 3 (três) anos.
d) Direta, quando não se justificar a imposição de penalidade mais grave;
e) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 8.9 a bem como nos demais casos que justifiquem a imposição da penalidade mais grave.
8 A fiscalização do contrato será realizada pelo servidor(a) designado:
9 A gestão do contrato será realizada pelo servidor (a) designado:

11. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

O fornecedor será selecionado por meio de DISPENSA DE LICITAÇÃO, com a interpretação mais flexível, e considerado o atual limite de R$59.906,02 para serviços e fornecimentos, conforme art. 75, inc. II, da Lei º 14.133/21 c/c Decreto nº 11.871/2023.

Tratamento diferenciado e favorecido a ser dispensado às microempresas, às empresas de pequeno porte e aos microempreendedores individuais conforme definido pelo documento de estudo técnico preliminar (ETP).

12. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

As quantidades previstas a serem adquiridas, conforme os itens descritos, são:

Item	Descrição	SKU	Quantidade	Valor Unit.	Valor
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160	R$ 358,19	R$ 57.310,40

A pesquisa de preço foi realizada considerando os parâmetros dispostos da Lei 14.133 no art. 23 § inciso IV – *"pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital"*. Do qual optou-se pelo menor preço ofertado.

Quanto à não utilização dos parâmetros dos § Incisos I e II do Art. 23, consultas no portal PNCP (Inciso I) e contratações similares feitas pela Administração Pública (II), conforme descrito no parágrafo anterior, torna-se ineficaz e escassa a busca por contratações similares em outros órgãos. Regendo-se pela economicidade, melhor tecnologia e melhores resultados pretendidos pelo órgão, a consulta aos fornecedores torna-se mais eficaz.

13. ADEQUAÇÃO ORÇAMENTÁRIA

ITEM	DOTAÇÃO
1	01.01.01.031.0001.2002.3.3.90.40.99.05 - AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE

Proc. Administrativo 13- 243/2024

De: Rodrigo N. - CMFI-DG-DIRTEC-EATI

Para: Envolvidos internos acompanhando

Data: 05/08/2024 às 12:46:13

RPP

_

Rodrigo Nishimori
Administrador de Rede

Anexos:

RELATORIA_PESQUISA_DE_PRECOS.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Rafael Sanches Alencar	05/08/2024 12:51:29	1Doc	RAFAEL SANCHES ALENCAR CPF 006.XXX.XXX-96

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **B8A0-324B-D4FB-C1EB**

RELATÓRIO DE PESQUISA DE PREÇOS, PLANILHA COMPARATIVA E DOCUMENTAÇÃO COMPROBATÓRIA

INTRODUÇÃO

O presente relatório é resultado da pesquisa de preços abaixo discriminada em cumprimento ao determinado na Lei nº 14.133/2021 em conformidade com o Ato da Presidência nº 136/2023.

AGENTE RESPONSÁVEL PELA PESQUISA: Rafael Sanches Alencar

OBJETO: Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses

MÉTODO ESTATÍSTICO APLICADO COM JUSTIFICATIVAS PARA A METODOLOGIA UTILIZADA, EM ESPECIAL PARA A DESCONSIDERAÇÃO DE VALORES INCONSISTENTES, INEXEQUÍVEIS OU EXCESSIVAMENTE ELEVADOS, SE APLICÁVEL: Os valores foram com base em orçamentos obtidos em mercado, no qual se optou pelo menor preço, a fim de satisfazer as demandas desta casa de leis.

CARACTERIZAÇÃO DAS FONTES DE PESQUISA CONSULTADAS: Foram realizadas pesquisas de preços utilizando-se dos seguintes parâmetros *estabelecidos no Ato da Presidência nº 136/2023, no qual Art. 6º "A pesquisa* de preços para fins de determinação do preço estimado na contratação direta para a aquisição de bens e contratação de serviços em geral, consolidada em mapa comparativo, terá prazo de validade de 6 (seis) meses e será realizada mediante a utilização dos seguintes parâmetros, **de forma combinada ou não"**. No qual foi utilizada IV – pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos orçamentos com mais de 6 (seis) meses de antecedência da data da pesquisa de preço;

JUSTIFICATIVA DAS FONTES CONSULTADAS: Foi consultado várias empresas, porém somente uma apresentou a proposta e editais citados no ETP, conforme os documentos juntados a este processo, e ainda devido a

especificidade da contração, bem como a necessidade do contrato de todos os itens, por terem interdependência entre si.

PERÍODO DE REALIZAÇÃO DA PESQUISA DE PREÇOS: Junho de 2024.

Abaixo relatório detalhado identificando cada um dos itens e seus valores obtidos:

PESQUISA DE MERCADO						
LOTE I - ITEM 1 - Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License						
FORNECEDOR	**MARCA**	**C/D**	**ART. 7º §4º**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL**
OPTIMUS DATA TECHNOLOGY LTDA		C	Exequível	160	R$ 358,19	R$ 57.310,40
Avant		C	Exequível	160	R$ 445,94	R$ 71.350,40
Solo Network		C	Exequível	160	R$ 411,26	R$ 65.801,60
		C		0		R$ 0,00
	-	C		1		R$ 0,00
	-	C		1		R$ 0,00
	-	C		1		R$ 0,00
MENOR PREÇO/FORNECEDOR					**R$ 57.310,40**	**#N/D**

VALOR TOTAL R$57.310,40 (Cinquenta e sete mil, trezentos e dez reais com quarenta centavos).

Eu, Rafael Sanches Alencar, declaro que efetuei a pesquisa de preços, na forma dos incisos I do artigo 23° da Lei n° 14.133/2021, em conformidade com o Ato da Presidência nº 136/2023 e que os preços aqui apresentados condizem com os praticados no mercado.

Proc. Administrativo 14- 243/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: CMFI-PRESID-DG-DIRFIN-COM-EC - Equipe Compras - A/C Débora R.

Data: 05/08/2024 às 14:32:53

Prezada Débora Borges Rengel - CMFI-PRESID-DG-DIRFIN-COM-EC,

Em resposta ao despacho 10 datado de 30/07/2024, constante no processo 243/2024 disponível no sistema 1Doc, onde são indicados itens que necessitam de adequação, esta diretoria informa que realizou as adequações.

Em tempo, evidenciamos que se trata uma contratação para fornecimento de licenças de solução de segurança pelo período de 36 meses, a formação da cesta de preço considerou o valor global, entretanto considerando a manifestação do setor de compras, esta equipe realizou o ajuste para a métrica de menor valor, mesmo que considerando a divisão dos valores pelo decurso de 36 meses, ficando dentro do teto máximo previsto inciso II do artigo 75 da Lei nº 14.133/2021.

Por fim, esta diretoria se manifesta favorável a publicação do ETP, considerando que o mesmo faz parte da fase preparatória conforme preconiza o artigo 18 da Lei nº 14.133.

–

Rafael Sanches
Diretoria de Tecnologia

Proc. Administrativo 15- 243/2024

De: CARLOS K. - CMFI-PRESID-DG-DIRFIN-COM

Para: CMFI-DG-DIRADM - Diretoria de Administração

Data: 06/08/2024 às 09:07:13

Prezados senhores,

Trata-se de contratação a ser realizada sob o **CNAE 6203-1/00 Desenvolvimento e licenciamento de programas de computador não customizáveis** que já foi objeto de contratação NO CORRENTE EXERCíCIO. Destaco que a previsão de gastos sob este CNAE está em **R$ 808.090,25 (oitocentos e oito mil, noventa reais e vinte e cinco centavos).**

Requeiro assim a conversão do presente processo em **Processo administrativo - Processo Licitatório**, eis que **não é possível** a realização de contratação direta através de dispensa de licitação por valor, no corrente exercício, para **nenhuma licença de software não customizável por expressa vedação legal** , exceto se **formalmente** forem canceladas todas as demais previsões de contratação.

–

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras

Proc. Administrativo 1- 279/2024

De: Nei S. - CMFI-DG-DIRADM

Para: CMFI-DG-DIRADM - Diretoria de Administração

Data: 06/08/2024 às 11:35:56

Encaminho para verificar a previsão do objeto e dos valores no PAC 2024

–

Nei Schlotefeldt
Consultor Legislativo

Proc. Administrativo 2- 279/2024

De: Nei S. - CMFI-DG-DIRADM

Para: CMFI-DG-DIRTEC-EATI - Tecnologia da Informação - A/C Jeverson S.

Data: 06/08/2024 às 11:38:00

Tendo em vista haver previsão dos valores e do objeto encaminho para as providências necessárias

–

Nei Schlotefeldt
Consultor Legislativo

Proc. Administrativo 3- 279/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: CMFI-PRESID-DG-DIRFIN-CON - Contabilidade

Data: 06/08/2024 às 11:58:03

Para indicação da rubrica orçamentária.

_

Rafael Sanches
Diretoria de Tecnologia

Anexos:

1_Termo_de_Referencia_Minuta.docx
ETP.docx

Proc. Administrativo 4- 279/2024

De: Nathalie N. - CMFI-PRESID-DG-DIRFIN-CON

Para: CMFI-DG-DIRTEC - Diretoria de Tecnologia

Data: 07/08/2024 às 09:27:50

Prezado,

Encaminho em anexo, Declaração de Adequação Orçamentária e Financeira e Demonstrativo da Despesa Realizada até 07/08/2024.

_

Nathalie Pereira Do Nascimento
Chefe da Contabilidade

Anexos:

DDR_07_08.pdf
DECLARACAO_DE_ADEQUACAO_ORCAMENTARIA_E_FINANCEIRA_Processo_Administrativo_279_2024_Renovacao_de_licencas_K

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Presidente da Câmara Munic...	07/08/2024 11:15:07	1Doc	PRESIDENTE DA CÂMARA MUNICIPAL DE FOZ DO IGU...

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **7970-C4AD-A066-F8AF**

DEMONSTRATIVO DA DESPESA REALIZADA COM PAGAMENTOS NO PERÍODO DE 01/01/2024 ATÉ 07/08/2024

DDR - Analítico

Orgão:01-CÂMARA MUNICIPAL DE FOZ DO IGUAÇU

Unidade:01-CÂMARA MUNICIPAL DE FOZ DO IGUAÇU

Dotação Orçamentária	Descrição da Dotação Orçamentária	Até o Período						No Período				Saldo Orc. Restante
		Orçado	Total	Bloqueado	Empenhado	Liquidado	Pago	Bloqueado	Empenhado	Liquidado	Pago	
		Alterações				Saldo a Liquidar	Consignado				Consignado	Saldo a Pagar
01.01.01.031.0001.2002	COORDENAÇÃO, SUPERVISÃO E ADMINISTRAÇÃO GERAL Recursos destinados a contribuição à ACAMOP (Associação das Câmaras Municipais do Oeste do Paraná) e a anuidade ao IBAM (Instituto Brasileiro de Administração Municipal) e Outros.	1.117.468,40	1.117.468,40	66.359,74	362.267,71	151.528,01	146.763,32	66.359,74	362.267,71	151.528,01	146.763,32	688.840,95
		0,00				210.739,70	4.764,69				4.764,69	210.739,70
3.3.90.40.00	SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – PESSOA JURÍDICA											
1.001	Recursos do Tesouro (Descentralizados) Exercício Corrente	1.117.468,40	1.117.468,40	66.359,74	362.267,71	151.528,01	146.763,32	66.359,74	362.267,71	151.528,01	146.763,32	688.840,95
		0,00				210.739,70	4.764,69				4.764,69	210.739,70
Total da Unidade:		1.117.468,40	1.117.468,40	66.359,74	362.267,71	151.528,01	146.763,32	66.359,74	362.267,71	151.528,01	146.763,32	688.840,95
		0,00				210.739,70	4.764,69				4.764,69	210.739,70
	Total do Orgão:	1.117.468,40	1.117.468,40	66.359,74	362.267,71	151.528,01	146.763,32	66.359,74	362.267,71	151.528,01	146.763,32	688.840,95
		0,00				210.739,70	4.764,69				4.764,69	210.739,70
	Total Geral:	**1.117.468,40**	**1.117.468,40**	**66.359,74**	**362.267,71**	**151.528,01**	**146.763,32**	**66.359,74**	**362.267,71**	**151.528,01**	**146.763,32**	**688.840,95**
		0,00				210.739,70	**4.764,69**				**4.764,69**	**210.739,70**

Este relatório foi configurado na coluna no período para calcular somente estornos de transações que ocorreram no período. Desta forma estornos de transações que ocorreram anterior a este período não serão computadas.

DECLARAÇÃO DE ADEQUAÇÃO ORÇAMENTÁRIA E FINANCEIRA

Processo Administrativo 279/2024 – Renovação de licenças Kaspersky

.

Eu, **João Morales**, Presidente desta Casa Legislativa, na qualidade de Ordenador da Despesa e em cumprimento às determinações no inciso II do artigo 16 da Lei Complementar nº 101, de 04 de maio de 2000, **DECLARO QUE AS DESPESAS RELACIONADAS AO OBJETO EM QUESTÃO TÊM ADEQUAÇÃO ORÇAMENTÁRIA E FINANCEIRA COM A LEI ORÇAMENTÁRIA ANUAL E COMPATIBILIDADE COM O PLANO PLURIANUAL E COM A LEI DE DIRETRIZES ORÇAMENTÁRIAS.**

Conforme estabelecido, a despesa correspondente será empenhada na seguinte dotação orçamentária:

2024:		
Item:	**Dotação:**	**Total:**
1 . KASPERSKY NEXT EDR OPTIMUM - 36 meses	01.01.01.031.0001.2002.3.3.90.40.99.05 - AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE	R$ 57.310,40

Foz do Iguaçu, 07 de agosto de 2024.

JOÃO MORALES
Presidente

Proc. Administrativo 5- 279/2024

De: Rodrigo N. - CMFI-DG-DIRTEC-EATI

Para: Envolvidos internos acompanhando

Data: 07/08/2024 às 11:20:11

ETP

_

Rodrigo Nishimori
Administrador de Rede

Anexos:

ETP_2_2_.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Jeverson Siqueira	07/08/2024 13:42:48	1Doc	JEVERSON SIQUEIRA CPF 080.XXX.XXX-74

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **86AC-350E-D424-A918**

ESTUDO TÉCNICO PRELIMINAR

1) DESCRIÇÃO DA NECESSIDADE

1.1. Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

1.2. A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

1.3. Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

1.4. Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

1.5. Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

1.6. Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

1.7. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.

2) REQUISITOS DA CONTRATAÇÃO

Item	Descriçao	SKU	Quantidade
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160

3) LEVANTAMENTO DE MERCADO

Considerando que a Câmara Municipal de Foz do Iguaçu já dispõe de um sistema de antivírus, foram avaliadas duas alternativas sendo uma delas a renovação e upgrade de versão do sistema e a outra a aquisição de um sistema integrado com o nosso sistema de Firewall.

Mantendo os investimentos já realizados, tendo em vista de que além da aquisição do sistema, foi também realizado a contratação de uma empresa especializada para nos auxiliar na configuração recomendadas pelo fabricante, e com base nas pesquisa de preços e estudo entre outras soluções, optou-se pela renovação e upgrade da versão já utilizada do licenciamento da solução Kaspersky e aquisição de novas licenças para contemplar a necessidade do parque computacional da CMFI, levando em consideração a ampliação do nosso parque computacional que ocorreu nesses últimos anos.

4) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

As especificações do objeto desta licitação deverão estar detalhadas no termo de referência elaborado com base neste estudo técnico preliminar e de acordo com a solicitação elaborada pelo setor demandante.

5) ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

Item	Descrição	SKU	Quantidade	Valor
1	KASPERSKY NEXT EDR OPTIMUM 36 meses	KL4066KASTJ	160	R$ 57.310,40

Descrição Item 1

A solução deve incluir treinamento em segurança cibernética

Do módulo de proteção de endpoint

Compatibilidade com diferentes sistemas operacionais, MAC OS, Linux de 32 e 64 bits (CentOS, Red Hat Enterprise, Debian, Ubuntu, Oracle Linux), Windows 7, 8, 8.1, 10,11 para desktops, para servidores S.O Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022, Windows Small Business Server 2011, Servidores de terminal Microsoft (Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022).

Módulo de gerenciamento avançado

A solução deve suportar arquitetura cloud-native e on-premisse, a solução deve incluir suporte para implantação baseada em nuvem (Amazon Web Services e/ou Microsoft Azure. Integração nativa com as seguintes opções de SIEM (HP (Microfoco) ArcSight, IBM QRadar, Splunk, Kaspersky KUMA). 2.4.

A solução deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

A solução deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

A solução deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

A solução deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

O servidor de gerenciamento primário da solução deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.
A solução deve suportar os seguintes canais de entrega de notificação, E-mail, registro de sistema e SMS ou equivalente.
A solução deve ter a capacidade de etiquetar/marcar computadores com base em Atributos de rede, Nome, Domínio e/ou Sufixo de Domínio, Endereço de IP, Endereço IP para servidor de gerenciamento, Localização no Active Directory, Unidade organizacional, Grupo, Sistema operacional, Número do pacote de serviço, Arquitetura Virtual, Registro de aplicativos, Nome da Aplicação, Versão do aplicativo, Fabricante, Tipo e versão, Arquitetura.
A solução deverá permitir especificamente o bloqueio dos seguintes dispositivos, Bluetooth, Dispositivos móveis, Modems externos, CD/DVD, Câmeras e scanners.
A solução deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.
A solução deve permitir realizar as seguintes ações para endpoints, verificação manual, verificação no acesso, verificação por demanda, verificação de arquivos compactados, verificação de arquivos individuais, pastas e unidades, bloqueio e verificação de scripts, proteção contra alteração de registros, proteção contra estouro de buffer, verificação em segundo plano/inativa.

A solução deverá suportar os seguintes servidores de banco de dados:
Windows,

- Microsoft SQL Server
- Microsoft Banco de dados SQL do Azure
- MySQL Standard e Enterprise
- MariaDB
- PostgreSQL

Linux:

- MySQL
- MariaDB
- PostgreSQL

A solução deverá suportar as seguintes plataformas virtuais:
Windows:

- VMware vSphere 6.7 e 7.0

- Estação de trabalho VMware 16 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Oracle VM VirtualBox 6.x

2.74.2. Linux:

- VMware vSphere 6.7, 7.0 e 8.0
- VMware Desktop 16 Pro e 17 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 e 8.x

Do módulo de gerenciamento simplificado

A solução deve suportar arquitetura cloud;

A solução deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

A solução deve permitir ao administrador gerar relatórios pré-definidos.

A solução deve incluir informações do endpoint, IP público de internet, IP interno do dispositivo, Versão do agente de proteção, ultima comunicação com a console, contendo data e hora, informações do sistema operacional;

Requisitos gerais

A solução deve ser capaz de detectar os seguintes tipos de ameaças:

Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

A solução deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
A solução deve ter capacidade de integração com a central de segurança do Windows Defender.
A solução deve suportar o subsistema Linux no Windows.
A solução deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

- Proteção contra ameaças sem arquivos (Fileless);
- Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

Do modulo de gerenciamento de dispositivos móveis

O modulo deve ser integrado a console de gerenciamento;
A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

- Android 5.0 ou posterior (incluindo Android 12L)

A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

- iOS 10–17 ou iPadOS 13–17

A solução deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

Do módulo de EDR

Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
A solução deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
Deve apresentar informações detalhadas contendo:

- Usuário que executou a ação;
- Informações acesso privilegiado;

A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas. O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único).

6) IMPACTOS AMBIENTAIS

Não foram identificados impactos ambientes nesta contratação

7) JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Não se aplica

8) CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

Não se identificou contratações interdependentes e/ou correlatas, sendo que a prestação dos serviços depende exclusivamente do presente procedimento.

9) ALINHAMENTO COM PAC – PLANO ANUAL DE CONTRATAÇÕES

A demanda em questão encontra-se prevista no plano anual de contratações.

10) RESULTADOS PRETENDIDOS

- Garantir um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;
- Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo estações de trabalho e notebooks comprometidos;
- Evitar, mitigar e conter a propagação de pragas digitais (vírus/malwares/spywares, spam, entre outros) com a administração centralizada da solução de proteção;
- Permitir o controle de acesso à rede por dispositivos computacionais, permitindo gerenciamento destes dispositivos;
- Possibilitar análise pormenorizada de arquivos, discos rígidos, unidades móveis, mensagens de e-mail e anexos, viabilizando detecção de ameaças, com intento de salvaguardar a estrutura tecnológica de ataques com teor e objetivo malicioso;
- Possibilitar o controle de acesso e tráfego de informações aos dispositivos e serviços operacionais na rede, através de gerenciamento centralizado, o que vem

a complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;

- Aprimorar a segurança de TIC da CMFI frente a ameaças sofisticadas.

11) PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Tendo em vista que nosso ambiente de tecnologia já possui uma solução de firewall, não será necessária nenhuma providência prévia.

12) VIABILIDADE DA CONTRATAÇÃO

Esta equipe de TI declara viável esta contratação

13) TRATAMENTO DIFERENCIADO E FAVORECIDO A SER DISPENSADO ÀS MICROEMPRESAS, ÀS EMPRESAS DE PEQUENO PORTE E AOS MICROEMPREENDEDORES INDIVIDUAIS

Após diversas tentativas de localização e contato com empresas qualificadas como microempresas (ME) e empresas de pequeno porte (EPP) na região de Foz do Iguaçu para fornecimento das licenças, constatou-se a inexistência, inclusive pelo embasamento da pesquisa na base de de empresas credenciadas junto ao portal do desenvolvedor, acessado na data de 10/06/2024 às 09:38. Durante o processo de prospecção, entramos em contato direto com diversas empresas locais, incluindo aquelas registradas como ME e EPP, para verificar a capacidade técnica e a disponibilidade para fornecimento do serviço requerido. Nenhuma das ME/EPP contactadas demonstrou capacidade técnica ou interesse em participar do certame.

Diante dessas circunstâncias, a manutenção da exclusividade do certame para ME e EPP pode inviabilizar a contratação, comprometendo a eficiência e a continuidade dos serviços públicos dependentes de uma conexão estável e de alta velocidade, eis que há sério risco da licitação ser deserta. Ressalta-se, porém, que as ME/EPP ainda poderão participar do certame com vantagens sobre os demais concorrentes conforme versa a legislação pátria.

Portanto, justifica-se o afastamento da exclusividade de participação de microempresas e empresas de pequeno porte neste certame específico, com base na inexistência de fornecedores locais qualificados e na necessidade imperiosa de garantir a prestação adequada e contínua dos serviços públicos.

14) RESPONSÁVEIS PELA ELABORAÇÃO DO ETP

Jeverson Siqueira
Cargo: Tecnico de Informatica
Matrícula: 202.045
Setor: Diretoria de Tecnologia

Proc. Administrativo 6- 279/2024

De: Rodrigo N. - CMFI-DG-DIRTEC-EATI

Para: Envolvidos internos acompanhando

Data: 07/08/2024 às 11:20:55

TR

_

Rodrigo Nishimori
Administrador de Rede

Anexos:

1_Termo_de_Referencia.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Rodrigo Nishimori	07/08/2024 11:21:14	1Doc	RODRIGO NISHIMORI CPF 007.XXX.XXX-01

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **ABC5-0F02-498C-9F1A**

TERMO DE REFERÊNCIA

1) DEFINIÇÃO DO OBJETO

Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

Item	CAT/MAT	Descrição	Prazo	SKU	Quantidade	Valor
1	350949	KASPERSKY NEXT EDR OPTIMUM 36 meses	36 meses	KL4066KASTJ	160	R$ 57.310,40

2) FUNDAMENTAÇÃO DA CONTRATAÇÃO

Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".
Considerando que esta casa de leis realiza a utilização da solução de segurança, sem ressalvas e visa proteger seu investimento, assegurar a padronização e compatibilidade com o ambiente computacional. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para, no mínimo, manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.
Com a iminente expiração da licença, torna-se necessária a renovação e aquisição para assegurar a proteção atualizada contra as ameaças virtuais mais recentes.
Sendo a demanda prevista no PAC, conforme documento de estudo técnico preliminar - ETP.

3) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução de segurança deve atender a necessidade de evolução e adequação desta casa em relação a suas ferramentas de proteção, esta casa de leis possui dois contratos ativos de licença da ferramenta KESB Select da desenvolvedora Kaspersky Global, em um deles possui o quantitativo de 130 licenças a expirar em 22/09/2024 e o outro de 20 licenças a expirar em 01/10/2024. Sendo assim, a solução apresentada deve fornecer 10 novas licenças e 150 em formato de renovação, adequada à nova linha de produtos das soluções de segurança com incremento de, no mínimo, EDR, bem como sua ativação. Referente a possibilidade de parcelamento, deve seguir de acordo com o ETP, por se tratar de uma solução integrada.

Custo Inicial Reduzido: Ao optar pela renovação, a empresa evita os altos custos iniciais de compra e instalação de novas soluções, permitindo a alocação de recursos para outras áreas críticas do negócio.

- **Suporte e atualizações:** Fornecimento dos serviços de suporte técnico, bem como atualizações, asseguram o perfeito funcionamento da solução.
- **Gestão Simplificada:** Por se tratar de uma solução integrada a gestão centralizada, permite aos profissionais maior autonomia e melhor condição de adaptação, visto que a equipe é reduzida.

Os itens da presente solução devem ser contratados em conjunto tendo em vista a necessidade de completa compatibilidade para o correto funcionamento.

a) Proteção antivírus de Arquivos;

b) Proteção antivírus da Web;

c) Firewall local de cada máquina;

d) Bloqueador de Ataques da Rede;

e) Inspeção do Sistema;

f) Inspeção avançada de dispositivos portáteis (pen drive, cartão de memória, etc);

g) Monitoramento de Vulnerabilidades.

4) REQUISITOS DA CONTRATAÇÃO

4.1. Do módulo de proteção de endpoint

a. A solução proposta deverá proteger os sistemas operacionais abaixo:

i. Windows 7
ii. Windows 8
iii. Windows 8.1
iv. Windows 10
v. Windows 11

b. Servidores

i. Windows Small Business Server 2011
ii. Windows MultiPoint Server 2011
iii. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

c. Servidores de terminal Microsoft

i. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

d. Sistemas operacionais Linux de 32 bits:

i. CentOS 6.7 e posterior
ii. Debian GNU/Linux 11.0 e posterior
iii. Debian GNU/Linux 12.0 e posterior
iv. Red Hat Enterprise Linux 6.7 e posterior

e. Sistemas operacionais Linux de 64 bits:

i. Amazon Linux 2.
ii. CentOS 6.7 e mais tarde
iii. CentOS 7.2 e posterior.
iv. CentOS Stream 8.
v. CentOS Stream 9.
vi. Debian GNU/Linux 11.0 e posterior.
vii. Debian GNU/Linux 12.0 e posterior.
viii. Linux Mint 20.3 e superior.
ix. Linux Mint 21.1 e posterior.
x. openSUSE Leap 15.0 e posterior.
xi. Oracle Linux 7.3 e posterior.
xii. Oracle Linux 8.0 e posterior.
xiii. Oracle Linux 9.0 e posterior.
xiv. Red Hat Enterprise Linux 6.7 e posterior
xv. Red Hat Enterprise Linux 7.2 e posterior.

xvi. Red Hat Enterprise Linux 8.0 e posterior.
xvii. Red Hat Enterprise Linux 9.0 e posterior.
xviii. Rocky Linux 8.5 e posterior.
xix. Rocky Linux 9.1.
xx. SUSE Linux Enterprise Server 12.5 ou posterior.
xxi. SUSE Linux Enterprise Server 15 ou posterior.
xxii. Ubuntu 20.04 LTS.
xxiii. Ubuntu 22.04 LTS.
xxiv. Sistemas operacionais Arm de 64 bits:
xxv. CentOS Stream 9.
xxvi. SUSE Linux Enterprise Server 15.
xxvii. Ubuntu 22.04 LTS.

f. Sistemas operacionais MAC OS:
i. macOS 12 – 14

g. Ferramentas de virtualização MAC OS:
i. Parallels Desktop 16 para Mac Business Edition
ii. VMware Fusion 11.5 Profissional
iii. VMware Fusion 12 Profissional

h. A solução proposta deverá suportar as seguintes plataformas virtuais:
i. VMware Workstation 17.0.2 Pro
ii. VMware ESXi 8.0 Update 2
iii. Microsoft Hyper-V Server 2019
iv. Citrix Virtual Apps e Desktop 7 2308
v. Citrix Provisioning 2308
vi. Citrix Hypervisor 8.2 Update 1

4.2. Do módulo de gerenciamento avançado

a. A solução proposta deve suportar arquitetura cloud-native e on-premisse;
b. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
i. Amazon Web Services
ii. Microsoft Azure
c. A solução proposta deve incluir as seguintes opções de integração SIEM:
i. HP (Microfoco) ArcSight
ii. IBM QRadar
iii. Splunk
iv. Kaspersky KUMA
d. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.
e. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;
f. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.
g. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.
h. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

i. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

j. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

k. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

l. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.

m. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

n. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:

i. Status do dispositivo
ii. Tag
iii. Diretório ativo
iv. Proprietários de dispositivos
v. Hardware

o. A solução proposta deve suportar os seguintes canais de entrega de notificação:

i. E-mail
ii. Registro de sistema
iii. SMS

p. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:

i. Atributos de rede
ii. Nome
iii. Domínio e/ou Sufixo de Domínio
iv. Endereço de IP
v. Endereço IP para servidor de gerenciamento
vi. Localização no Active Directory
vii. Unidade organizacional
viii. Grupo
ix. Sistema operacional
x. Número do pacote de serviço
xi. Arquitetura Virtual
xii. Registro de aplicativos
xiii. Nome da Aplicação
xiv. Versão do aplicativo
xv. Fabricante
xvi. Tipo e versão
xvii. Arquitetura

q. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

r. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

s. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

i. Dispositivos Desktop/Servidores
ii. Dispositivos móveis
iii. Dispositivos de rede
iv. Dispositivos virtuais
v. Componentes OEM
vi. Periféricos de computador
vii. Dispositivos IoT conectados
viii. Telefones VoIP
ix. Repositórios de rede

t. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

i. Nome da Aplicação
ii. Caminho do aplicativo
iii. Metadados do aplicativo
iv. Aplicativo Certificado digital
v. Categorias de aplicativos predefinidas pelo fornecedor
vi. SHA256 e MD5

u. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

i. Bluetooth
ii. Dispositivos móveis
iii. Modems externos
iv. CD/DVD
v. Câmeras e scanners
vi. MTPs
vii. E a transferência de dados para dispositivos móveis

v. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

w. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

x. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

i. Estruturas de domínios e grupos de trabalho do Windows
ii. Estruturas de grupos do Active Directory
iii. Conteúdo de um arquivo de texto criado manualmente pelo administrador

y. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

z. A solução proposta deve permitir realizar as seguintes ações para endpoints:

i. Verificação manual;
ii. Verificação no acesso;
iii. Verificação por demanda;
iv. Verificação de arquivos compactados
v. Verificação de arquivos individuais, pastas e unidades;
vi. Bloqueio e verificação de scripts

vii. Proteção contra alteração de registros;
viii. Proteção contra estouro de buffer;
ix. Verificação em segundo plano/inativa

1.1. Verificação de unidade removível na conexão com o sistema;
1.2. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.
1.3. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.
1.4. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.
1.5. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.
1.6. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.
1.7. A solução proposta deve suportar Windows Failover Cluster.
1.8. A solução proposta deve ter um recurso de clustering integrado.
1.9. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.
1.10. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.
1.11. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.
1.12. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.
1.13. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.
1.14. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.
1.15. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.
1.16. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.
1.17. A solução proposta deverá possuir controles para download de DLL e drivers.
1.18. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão.
1.19. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.
1.20. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).
1.21. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.
1.22. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir

as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.
1.23. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.
1.24. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.
1.25. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.
1.26. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.
1.27. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.
1.28. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.
1.29. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.
1.30. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.
1.31. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. .
1.32. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.
1.33. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.
1.34. A solução proposta deve permitir ao administrador personalizar relatórios.
1.35. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.
1.36. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.
1.37. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.
1.38. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.
1.39. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.

1.40. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.
1.41. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;
1.42. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.
1.43. A solução proposta deve suportar integração com solução APT.
1.44. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.
1.45. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:
1.45.1. Windows
1.45.2. Linux
1.46. A solução proposta deverá suportar os seguintes servidores de banco de dados:
1.46.1.1. Windows:
1.46.1.2. Microsoft SQL Server
1.46.1.3. Microsoft Banco de dados SQL do Azure
1.46.1.4. MySQL Standard e Enterprise
1.46.1.5. MariaDB
1.46.1.6. PostgreSQL
1.46.2. Linux:
1.46.2.1. MySQL
1.46.2.2. MariaDB
1.46.2.3. PostgreSQL
1.47. A solução proposta deverá suportar as seguintes plataformas virtuais:
1.47.1.1. Windows:
1.47.1.2. VMware vSphere 6.7 e 7.0
1.47.1.3. Estação de trabalho VMware 16 Pro
1.47.1.4. Servidor Microsoft Hyper-V 2012 de 64 bits
1.47.1.5. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
1.47.1.6. Microsoft Servidor Hyper -V 2016 de 64 bits
1.47.1.7. Servidor Microsoft Hyper-V 2019 de 64 bits
1.47.1.8. Servidor Microsoft Hyper-V 2022 de 64 bits
1.47.1.9. Citrix XenServer 7.1 LTSR
1.47.1.10. Citrix XenServer 8.x
1.47.1.11. Oracle VM VirtualBox 6.x
1.47.2. Linux:
1.47.2.1. VMware vSphere 6.7, 7.0 e 8.0
1.47.2.2. VMware Desktop 16 Pro e 17 Pro
1.47.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits
1.47.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
1.47.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits
1.47.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits
1.47.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits
1.47.2.8. Citrix XenServer 7.1 e 8.x

1.47.2.9. Oracle VM VirtualBox 6.x e7.x
1.48. A solução proposta deve suportar criptografia em vários níveis:
1.48.1. Criptografia completa do disco – incluindo disco do sistema
1.48.2. Criptografia de arquivos e pastas
1.48.3. Criptografia de mídia removível
1.48.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2
1.49. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:
1.49.1. A criptografia de arquivos em unidades de computador locais.
1.49.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.
1.49.3. A criação de listas criptografadas de pastas em unidades de computador locais.
1.50. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:
1.50.1. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.
1.50.2. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.
1.51. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:
1.51.1. A criptografia de todos os arquivos armazenados em unidades removíveis.
1.51.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.
1.52. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia
1.53. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.
1.54. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.
1.55. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.
1.56. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.
1.57. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.
1.58. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.

1.59. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.
1.60. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.
1.61. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.
1.62. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.
1.63. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.
1.64. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.
1.65. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário.
1.66. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.
1.67. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.
1.68. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:
1.68.1. Uso do Trusted Platform Module e configurações de senha.
1.68.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.
1.69. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).
1.70. A solução proposta deve suportar criptografia em Microsoft Surface Tablets.
1.71. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
1.71.1. Instalação remota de software de terceiros
1.71.2. Relatórios sobre software e hardware existentes
1.71.3. Monitoramento para instalação de software não autorizado
1.71.4. Remoção de software não autorizado
1.72. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.
1.73. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.
1.74. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.
1.75. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.
1.76. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.

1.77. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.
1.78. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.
1.79. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança
1.80. A solução proposta deve permitir ao administrador aprovar atualizações.
1.81. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.
1.82. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.
1.83. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.
1.84. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.
1.85. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.
1.86. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).
1.87. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.
1.88. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.
1.89. A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’.
1.90. A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”.
1.91. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.
1.92. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.
1.93. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.
1.94. A solução proposta deve apoiar a implantação do sistema operacional.
1.95. A solução proposta deve suportar Wake-on LAN e UEFI.
1.96. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.
1.97. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.
1.98. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.
1.99. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.
1.100. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.

1.101. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.
1.102. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.
1.103. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.
1.104. A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.
1.105. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:
1.105.1. Inicie a instalação ao reiniciar ou desligar o computador.
1.105.2. Instale o gerador necessário todos os pré-requisitos do sistema.
1.105.3. Permitir a instalação de novas versões de aplicativos durante as atualizações.
1.105.4. Baixe atualizações para o dispositivo sem instalá-las.
1.106. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.
1.107. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.
1.108. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:
1.108.1. CEF;
1.108.2. LEEF;
1.109. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.
1.110. O relatório da solução proposta deve conter informações CVE.
1.111. A solução proposta deve suportar instalação de aplicações e software de terceiros;

4.3. Do módulo de gerenciamento simplificado

1.112. A solução proposta deve suportar arquitetura cloud;
1.113. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.
1.114. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.
1.115. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.
1.116. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.
1.117. A solução proposta deve atender as condições apontadas no item e subintes 6.
1.118. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.
1.119. A solução proposta deve incluir informações do endpoint:
1.119.1. IP público de internet;
1.119.2. IP interno do dispositivo;
1.119.3. Versão do agente de proteção;

1.119.4. Ultima comunicação com a console, contendo data e hora;
1.119.5. Informações do sistema operacional;
1.120. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.
1.121. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.
1.122. A solução proposta deve incluir treinamento em segurança cibernética.

4.4. Requisitos gerais

1.123. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
1.123.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.
1.124. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
1.125. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).
1.126. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.
1.127. A solução proposta deve suportar o subsistema Linux no Windows.
1.128. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
1.128.1. Proteção contra ameaças sem arquivos (Fileless);
1.128.2. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;
1.129. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;
1.130. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.
1.131. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.
1.132. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.
1.133. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.
1.134. A solução proposta deve fornecer análise comportamental baseada em machine learning.
1.135. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.
1.136. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
1.136.1. Controles de aplicativos,
1.136.2. Controle web e dispositivos
1.136.3. HIPS e Firewall
1.136.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;

1.136.5. Gerenciamento de criptografia de arquivos e discos;
1.136.6. Controle adaptativo para detecção de anomalias;
1.137. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.
1.138. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.
1.139. A solução proposta deve ter bancos de dados de reputação locais e globais.
1.140. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.
1.141. A solução proposta deve incluir um módulo capaz, no mínimo, de:
1.141.1. Bloqueio de aplicativos com base em sua categorização.
1.141.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.
1.141.3. A adição de sub-redes e a modificação de permissões de atividade.
1.142. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.
1.143. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.
1.144. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.
1.145. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
1.145.1. Modo silencioso;
1.145.2. Discos rígidos e dispositivos removíveis;
1.145.3. De todos as contas de usuários do dispositivo.
1.146. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:
1.146.1. Exclusão imediata de dados;
1.146.2. Exclusão de dados adiada.
1.147. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:
1.147.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
1.147.2. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.
1.148. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.
1.149. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.
1.150. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.
1.151. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

1.152. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.
1.153. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.
1.154. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.
1.155. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;
1.156. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;
1.157. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.
1.158. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.
1.159. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.
1.160. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.
1.161. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.
1.162. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.
1.163. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.
1.164. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.
1.165. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.
1.166. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.
1.167. A solução proposta deve ter categoria de detecção para bloquear banners de sites.
1.168. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;
1.169. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.
1.170. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.
1.171. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.
1.172. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

1.173. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.
1.174. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.
1.175. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.
1.176. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.
1.177. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.
1.178. A solução proposta deve suportar o controle de scripts executados em PowerShell.
1.179. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.
1.180. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.
1.181. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.
1.182. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.
1.183. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.
1.184. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.
1.185. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
1.185.1. Filtro de anexos.
1.185.2. Verificação de mensagens de email ao receber, ler e enviar.
1.186. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.
1.187. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;
1.188. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);
1.189. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.
1.190. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.
1.191. A solução proposta deve incluir suporte ao protocolo IPv6.
1.192. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.
1.193. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
1.194. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.

1.195. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.
1.196. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.
1.197. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.
1.198. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.
1.199. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.
1.200. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.
1.201. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.
1.202. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.
1.203. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.
1.204. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.
1.205. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.
1.206. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.
1.207. A solução proposta deve suportar endereços IPv6.
1.208. A solução proposta deve suportar verificação em duas etapas (autenticação).
1.209. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.
1.210. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.
1.211. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.
1.212. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.
1.213. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.
1.214. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.
1.215. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.
1.216. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.

1.217. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.
1.218. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.
1.219. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.
1.220. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.
1.221. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.
1.222. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.
1.223. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.
1.224. A solução proposta deve ter a capacidade de excluir atualizações baixadas.
1.225. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.
1.226. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.
1.227. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.
1.228. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.
1.229. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.
1.230. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.
1.231. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.
1.232. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.
1.233. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
1.233.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.
1.233.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.
1.234. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.
1.235. A solução proposta deve gerar relatoiros de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

4.5. Do modulo de gerenciamento de dispositivos móveis

1.236. O modulo deve ser integrado a console de gerenciamento;
1.237. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
1.237.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)

1.238. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
1.238.1. iOS 10–17 ou iPadOS 13–17
1.239. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.
1.240. A solução proposta deve suportar dispositivos iOS supervisionados.
1.241. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.
1.242. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.
1.243. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.
1.244. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).
1.245. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.
1.246. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.
1.247. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.
1.248. A solução proposta deve ter recursos de conteinerização para dispositivos Android.
1.249. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:
1.249.1. Dados em contêineres
1.249.2. Contas de e-mail corporativo
1.249.3. Configurações para conexão à rede Wi-Fi corporativa e VPN
1.249.4. Nome do ponto de acesso (APN)
1.249.5. Perfil do Android for Work
1.249.6. Recipiente KNOX
1.249.7. Chave do gerenciador de licença KNOX
1.250. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
1.250.1. Todos os perfis de configuração instalados
1.250.2. Todos os perfis de provisionamento
1.250.3. O perfil iOS MDM
1.251. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas
1.252. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo .
1.253. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:
1.253.1. Critérios de verificação do dispositivo;

1.253.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;
1.254. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.
1.255. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:
1.255.1. Cartões de memória e outras unidades removíveis
1.255.2. Câmera do dispositivo
1.255.3. Conexões Wi-Fi
1.255.4. Conexões Bluetooth
1.255.5. Porta de conexão infravermelha
1.255.6. Ativação do ponto de acesso Wi-Fi
1.255.7. Conexão de área de trabalho remota
1.255.8. Sincronização de área de trabalho
1.255.9. Definir configurações da caixa de correio do Exchange
1.255.10. Configurar caixa de e-mail em dispositivos iOS MDM
1.255.11. Configure contêineres Samsung KNOX.
1.255.12. Definir as configurações do perfil do Android for Work
1.255.13. Configurar e-mail/calendário/contatos
1.255.14. Defina as configurações de restrição de conteúdo de mídia.
1.255.15. Definir configurações de proxy no dispositivo móvel
1.255.16. Configurar certificados e SCEP
1.256. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay .
1.257. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:
1.257.1. Google Play, Huawei App Gallery e Apple App Store
1.257.2. Portal de inscrição móvel KNOX
1.257.3. Pacotes de instalação pré-configurados independentes
1.258. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.
1.259. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.
1.260. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
1.260.1. VMware AirWatch 9.3 ou posterior
1.260.2. MobileIron 10.0 ou posterior
1.260.3. IBM MaaS360 10.68 ou posterior
1.260.4. Microsoft Intune 1908 ou posterior
1.260.5. SOTI MobiControl 14.1.4 (1693) ou posterior
1.261. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.
1.262. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:
1.262.1. Google Play
1.262.2. Galeria de aplicativos Huawei

1.262.3. Loja de aplicativos da Apple
1.263. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.
1.264. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.
1.265. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.
1.266. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.
1.267. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.
1.268. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.
1.269. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.
1.270. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.
1.271. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.
1.272. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.
1.273. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.
1.274. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.
1.275. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
1.276. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

4.6. Do módulo de EDR

4.6.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
4.6.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
4.6.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
4.6.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
4.6.5. Deve apresentar informações detalhadas contendo:
4.6.5.1.Usuário que executou a ação;
4.6.5.2.Informações acesso privilegiado;
4.6.6. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.
4.6.7. A solução proposta deve suportar integração com serviço de reputação em nuvem.
4.6.8. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)

4.6.9. O agente EDR deve ter integração com o aplicativo de proteção de endpoint(agente único).
4.6.10. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;
4.6.11. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.
4.6.12. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.
4.6.13. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.
4.6.14. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.
4.6.15. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.
4.6.16. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.
4.6.17. A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.
4.6.18. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.
4.6.19. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.
4.6.20. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:
4.6.21. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).
4.6.22. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.
4.6.23. Informações gerais sobre a detecção, incluindo modo de detecção.
4.6.24. Alterações no registro associadas à detecção.
4.6.25. Histórico da presença de arquivos no dispositivo.
4.6.26. Ações de resposta executadas pela aplicação.
4.6.27. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.
4.6.28. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:
4.6.29. Processo
4.6.30. Conexões de rede
4.6.31. Alterações no registro
4.6.32. Detalhes do download de objeto
4.6.33. A solução proposta deve fornecer orientação de resposta (resposta guiada).
4.6.34. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente

4.6.35. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
4.6.36. Impedir a execução de objetos
4.6.37. Isolamento de host
4.6.38. Excluir objeto do host ou grupo de hosts
4.6.39. Encerrar um processo no dispositivo
4.6.40. Colocar um objeto em quarentena
4.6.41. Execute a verificação do sistema
4.6.42. Execução remota de programa/processo/comando
4.6.43. Iniciar a varredura IoC para um grupo de hosts.

4.1. Requisitos para documentação da solução.
4.1.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:
4.1.2. Ajuda on-line para administradores
4.1.3. Ajuda on-line para melhores práticas de implementação
4.1.4. Ajuda on-line para proteção de servidores de administração
4.1.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.
4.2. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

5. PRAZO DE GARANTIA

5.1. As empresas licitantes deverão indicar o prazo da garantia do Software ou licença, que deverá ser de 36 meses oferecido diretamente ou com a autorização e responsabilidade do fabricante, sendo este o período em que se obrigam a prestar a manutenção e assistência técnica gratuita, nos termos regulados na minuta do contrato.

5.2. Serão desclassificadas as propostas que não ofereçam prazo de garantia ou abaixo do mínimo estipulado. As empresas licitantes indicarão, SOB PENA DE DESCLASSIFICAÇÃO, informações relacionadas à PADRONIZAÇÃO e COMPATIBILIDADE da solução, conforme detalhamento no ETP.

6. OBRIGAÇÕES DA CONTRATANTE

6.1. Comunicar à Contratada quaisquer irregularidades nos equipamentos, para adoção das providências cabíveis;

6.2. Designar funcionário para acompanhar/fiscalizar a entrega;

6.3. Efetuar os pagamentos relativos ao presente contrato em moeda corrente quando da apresentação da fatura de serviços executados respeitando os prazos de vencimentos;

6.4. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;

6.5. Qualquer alteração deste, somente deverá ser com o aval dos gestores do contrato;

6.6. Aplicar a contratada as sanções administrativas regulamentares e contratuais cabíveis;

7. OBRIGAÇÕES DA CONTRATADA

7.1. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

7.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do contrato, inerentes à execução do objeto contratual;

7.3. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

7.4. É de responsabilidade da CONTRATADA, manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

8. DA SUBCONTRATAÇÃO

8.1. Não será admitida a subcontratação do objeto.

9. MODELO DE EXECUÇÃO DO OBJETO

Em até, 30 dias, a contar da assinatura do contrato, as novas licenças deverão ser fornecidas e registradas em nome de CÂMARA MUNICIPAL DE FOZ DO IGUAÇU, nome fantasia PODER LEGISLATIVO, CNPJ 75.914.051/0001-28, atreladas a conta suporte@fozdoiguacu.pr.leg.br , dentro da plataforma da desenvolvedora Kaspersky Global.
Quando que realizada a disponibilização da licença, notificar via e-mail os responsáveis técnicos, sanches@fozdoiguacu.pr.leg.br e rodrigo@fozdoiguacu.pr.leg.br com detalhes do acesso.

10. MODELO DE GESTÃO DO CONTRATO E CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

A execução do objeto seguirá a seguinte dinâmica:

6.1 A contratante indicará Fiscal de contratos que irá acompanhar a execução do contrato em conformidade com este termo de referência.

6.2 O Contrato terá o prazo de 3 (três) anos, podendo ser prorrogado.

6.3 A Contratada formalizará a designação do preposto da empresa, especificando os poderes e responsabilidades relacionados à execução do objeto contratado.

6.4 Toda comunicação entre a Contratante e a Contratada deverá ser formalizada por escrito, especialmente quando exigido por lei, podendo ser realizada por meio de mensagem eletrônica, quando aplicável.

6.5 A execução será realizada de forma parcelada formalizada pelo envio da ordem de compra.

6.6 Os prazos e critérios para recebimento e pagamento estão detalhados nos itens 7.3 a 7.4.

6.7 Considera-se ocorrido o recebimento da nota fiscal quando a Gestão de contratos atestar a execução do objeto do contrato através do termo de recebimento definitivo.

6.8 Não haverá exigência de garantia contratual da execução, devido às características da

contratação.

6.9 A apresentação da Nota Fiscal/fatura é indispensável a cada fornecimento de bem ou serviço, para fins de liquidação e pagamento da despesa, emitida ao destinatário: Razão social: CÂMARA MUNICIPAL DE FOZ DO IGUACU; CNPJ: 75.914.051/0001-28; Endereço: Travessa Oscar Muxfeldt, nº 81, Centro, na cidade de Foz do Iguaçu-Paraná, CEP 85.851-490. Telefone: (45) 3521-8100.

6.10 Antes de cada pagamento à Contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

6.11 Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se- á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

6.12 Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

6.13 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

6.14 Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 20 (vinte) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da Contratante.

6.15 Persistindo a irregularidade, a Contratante deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa.

6.16 Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso a Contratada não regularize sua situação junto ao SICAF.

6.17 O prazo desta contratação será de 36 meses, contados da assinatura do contrato.

6.18 Pagamento:

6.18.1 Os pagamentos serão efetuados até o 10° (décimo) dia após o recebimento definitivo dos bens, condicionado a apresentação da Nota Fiscal/Fatura, bem como os documentos de regularidade

fiscal, social e trabalhista exigidos pelo art. 68 da Lei n° 14.133/2021

6.18.2 Na eventualidade de ocorrer atraso no pagamento, o valor será atualizado pela variação acumulada do IPCA/IBGE, ocorrida entre a data de seu adimplemento e a do efetivo pagamento, calculada pro rata tempore.

7 Sanções:

7.1 Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei n° 14.133, de 2021, quais sejam:

7.2 Dar causa à inexecução parcial do contrato;

7.3 Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

7.4 Dar causa à inexecução total do contrato;

7.5 Deixar de entregar a documentação exigida para o certame;

7.6 Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

7.7 Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

7.8 Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

7.9 Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

7.10 Fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

7.11 Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

7.12 Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

7.13 Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;

7.14 O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Multa de até 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor,

b) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver

c) aplicado a sanção, pelo prazo máximo de 3 (três) anos.

d) Direta, quando não se justificar a imposição de penalidade mais grave;

e) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 8.9 a bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

8 A fiscalização do contrato será realizada pelo servidor(a) designado:

9 A gestão do contrato será realizada pelo servidor (a) designado:

11. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço.

Tratamento diferenciado e favorecido a ser dispensado às microempresas, às empresas de pequeno porte e aos microempreendedores individuais conforme definido pelo documento de estudo técnico preliminar (ETP).

12. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

As quantidades previstas a serem adquiridas, conforme os itens descritos, são:

Item	Descrição	SKU	Quantidade	Valor Unit.	Valor
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160	R$ 358,19	R$ 57.310,40

A pesquisa de preço foi realizada considerando os parâmetros dispostos da Lei 14.133 no art. 23 § inciso IV – *"pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital"*. Do qual optou-se pelo menor preço ofertado.

Quanto à não utilização dos parâmetros dos § Incisos I e II do Art. 23, consultas no portal PNCP (Inciso I) e contratações similares feitas pela Administração Pública (II), conforme descrito no parágrafo anterior, torna-se ineficaz e escassa a busca por contratações similares em outros órgãos. Regendo-se pela economicidade, melhor tecnologia e melhores resultados pretendidos pelo órgão, a consulta aos fornecedores torna-se mais eficaz.

13. ADEQUAÇÃO ORÇAMENTÁRIA

ITEM	DOTAÇÃO
1	01.01.01.031.0001.2002.3.3.90.40.99.05 - AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE

Proc. Administrativo 7- 279/2024

De: Rodrigo N. - CMFI-DG-DIRTEC-EATI

Para: Envolvidos internos acompanhando

Data: 07/08/2024 às 12:18:24

RPP

–

Rodrigo Nishimori
Administrador de Rede

Anexos:

RELATORIA_PESQUISA_DE_PRECOS_2.pdf

RELATÓRIO DE PESQUISA DE PREÇOS, PLANILHA COMPARATIVA E DOCUMENTAÇÃO COMPROBATÓRIA

INTRODUÇÃO

O presente relatório é resultado da pesquisa de preços abaixo discriminada em cumprimento ao determinado na Lei nº 14.133/2021 em conformidade com o Ato da Presidência nº 136/2023.

AGENTE RESPONSÁVEL PELA PESQUISA: Rafael Sanches Alencar

OBJETO: Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses

MÉTODO ESTATÍSTICO APLICADO COM JUSTIFICATIVAS PARA A METODOLOGIA UTILIZADA, EM ESPECIAL PARA A DESCONSIDERAÇÃO DE VALORES INCONSISTENTES, INEXEQUÍVEIS OU EXCESSIVAMENTE ELEVADOS, SE APLICÁVEL: Os valores foram com base em orçamentos obtidos em mercado, no qual se optou pelo menor preço, a fim de satisfazer as demandas desta casa de leis.

CARACTERIZAÇÃO DAS FONTES DE PESQUISA CONSULTADAS: Foram realizadas pesquisas de preços utilizando-se dos seguintes parâmetros estabelecidos no Ato da Presidência nº 136/2023, no qual Art. 6º

> *"A pesquisa de preços para fins de determinação do preço estimado* na contratação direta para a aquisição de bens e contratação de serviços em geral, consolidada em mapa comparativo, terá prazo de validade de 6 (seis) meses e será realizada mediante a utilização dos seguintes parâmetros, **de forma combinada ou não"**.

No qual foi utilizada IV – pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos orçamentos com mais de 6 (seis) meses de antecedência da data da pesquisa de preço;

JUSTIFICATIVA DAS FONTES CONSULTADAS: Foi consultado várias empresas, porém somente uma apresentou a proposta e editais citados no ETP, conforme os documentos juntados a este processo, e ainda devido a

especificidade da contração, bem como a necessidade do contrato de todos os itens, por terem interdependência entre si.

PERÍODO DE REALIZAÇÃO DA PESQUISA DE PREÇOS: Junho de 2024.

Abaixo relatório detalhado identificando cada um dos itens e seus valores obtidos:

PESQUISA DE MERCADO						
LOTE I - ITEM 1 - Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License						
FORNECEDOR	**MARCA**	**C/D**	**ART. 7º §4º**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL**
OPTIMUS DATA TECHNOLOGY LTDA		C	Exequível	160	R$ 358,19	R$ 57.310,40
Avant		C	Exequível	160	R$ 445,94	R$ 71.350,40
Solo Network		C	Exequível	160	R$ 411,26	R$ 65.801,60
		C		0		R$ 0,00
	-	C		1		R$ 0,00
	-	C		1		R$ 0,00
	-	C		1		R$ 0,00
MENOR PREÇO/FORNECEDOR					**R$ 57.310,40**	**#N/D**

VALOR TOTAL R$57.310,40 (Cinquenta e sete mil, trezentos e dez reais com quarenta centavos).

Eu, Rafael Sanches Alencar, declaro que efetuei a pesquisa de preços, na forma dos incisos I do artigo 23° da Lei n° 14.133/2021, em conformidade com o Ato da Presidência nº 136/2023 e que os preços aqui apresentados condizem com os praticados no mercado.

Proc. Administrativo 8- 279/2024

De: Rodrigo N. - CMFI-DG-DIRTEC-EATI

Para: CMFI-PRESID-DG-DIRFIN-COM-EC - Equipe Compras - A/C CARLOS K.

Data: 07/08/2024 às 13:02:27

Segue as propostas apresentadas e o relatorio da pesquisa de preço assinado.

–

Rodrigo Nishimori
Administrador de Rede

Anexos:

Modelo_Pesquisa_de_Mercado_Media.xlsx
Proposta_CAMARA_MUNICIPAL_DE_FOZ_DO_IGUACU.pdf
Proposta_Camara_Renovacao_Kaspersky_V4_Optimus_Data.pdf
RELATORIA_PESQUISA_DE_PRECOS_Assinado.pdf
Solo_Network_Proposta_P24_570597A_Kaspersky.pdf

Proposta Comercial
Data: 12/07/2024
Validade: 12/08/2024

DADOS DO CONSULTOR
Responsável: Bianca Rosa
Email: bianca.rosa@avantservices.com.br

DADOS DO CLIENTE
Razão Social: CAMARA MUNICIPAL DE FOZ DO IGUACU
CNPJ de Faturamento: 75.914.051/0001-28
Contato: Rafael Sanches
Email: sanches@fozdoiguacu.pr.leg.br

Part Number	Descrição do Produto	Qtd	Valor Unitário	Valor Total
KL4066KASTJ	Kaspersky Endpoint Next EDR Optimum Brazilian Edition. 150-249 User 3 years Renew License	160	R$ 445,94	R$ 71.350,40
			Total da Proposta	R$ 71.350,40

Formas de Pagamento

( ) 1x Duplicata - 30 Dias

Informações Importantes
Valores em reais;
Proposta sujeita à aprovação de crédito;
Prazo de entrega em até 5 dias úteis;
Passa a contar após aprovação do cadastro e/ou confirmação do depósito;
Suporte nível 1 Incluso em toda vigência do contrato;
Para aceitar as condições dessa Proposta Comercial assine abaixo e preencha os dados;
Faturado por: **Avant Services - CNPJ 29.140.121/0001-10**

_____
Responsável:
Função:

PROPOSTA COMERCIAL

Projeto: Prestação de serviços especializados em proteção de ativos de TI

Gerente de Contas:	Claudinei Gonçalves – claudinei.goncalves@optimusdata.com.br
Nº. da proposta:	Proposta Nº 0052024_V2

OPTIMUS DATA TECHNOLOGY LTDA
RUA ELBA, 1083 – IPIRANGA
SÃO PAULO – SP – CEP 04285-001
FONE: +55 11 9 8185-5447
www.optimusdata.com.br

À
Câmara Municipal de Foz do Iguaçu

Prezados

Em resposta ao pedido de V.Sa., encaminhamos a seguir nossa proposta de fornecimento de Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License.

Agradecemos a oportunidade de apresentar nossa proposta à vossa empresa. Nossa filosofia é fundamentada no trabalho em conjunto, buscando prestar um serviço com qualidade, rapidez e baixos custos com foco principal na superação das expectativas de nossos clientes.

Estamos à disposição para quaisquer esclarecimentos adicionais que se fizerem necessários.

Sem mais

Atenciosamente

Claudinei Gonçalves
Diretor Comercial
Optimus Data

OPTIMUS DATA TECHNOLOGY LTDA
RUA ELBA, 1083 – IPIRANGA
SÃO PAULO – SP – CEP 04285-001
FONE: +55 11 9 8185-5447
www.optimusdata.com.br

PROPOSTA COMERCIAL

Apresentamos os preços correspondentes ao fornecimento de licenças de Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License.

1. Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License.

Kaspersky Next EDR Optimum combina EDR simplificado com uma proteção poderosa para endpoints, oferecendo às empresas em crescimento uma defesa direta e robusta contra uma ampla gama de ameaças. Suas funcionalidades incluem:

- Proteção de endpoint: proteção para arquivos, web e anti-virus de email, proteção de rede, AMSI, proteção contra exploit, remediação, behavior detection, HIPS.
- Gerenciamento de segurança: firewall, web, dispositivos, controle de aplicativos e cloud discovery.
- Proteção e gerenciamento móvel: Proteção, controle e gerenciamento de dispositivos móveis.
- Cenários de TI: Avaliação de vulnerabilidade, patch management, limpeza de dados, inventário de software e hardware, 3rd party apps e instalação de sistemas operacionais, conexão remota.
- Criptografia: Gerenciamento de criptografia e descriptografia.
- Cloud protection: Cloud discovery, segurança para MS365, data discovery.
- Educação: Treinamento de cibersegurança para administradores de TI.
- Capacidades essenciais de EDR: Análise de causa raiz, IOC scan, resposta de endpoint.

SUPORTE PADRÃO

O Suporte Técnico/Atendimento ao Cliente Kaspersky se esforça ao máximo para fornecer suporte de qualidade em tempo adequado, dependendo na natureza da solicitação. A obrigação de atender em um prazo fixo de tempo só pode ser oferecida como parte de serviços pagos.
Para alguns tipos de Software, os termos e condições de Suporte podem diferir dos termos e condições padrão. Os Termos e Condições estão disponíveis aqui.

1. O Suporte Padrão inclui o seguinte:

1.1. Processamento de solicitações relacionadas ao mau funcionamento do software e atualizações regulares de banco de dados
1.2. Processamento de solicitações relacionadas a malware:
Falsos positivos do software
Malware não detectado
Recomendações de desinfecção de computadores infectados por malware
1.3. Assistência com informações de recuperação de uma licença perdida ou danificada (se possível)
1.4. Consultas sobre as dúvidas a seguir:
Como e onde baixar o Software
Onde encontrar informações sobre o Software. Por exemplo, guias de usuários e material de treinamento.
Como usar serviços online: My Kaspersky ou CompanyAccount

2. O Suporte Padrão não inclui o seguinte:
2.1. Desenvolvimento de novas funcionalidades do Software a pedido de um Usuário
2.2. Aprimoramento do desempenho e configuração do dispositivo do Usuário
2.3. Desinfecção de computadores infectados por um malware (incluindo a mitigação dos efeitos de tais infecções) pelos especialistas do Suporte Técnico/Atendimento ao Cliente
2.4. Descrição do malware
2.5. Sessões de suporte remoto e no local (podem ser compradas como um serviço adicional nos Serviços Profissionais da Kaspersky)
2.6. Assistência ao usuário por telefone ou bate papos na Web enquanto coleta dados para análise e/ou aplicação de recomendações
2.7. Questões sobre aplicativos e/ou sistemas operacionais de terceiros
2.8. Uso de patches de terceiros em sistemas operacionais e aplicativos para corrigir vulnerabilidades
2.9. Integração de software da Kaspersky com software de terceiros
2.10. Configuração e verificação de desempenho de software por especialistas do Suporte Técnico/Atendimento ao Cliente e recomendação sobre configuração de segurança de rede (pode ser comprados como um serviço adicional nos Serviços Profissionais da Kaspersky)
2.11. Treinamento de software
2.12. Demonstração, implantação e configuração de software (podem ser compradas como um serviço adicional no Kaspersky Professional Services)
2.13. Análise e provisão de opinião oficial sobre causas de erro técnico
2.14. Análise e investigação sobre causas de incidentes resultantes em infecção por malware (podem ser compradas como um serviço adicional no Kaspersky Incident Response)

3. A Kaspersky não fornece Suporte nos seguintes casos:

3.1. O software específico de um hardware e/ou plataforma não atende aos requisitos mínimos de sistema do Software.
3.2. A versão do software não é mais compatível (a renovação do suporte pode ser comprada mediante solicitação)

4. A Kaspersky não garante instalação bem-sucedida, estabilidade da operação do Software, bem como resolução de problemas nos seguintes casos:
   1. A instalação é realizada em um dispositivo infectado.
   2. O Software Kaspersky está instalado em um ambiente misto, juntamente com outras aplicações incompatíveis.
   3. As interrupções do Software são causadas por problemas no hardware.
   4. As interrupções no Software são causadas por versões incompatíveis do software específico da plataforma.
   5. O Usuário não consegue ou se recusa a fornecer ao Suporte Técnico/Atendimento ao Cliente Kaspersky as informações necessárias para reprodução, análise e reparo do problema específico.
   6. O problema surgiu devido ao uso incorreto ou não consideração às instruções fornecidas pelo Suporte Técnico/Atendimento ao Cliente Kaspersky ou pela documentação da Kaspersky.
5. A Kaspersky fornece Suporte mediante as seguintes condições:
   Todo Software comercial e freemium para uso doméstico e dispositivos móveis é suportado, independentemente do status da Licença.
   É necessária uma Licença válida para suporte de todos os tipos de Software comerciais para pequenas, médias e grandes empresas.

Alguns serviços não incluídos no Suporte Padrão podem ser oferecidos como parte dos serviços pagos.

PREÇOS E CONDIÇÕES COMERCIAIS

A tabela a seguir mostra o produto e o valor.

ITEM	QTD	VL UNITÁRIO	VALOR
1 - Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License.	160	R$ 358,19	R$ 57.310,40
Valor total para o projeto			R$ 57.310,40

OPTIMUS DATA TECHNOLOGY LTDA
RUA ELBA, 1083 – IPIRANGA
SÃO PAULO – SP – CEP 04285-001
FONE: +55 11 9 8185-5447
www.optimusdata.com.br

CONDIÇÕES GERAIS

- Todos os valores já incluem os impostos.
- pagamento deverá ser efetuado no prazo de 15 (quinze) dias corridos, após a entrega da respectiva Nota Fiscal.
- O não pagamento dos valores devidos até a data de vencimento, acarretará multa de 2% e juros de mora de 1% ao mês, calculados pro-rata-die.

FORMALIZAÇÃO

Prazo de Validade: Esta proposta é válida por um período de 30 dias a partir da data de emissão. Após esse período, está sujeita a revisão e ajustes.

Confidencialidade: Ambas as partes concordam em manter todas as informações confidenciais obtidas durante a execução deste projeto. Essas informações não devem ser divulgadas a terceiros sem o consentimento prévio por escrito da outra parte.

São Paulo, 03 de julho de 2024

03/07/2024

X Claudinei Gonçalves da Silva

Claudinei Gonçalves da Silva
Sócio Diretor
Assinado por: CLAUDINEI GONCALVES DA SILVA:08814206899

Optimus Data Technology

OPTIMUS DATA TECHNOLOGY LTDA
RUA ELBA, 1083 – IPIRANGA
SÃO PAULO – SP – CEP 04285-001
FONE: +55 11 9 8185-5447
www.optimusdata.com.br

RELATÓRIO DE PESQUISA DE PREÇOS, PLANILHA COMPARATIVA E DOCUMENTAÇÃO COMPROBATÓRIA

INTRODUÇÃO

O presente relatório é resultado da pesquisa de preços abaixo discriminada em cumprimento ao determinado na Lei nº 14.133/2021 em conformidade com o Ato da Presidência nº 136/2023.

AGENTE RESPONSÁVEL PELA PESQUISA: Rafael Sanches Alencar

OBJETO: Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses

MÉTODO ESTATÍSTICO APLICADO COM JUSTIFICATIVAS PARA A METODOLOGIA UTILIZADA, EM ESPECIAL PARA A DESCONSIDERAÇÃO DE VALORES INCONSISTENTES, INEXEQUÍVEIS OU EXCESSIVAMENTE ELEVADOS, SE APLICÁVEL: Os valores foram com base em orçamentos obtidos em mercado, no qual se optou pelo menor preço, a fim de satisfazer as demandas desta casa de leis.

CARACTERIZAÇÃO DAS FONTES DE PESQUISA CONSULTADAS: Foram realizadas pesquisas de preços utilizando-se dos seguintes parâmetros estabelecidos no Ato da Presidência nº 136/2023, no qual Art. 6º

> *"A pesquisa de preços para fins de determinação do preço estimado* na contratação direta para a aquisição de bens e contratação de serviços em geral, consolidada em mapa comparativo, terá prazo de validade de 6 (seis) meses e será realizada mediante a utilização dos seguintes parâmetros, **de forma combinada ou não"**.

No qual foi utilizada IV – pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos orçamentos com mais de 6 (seis) meses de antecedência da data da pesquisa de preço;

JUSTIFICATIVA DAS FONTES CONSULTADAS: Considerando que o desenvolvedor da solução, possui uma rede de empresas autorizadas,

consultou-se as mesmas visando obtenção de propostas, por meio eletrônico de, no mínimo, 3 (três) fornecedores.

PERÍODO DE REALIZAÇÃO DA PESQUISA DE PREÇOS: Junho de 2024.

Abaixo relatório detalhado identificando cada um dos itens e seus valores obtidos:

PESQUISA DE MERCADO						
LOTE I - ITEM 1 - Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License						
FORNECEDOR	**MARCA**	**C/D**	**ART. 7º §4º**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL**
OPTIMUS DATA TECHNOLOGY LTDA		C	Exequível	160	R$ 358,19	R$ 57.310,40
Avant		C	Exequível	160	R$ 445,94	R$ 71.350,40
Solo Network		C	Exequível	160	R$ 411,26	R$ 65.801,60
		C		0		R$ 0,00
	-	C		1		R$ 0,00
	-	C		1		R$ 0,00
	-	C		1		R$ 0,00
MENOR PREÇO/FORNECEDOR					**R$ 57.310,40**	**#N/D**

VALOR TOTAL R$57.310,40 (Cinquenta e sete mil, trezentos e dez reais com quarenta centavos).

Eu, Rafael Sanches Alencar, declaro que efetuei a pesquisa de preços, na forma dos incisos I do artigo 23° da Lei n° 14.133/2021, em conformidade com o Ato da Presidência nº 136/2023 e que os preços aqui apresentados condizem com os praticados no mercado.

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: 1B82-B3AF-CB66-C7E4

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

RAFAEL SANCHES ALENCAR (CPF 006.XXX.XXX-96) em 07/08/2024 12:56:15 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://fozdoiguacu.1doc.com.br/verificacao/1B82-B3AF-CB66-C7E4

SOLUÇÕES QUE VALORIZAM
E IMPULSIONAM SEU NEGÓCIO

P24-570597A

PROPOSTA COMERCIAL
Data: 12/07/2024
Validade: 19/07/2024
Moeda: Real

Camara Municipal De Foz Do Iguacu
75.914.051/0001-28
Rodrigo Nishumori
99 9999-9999
sanches@fozdoiguacu.pr.leg.br; rodrigo@fozdoiguacu.pr.leg.br

Rafael Felix Hahn Lehmkuhl
(41) 3051-7519
rafael.felix@solonetwork.com.br

ID	Produto/Serviço	Qtde	Preço Unidade	Preço Total
1.1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental License PN: KL4066KASTC FABRICANTE: Kaspersky ENTREGA: 5 dias úteis GARANTIA	160	411.26	65,801.60

Total Proposta (R$) 65,801,60

Detalhes Técnicos Itens

1.1 KL4066KASTC - Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental License

Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental License

CONDIÇÕES DE TRANSPORTE/ENTREGA

Entrega Eletrônica (Via E-Mail).

CONDIÇÕES DE PAGAMENTO/FATURAMENTO

Pagamento através de depósito bancário, prazo de 30 dias. Sujeito à identificação de crédito.
Solo Network Brasil SA.
CNPJ: 00.258.246/0001-68
IE: 90586791-16
Banco Itaú: 341 Agência: 1568 CC: 20.222-8
Banco do Brasil: 001 Agência: 1622-5 CC: 114.557-6

CONDIÇÕES COMERCIAIS

Validade Preços
Os preços constantes nesta proposta são válidos para as quantidades apresentadas neste documento e dentro da validade do mesmo. Havendo diminuição de quantidades ou vencimento da validade, nova proposta com novos valores deverá ser gerada.

Condições de Faturamento
Os preços e condições comerciais apresentados observam a política econômica vigente nesta data. Qualquer mudança nesta política, que implique em alteração real do valor ofertado, face ao prazo de validade, condições de pagamento ou cláusula de reajuste, permitirá que a oferta seja revista e adaptada a fim de manter seu equilíbrio econômico financeiro original.

Impostos
Os impostos vigentes na data da emissão da proposta (IPI, ISS, ICMS e PIS/Cofins) estão inclusos em nossos preços. Nos casos de faturamento direto para clientes contribuintes do ICMS nos estados assinantes de convênios de substituição tributária e para clientes não contribuintes ou isentos, a venda pode estar sujeita a encargos adicionais (substituição tributária - ST e/ou diferencial de alíquotas). Os mesmos deverão ser pagos pelo cliente e serão informados após o aceite. Caso o pagamento não ocorra, o produto poderá ficar retido no Posto Fiscal da Secretaria de Fazenda Estadual (SEFAZ) do estado destino. Caso haja alteração na legislação atual, que afetem nossos preços na ocasião do faturamento, os mesmos poderão ser revistos de modo a refletir estas mudanças.
Prazo de Validade
Prazo de validade descrito no cabeçalho da proposta ou enquanto durarem os estoques.

Prazo De Entrega
Prazo de entrega especificado para cada item na proposta.

Garantia Hardwares
Prazo de garantia especificado para cada item na proposta. A garantia cobrirá falhas de materiais e defeitos de fabricação. A responsabilidade por defeitos não abrange danos causados pelo comprador, por acidentes em decorrência de operação indevida ou negligente, manutenção ou armazenagem inadequadas, operação anormal ou em desacordo com as especificações, obras civis mal acabadas, má qualidade das bases em que se assentam, influências de natureza química, eletro-química, elétrica, climática ou atmosférica, tais como: enchentes, inundações,descargas elétricas e raios, incêndio, terremoto, sabotagem, vandalismo e outros casos fortuitos ou de força maior previstos na legislação. Neste caso todo e qualquer material e mão de obra utilizados na reparação dos danos oriundos serão cobrados de acordo com os preços vigentes na oportunidade. O prazo para reparo de equipamentos pode variar de 5 a 60 dias e a Solo Network não efetua substituição de equipamentos em conserto, nem pode ser responsabilizada por qualquer despesa adicional, danos indiretos ou lucros cessantes.

Trocas e devoluções só serão aceitas com a embalagem original e em perfeitas condições, de acordo com as regras do Código de Defesa do Consumidor.
É recomendado que o equipamento e a Nota fiscal sejam conferidos no momento do recebimento para evitar transtornos em casos de necessidades de devoluções.

Garantia Softwares
A garantia sobre programas de computador abrange tão somente a existência de defeitos de fabricação na mídia entregue ao cliente, de acordo com o Termo de Garantia emitido pelo fabricante do produto e que com ele segue anexo.

Privacidade de dados

Cláusula A: A Solo Network está de acordo a Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, (`LGPD_).
Cláusula B: O CLIENTE ou CONTRATANTE, para efeitos da LGPD, é o Titular dos dados, pessoa natural a quem se referem os dados pessoais.
Cláusula C: O CONTRATADO, para efeitos da LGPD, é o Controlador, pessoa jurídica que decide quanto ao tratamento dos dados do titular.
Cláusula D: Os Dados Pessoais do CLIENTE ou CONTRATANTE, para efeitos da LGPD, são informações relacionadas a pessoa natural identificável, que neste documento é identificada
Cláusula F: O CONTRATADO, nos termos da LGPD, realizará o tratamento ou todo o manuseio dos dados pessoais do CLIENTE ou CONTRATANTE, envolvendo desde a coleta, até o seu armazenamento, sua transmissão, entre outros, como descrito no inciso X, do art. 5º da Lei.
Cláusula G: O tratamento dos dados pessoais tem a finalidade legítima de cumprir as obrigações contratuais e para o exercício regular de direitos em processo judicial, administrativo ou arbitral do CLIENTE ou CONTRATANTE, com a adequação do tratamento à finalidade e transparência de informações aos titulares.
Cláusula H: Os dados pessoais do CLIENTE ou CONTRATANTE, ficam armazenados no Centro de Dados, localizado em território nacional no endereço do CONTRATADO.
Cláusula I: O CONTRATADO, garante ao CLIENTE ou CONTRATANTE, o cumprimento dos direitos do titular, descritos no CAPÍTULO III da LGPD, desde que não violem o cumprimento de obrigação legal por parte do CONTRATADO.
Cláusula J: O CONTRATADO, adotará os controles e medidas de Segurança da Informação e Governança de acordo com as Boas Práticas de Mercado, no tratamento dos dados pessoais do titular dos dados.
Cláusula L: O CLIENTE ou CONTRATANTE autoriza ou consente o CONTRATADO a coletar os dados pessoais, por meio físico e ou digital, necessários para o cumprimento das obrigações contratuais e para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

`Para clientes do Setor Público:
A empresa Solo Network Brasil S.A., declara que é empresa revendedora autorizada Microsoft caracterizada como License Solution Partner (LSP), estando apta a operacionalizar por sua matriz e/ou suas filiais legalmente constituídas acordos Microsoft Select, Select Plus, Academic Select Plus, GGWA for Large Organizations, Enterprise Agreements (EA, EAS e SCE), Government Select, Enrollment for Education Solutions (EES), Microsoft Products and Services Agreements (MPSA) e GIA (Government Integrator Agreement). Sendo também reconhecida como integrante dos seguintes programas: Government Program Partner (GPP), Microsoft Authorized Education Partner (AEP), e Microsoft Cloud Solution Provider (CSP).
Validação através do link de acesso público: <https://partner.microsoft.com/pt-br/licensing/parceiros%20lsp>
Razão pela qual a presente proposta foi redigida de acordo com a terminologia e condições da fabricante Microsoft, respeitando e acatando suas determinações, que poderão ser consultadas através do link: <https://solonetwork.com.br/Microsoft/Apendice-A.pdf> _

Exclusões
Estão exclusos desta proposta: instalação física, instalação lógica, migração de dados, treinamento, orientações aos usuários finais ou qualquer outro serviço aplicado aos equipamentos ou softwares propostos, tratando-se, portanto de uma proposta exclusiva de fornecimento de equipamentos ou softwares. O suporte nestes casos é dado pelo próprio fabricante do equipamento ou software. Caso suporte da Solo Network seja necessário ou desejado, solicite nova proposta, com adição de serviços de suporte e seus custos adicionais.

TERMO DE ACEITE

Para aprovação desta proposta preencher **esta folha e subsequentes.**

O preenchimento pode ser feito de maneira digital, incluindo assinatura, ou então através de cópia escaneada (neste caso além da assinatura inclua também o carimbo de sua empresa). Não esqueça de preencher os dados de sua empresa para faturamento e entrega, itens escolhidos dentre aqueles constantes na proposta, quantidades, valores e totais, condições de pagamento e data. Anexe qualquer outra documentação solicitada e envie tudo por e-mail para seu consultor Solo Network.

A entrega dos produtos poderá ser realizada através de faturamento direto do distribuidor do fabricante, podendo ainda ser realizado parcialmente e através de mais de um distribuidor. Atente para o e-mail informado para recebimento da Nota Fiscal Eletrônica e verifique também no lixo eletrônico, pois eventualmente, o arquivo .xml pode ser direcionado para esta pasta. Os boletos são enviados via correios ou anexados ao e-mail, juntamente com a nota fiscal. Caso não os receba, entre em contato imediatamente conosco para que possamos encaminhar uma segunda via. O não recebimento dos mesmos não desobriga o pagamento e pagamentos em atraso incorrem em multa e juros. Prorrogações de títulos só são aceitas em caso de atraso na entrega do produto. Dúvidas, contate-nos pelo **nfe@solonetwork.com.br.**

Entendemos que o aceite dessa proposta comercial será assinado por um representante legal com plenos poderes para assumir aqui as obrigações estabelecidas.

Se você tem dúvidas em como assinar um pdf digitalmente, acesse o link
https://solonetwork.com.br/downloads/Solo-Network-Assinando-um-documento-digitalmente.pdf

OK	ID	PN	Produto/Serviço	Qtde	Preço Unidade	Preço Total
4	1.1	KL4066KASTC	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental License			
Total Aceito						
Condições de Pagamento						
Observações						

Dados Faturamento

Razão Social/Nome			
CNPJ/CPF		IE/RG	
Endereço			
Bairro		Cidade/Estado	
CEP		País	
Contato Principal		Cargo Contato	
Telefone Contato			
E-mail Contato			
E-mail NFE			
E-mail Licenças			

Dados Fiscais

Regime Tributário	☐ Lucro Real	☐ Lucro Presumido	☐ Simples Nacional	☐ Produtor Rural
ICMS	☐ Contribuinte	☐ Não Contribuinte		
Natureza	☐ Orgão Público Federal	☐ Orgão Público Estadual/Municipal	☐ PJ Direito Privado	
	☐ Outros.Especificar:			
Retenção Fonte	☐ PIS - 0,65%	☐ COFINS - 3,0%	☐ CSLL - 1,0%	
	☐ INSS - 11,0%	☐ IR - 1,5%	☐ IR - 1,2% ou 4,8%	☐ Nenhum
Regime Especial	☐ Não Possui	☐ Possui Regime Especial Retenção. Especificar Abaixo:		

Referências Bancárias

Banco(1)		Banco(2)	
Gerente(1)		Gerente(2)	
E-mail(1)		E-mail(2)	
Telefone(1)		Telefone(2)	
Agência(1)		Agência(2)	
Conta(1)		Conta(2)	

Local/Data	Nome/Assinatura/Carimbo

Proc. Administrativo 9- 279/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: CMFI-PRESID-DG-DIRFIN-COM - Chefia Compras

Data: 07/08/2024 às 14:03:19

Encaminha-se.

–

Rafael Sanches
Diretoria de Tecnologia

Proc. Administrativo 10- 279/2024

De: CARLOS K. - CMFI-PRESID-DG-DIRFIN-COM

Para: CMFI-PRESID-DG-DIRFIN-GESTCON - Gestão de Contratos Administrativos

Data: 09/08/2024 às 11:29:10

Ao senhor gestor de contratos para indicação da minuta do instrumento de contrato a ser utilizado.

–

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras

Proc. Administrativo 11- 279/2024

De: José T. - CMFI-PRESID-DG-DIRFIN-GESTCON

Para: AGCONT - Agente de contratação

Data: 26/08/2024 às 13:20:06

Prezados, com a Minuta de Contrato a ser firmada em anexo, encaminho para os devidos fins.

Att.

_

José Marcelo Nicoletti Teixeira,
Consultor Técnico Legislativo.

Anexos:

Minuta_Contrato_XX_2024_antivirus.pdf

M I N U T A

CONTRATO Nº XX/2024

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS, QUE FAZEM ENTRE SI A CÂMARA MUNICIPAL DE FOZ DO IGUAÇU E A EMPRESA XXXXXXXXXXXXXXXXXX.

A **Câmara Municipal de Foz do Iguaçu**, pessoa jurídica de direito público, com sede em Foz do Iguaçu, Estado do Paraná, situada na Travessa Oscar Muxfeldt, 81, Centro, inscrita no CNPJ/MF sob o nº 75.914.051/0001-28, neste ato representada por seu Presidente, João José Arce Rodrigues, consoante competência originária prevista no art. 17 do Regimento Interno da Câmara Municipal de Foz do Iguaçu, daqui para frente denominada simplesmente de **CONTRATANTE,** e, de outro lado, a empresa XXXXXXXXXXXXXXXXXXXXXX, inscrita no CNPJ/MF sob o nº XXXXXXXXX/XXXX-XX, situado na XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, cidade de XXXXXXXXXX, Estado XXXXXXXXX, CEP: XX.XXX-XXX, representada por seu representante legal XXXXXXXXXXXXXXXXXXXX, inscrito junto ao CPF/MF sob n. XXXXXXXXXX, a seguir denominada simplesmente **CONTRATADA**, firmam o presente contrato, sujeitando-se às cláusulas a seguir expostas e às normas da Lei n. 14.133/2021, têm entre si justo e contratado o que segue:

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O objeto do presente contratação de empresa especializada e tecnicamente qualificada para o fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 meses, de acordo com as características e especificações técnicas e, quantitativos descritos em termo de referência, bem como em seus anexos, conforme descrição a seguir:

ITEM	CAT/MAT	DESCRIÇÃO	QUANT.	UNIDADE	VALOR UNIT.	VALOR TOTAL
1	350949	KASPERSKY NEXT EDR OPTIMUM	160	Uni	R$ XXXXX,XX	R$ XXXXXX,XX
TOTAL						R$ XXXXXX,XX

2. CLÁUSULA SEGUNDA – DA VINCULAÇÃO

2.1. Os Contraentes reconhecem a vinculação desta contratação aos termos do Pregão Eletrônico n. XX/XXXX, emitido pela CONTRATANTE e à respectiva proposta que for vencedora, sendo que as

especificações técnicas mínimas do objeto, a fundamentação da contratação, a descrição da solução como um todo, as condições da garantia, os requisitos de habilitação, qualificação, técnica e capacidade operacional e de fornecimento, os requisitos da contratação, dentre outras informações, estão constantes em Termo de Referência, que é parte integrante deste Contrato independentemente de sua transcrição, ao qual também se declaram vinculados os contraentes.

3. CLÁUSULA TERCEIRA – DA LEGISLAÇÃO APLICÁVEL E DOS CASOS OMISSOS

3.1. Aplica-se a Lei n. 14.133/2021 à execução deste Contrato, sendo esta também a legislação a ser aplicadas aos casos omissos.

4. CLÁUSULA QUARTA – DO REGIME DE EXECUÇÃO

4.1. Os serviços serão executados sob o regime de execução indireta.

4.2. A execução dos serviços especificados neste Contrato e em Termo de Referência deverá ter início em até 30 dias, contados da assinatura do contrato, mediante fornecimento das licenças registradas em nome da CÂMARA MUNICIPAL DE FOZ DO IGUAÇU, nome fantasia PODER LEGISLATIVO, CNPJ n. 75.914.051/0001-28, atreladas a conta suporte@fozdoiguacu.pr.leg.br, dentro da plataforma da desenvolvedora Karpersky Global.

4.2. Quando realizada a disponibilização da licença, notificar via e-mail os responsáveis técnicos, sanches@fozdoiguacu.pr.leg.br e rodrigo@fozdoiguacu.pr.leg.br com detalhes do acesso.

4.3. Os serviços de instalação e manutenção deverão ser realizados na sede administrativa da CONTRATANTE, no endereço Travessa Oscar Muxfeldt, 81 - Centro, Foz do Iguaçu - PR, 85851-490

4.4. Os serviços a serem contratados constituem-se em atividades materiais acessórias, instrumentais ou complementares à área de competência legal da CONTRATANTE, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

4.5. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e a Administração, vedando-se qualquer relação entre elas que caracterize pessoalidade e subordinação direta.

4.6. Os serviços contratados são enquadrados como continuados, tendo em vista a sua necessidade permanente para a CONTRATANTE.

5. CLÁUSULA QUINTA – PREÇO

5.1. Em contra partida aos serviços prestados a CONTRATANTE pagará à CONTRATADA o valor mensal de até R$ XXXXX, totalizando estimativa de pagamento anual de até R$ XXXXX, conforme descrito na proposta apresentada pela empresa e constante no processo administrativo.

5.2. No valor indicado estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, seguro e outros necessários ao cumprimento integral do objeto da contratação.

6. CLÁUSULA SEXTA – DO REAJUSTE

6.1. Mediante expresso pedido da CONTRATADA, os valores contratados poderão ser reajustados a cada 12 (doze) meses, contados a partir da data da proposta apresentada pela CONTRATADA, com aplicação do índice de variação do IPCA para o mesmo período ou outro índice que o substitua.
6.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de 12 (doze) meses para a próxima reajustamento, será contado a partir dos efeitos financeiros do último reajuste.
6.3. O reajuste previsto nesta cláusula poderá ser formalizado por Termo de Apostilamento.

7. CLÁUSULA SÉTIMA – DOS CRITÉRIOS DE MEDIÇÃO
7.1. Os Materiais entreguem dever estar em conformidade com as quantidades solicitadas dos itens já descritos neste documento;
7.2. A qualidade exigida dos equipamentos e materiais utilizados tem que estar de acordo com a qualidade de cada item, sendo vedada a utilização de materiais de qualidade inferior ou de não garantia.
7.3. Todos os pontos instalados devem ser certificados para assim constatar a qualidade do serviço e garantia de transmissão do mesmo.
7.4. Dos demais todos os itens devem ser novos seguidos rigidamente as especificações mínimas descritas na seção Requisitos da Contratação e amparados em seu prazo de garantia estabelecidos.

8. CLÁUSULA OITAVA – DO RECEBIMENTO
8.1. Os serviços serão recebidos provisoriamente no prazo de 05 (cinco) dias, para efeito de posterior verificação de sua conformidade com as especificações constantes na proposta;
8.2. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes na proposta, devendo ser substituídos no prazo de 10 (dez) dias, a contar da notificação da CONTRATANTE, às suas custas, sem prejuízo da aplicação das penalidades;
8.3. Na impossibilidade de realização dos serviços, a empresa vencedora deverá substituir o serviço por outro com especificações iguais ou superiores;
8.4. Os serviços serão recebidos definitivamente no prazo de 10 (dez) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação;
8.5. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo;
8.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

9. CLÁUSULA NONA – DO PAGAMENTO
9.1. Os pagamentos serão efetuados até o 10º (décimo) dia após o recebimento definitivo dos produtos/serviços, condicionado a apresentação da Nota Fiscal/Fatura, bem como os documentos de regularidade fiscal, social e trabalhista exigidos pelo art. 68 da Lei nº 14.133/2021.
9.2. Na eventualidade de ocorrer atraso no pagamento, o valor será atualizado pela variação acumulada do IPCA, ocorrida entre a data de seu adimplemento e a do efetivo pagamento, calculada pro rata tempore.
9.3. A apresentação da nota fiscal/fatura é indispensável a cada entrega de produtos ou prestação de

serviços, para fins de liquidação e pagamento da despesa, a ser emitida ao destinatário: Razão social: CÂMARA MUNICIPAL DE FOZ DO IGUACU; CNPJ: 75.914.051/0001-28; Endereço: Travessa Oscar Muxfeldt, nº 81, Centro, na cidade de Foz do Iguaçu-Paraná, CEP 85.851-490. Telefone: (45) 3521-8100.

9.4. Antes de cada pagamento à CONTRATADA, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

9.5. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se- á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

9.6. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

9.7. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

9.8. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua notificação, por escrito, para que, no prazo de 15 (quinze) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.

9.9. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.

9.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso a CONTRATADA não regularize sua situação junto ao SICAF.

9.11. O prazo desta contratação será de 36 meses, contados da assinatura do contrato.

10. CLÁUSULA DÉCIMA – DO PRAZO PARA RESPOSTA AOS PEDIDOS DE REPACTUAÇÃO DE PREÇOS E RESTABELECIMENTO DO EQUILÍBRIO ECONÔMICO

10.1. Quando for o caso de repactuação de preços e/ou de restabelecimento do equilíbrio econômico deste Contrato, será de 30 dias úteis o prazo resposta da CONTRATANTE, a contar da data de formalização do pedido por parte da CONTRATADA.

11. CLÁUSULA DÉCIMA PRIMEIRA - DA INEXIGÊNCIA DE GARANTIAS À EXECUÇÃO DO CONTRATO

11.1. Dadas as características da contratação, não haverá exigência de garantia à execução do contrato.

12. CLÁUSULA DÉCIMA SEGUNDA – DA GARANTIA DOS PRODUTOS E SERVIÇOS

12.1. As empresas licitantes deverão indicar o prazo da garantia do Software ou licença, que deverá ser de 36 meses oferecido diretamente ou com a autorização e responsabilidade do fabricante, sendo este o período em que se obrigam a prestar a manutenção e assistência técnica gratuita, nos termos regulados em termo de referência.
12.2. Serão desclassificadas as propostas que não ofereçam prazo de garantia ou abaixo do mínimo estipulado. As empresas licitantes indicarão, SOB PENA DE DESCLASSIFICAÇÃO, informações relacionadas à PADRONIZAÇÃO e COMPATIBILIDADE da solução, conforme detalhamento no ETP.

13. CLÁUSULA DÉCIMA TERCEIRA – DOTAÇÃO ORÇAMENTÁRIA
13.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da Câmara Municipal, para o exercício de 2024 nas classificações: item 1 – 01.01.01.031.0001.2002.3.3.90.40.99.05 – AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE.
13.2. Nos exercícios seguintes, correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

14. CLÁUSULA DÉCIMA QUARTA – DAS OBRIGAÇÕES DA CONTRATANTE
14.1. A CONTRATANTE obriga-se a:
14.1.1. Comunicar à Contratada quaisquer irregularidades nos equipamentos, para adoção das providências cabíveis;
14.1.2. Designar funcionário para acompanhar/fiscalizar a entrega;
14.1.3. Efetuar os pagamentos relativos ao presente contrato em moeda corrente quando da apresentação da fatura de serviços executados respeitando os prazos de vencimentos;
14.1.4. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;
14.1.5. Qualquer alteração deste, somente deverá ser com o aval dos gestores do contrato;
14.1.6. Aplicar a contratada as sanções administrativas regulamentares e contratuais cabíveis.

15. CLÁUSULA DÉCIMA QUINTA – DAS OBRIGAÇÕES DA CONTRATADA
15.1. A CONTRATADA obriga-se a:
15.1.1. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;
15.1.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do contrato, inerentes à execução do objeto contratual;
15.1.3. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;
15.1.4. É de responsabilidade da CONTRATADA, manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

16. CLÁUSULA DÉCIMA SEXTA – DAS SANÇÕES ADMINISTRATIVAS

16.1. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei n° 14.133, de 2021, quais sejam:

16.1.1. Dar causa à inexecução parcial do contrato;

16.1.2. Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

16.1.3. Dar causa à inexecução total do contrato;

16.1.4. Deixar de entregar a documentação exigida para o certame;

16.1.5. Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

16.1.6. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

16.1.7. Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

16.1.8. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

16.1.9. Fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

16.1.10. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

16.1.11. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

16.1.12. Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;

16.1.13. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

16.1.13.1. Multa de até 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor;

16.1.15. Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, quando não se justificar a imposição de penalidade mais grave;

16.1.16. Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 16.1.8 e bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

16.2. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao fornecedor.

17. CLÁUSULA DÉCIMA SÉTIMA - DA OBRIGAÇÃO DE MANUTENÇÃO DAS CONDIÇÕES DE QUALIFICAÇÃO

17.1. A CONTRATADA obriga-se a manter, durante toda a execução do Contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições para a qualificação na contratação direta que precedeu a este instrumento;

18. CLÁUSULA DÉCIMA OITAVA - DA OBRIGAÇÃO DE RESERVA DE CARGOS PREVISTA EM LEI

18.1. A CONTRATADA, durante toda a execução do Contrato, obriga-se a cumprir as exigências de reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz.

19. CLÁUSULA DÉCIMA NONA – MODELO DE GESTÃO DO CONTRATO

19.1. A execução do objeto seguirá a seguinte dinâmica:

19.1.1. A contratante indicará Fiscal de contratos que irá acompanhar a execução do contrato em conformidade com este termo de referência.

19.1.2. O Contrato terá o prazo de 3 (três) anos, podendo ser prorrogado.

19.1.3. A Contratada formalizará a designação do preposto da empresa, especificando os poderes e responsabilidades relacionados à execução do objeto contratado.

19.1.4. Toda comunicação entre a Contratante e a Contratada deverá ser formalizada por escrito, especialmente quando exigido por lei, podendo ser realizada por meio de mensagem eletrônica, quando aplicável.

19.1.5. A execução será realizada de forma parcelada formalizada pelo envio da ordem de compra.

19.1.6. Os prazos e critérios para recebimento e pagamento estão detalhados nas cláusulas 7 a 9 retro.

19.1.7. Considera-se ocorrido o recebimento da nota fiscal quando a Gestão de contratos atestar a execução do objeto do contrato através do termo de recebimento definitivo.

19.1.8. Não haverá exigência de garantia contratual da execução, devido às características da contratação.

20. CLÁUSULA VIGÉSIMA – DA INEXECUÇÃO E DA EXTINÇÃO DO CONTRATO

20.1. A inexecução total ou parcial do contrato ensejará a sua extinção com as consequências contratuais e as previstas em lei, com fulcro no Título III, Capítulo VIII da Lei n. 14.133/2021, nos seguintes modos:

20.1.1. determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta;

20.1.2. consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração;

20.1.3. determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

20.2. Constituirão motivos para extinção do contrato, a qual deverá ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa, as seguintes situações:

20.2.1. não cumprimento ou cumprimento irregular de normas editalícias ou de cláusulas contratuais, de especificações, de projetos ou de prazos;

20.2.2. desatendimento das determinações regulares emitidas pela autoridade designada para acompanhar e fiscalizar sua execução ou por autoridade superior;

20.2.3. alteração social ou modificação da finalidade ou da estrutura da empresa que restrinja sua capacidade de concluir o contrato;

20.2.4. decretação de falência ou de insolvência civil, dissolução da sociedade ou falecimento do contratado;
20.2.5. caso fortuito ou força maior, regularmente comprovados, impeditivos da execução do contrato;
20.2.6. atraso na obtenção da licença ambiental, ou impossibilidade de obtê-la, ou alteração substancial do anteprojeto que dela resultar, ainda que obtida no prazo previsto;
20.2.7. atraso na liberação das áreas sujeitas a desapropriação, a desocupação ou a servidão administrativa, ou impossibilidade de liberação dessas áreas;
20.2.8. razões de interesse público, justificadas pela autoridade máxima do órgão ou da entidade CONTRATANTE.
20.3. O descumprimento, por parte da CONTRATADA, de suas obrigações legais e/ou contratuais assegurará ao CONTRATANTE o direito de extinguir o contrato a qualquer tempo, independentemente de aviso, interpelação judicial e/ou extrajudicial.
20.4. A extinção por ato unilateral do CONTRATANTE sujeitará a CONTRATADA à multa rescisória de até 10% (dez por cento) sobre o valor do saldo do contrato existente na data da extinção, independentemente de outras penalidades.
20.5. Caso o valor do prejuízo do CONTRATANTE advindo da extinção contratual por culpa da CONTRATADA exceder o valor da Cláusula Penal prevista no parágrafo anterior, esta valerá como mínimo de indenização, na forma do disposto no art. 416, parágrafo único, do Código Civil.
20.6. A extinção determinada por ato unilateral da Administração e a extinção consensual deverão ser precedidas de autorização escrita e fundamentada da autoridade competente e reduzidas a termo no respectivo processo.
20.7. A CONTRATANTE poderá rescindir o presente instrumento contratual, sem qualquer ônus à Administração, quando da conclusão de eventual novo procedimento de contratação de interesse público para objeto afim.

21. CLÁUSULA VIGÉSIMA PRIMEIRA – DA VIGÊNCIA
21.1. O presente Contrato terá validade de 36 (trinta e seis) meses, contados da data da assinatura, podendo ser prorrogado, a critério da Administração, conforme o disposto no art. 107, da Lei n. 14.133/2021 e suas alterações posteriores.
21.2. A prorrogação deste contrato deverá ser promovida mediante celebração de termo aditivo.

22. CLÁUSULA VIGÉSIMA SEGUNDA – DA FISCALIZAÇÃO
22.1. O acompanhamento e a fiscalização da execução das obrigações oriundas deste contrato ficarão a cargo do Gestor José Marceo Nicoletti Teixeira, e do Fiscal de Contratos, Jeverson Siqueira, e consiste na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da CONTRATANTE, especialmente designados, na forma do art. 117 da Lei nº 14.133/2021.
22.2. O fiscal do contrato deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 117 da Lei nº 14.133/2021.

22.3. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela CONTRATADA ensejará a aplicação de sanções administrativas, previstas neste Termo de Contrato e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 156 e 137 da Lei nº 14.133/2021.
22.4. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da CONTRATANTE ou de seus agentes e prepostos, de conformidade com art. 120 da Lei nº 14.133/2021.

23. CLÁUSULA VIGÉSIMA TERCEIRA – DA SUBCONTRATAÇÃO
23.1. É vedada a subcontratação total ou parcial do objeto deste Termo de Contrato.

24. CLÁUSULA VIGÉSIMA QUARTA – DAS VEDAÇÕES
24.1. É vedado à CONTRATADA:
24.1.1. Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;
24.1.2. Interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

25. CLÁUSULA VIGÉSIMA QUINTA – DAS ALTERAÇÕES
25.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos art. 124 a 136 da Lei n. 14.133/2021.

26. CLÁUSULA VIGÉSIMA SEXTA – DA PUBLICAÇÃO
26.1. A CONTRATANTE providenciará a publicação deste contrato no Diário Oficial do Município de Foz do Iguaçu, na página da Câmara Municipal de Foz do Iguaçu nos termos do art. 174 da Lei n. 14.133/2021 e no Portal Nacional de Contratações Públicas (PNCP), para fins de garantia a ampla publicidade.

27. CLÁUSULA VIGÉSIMA SÉTIMA – DO FORO
27.1. Fica eleito o foro desta cidade de Foz do Iguaçu, Estado do Paraná, para dirimir toda e qualquer questão que derivar deste contrato.

E por estarem justas e acordadas, assinam as partes o presente instrumento, na presença de duas testemunhas, que também o subscrevem, para que surtam todos os efeitos jurídicos e legais.

Foz do Iguaçu, xx de xxxxx de 2024.

CÂMARA MUNICIPAL DE FOZ DO IGUAÇU
João José Arce Morales

XXXXXXXXXXX
xxxxxxxxxxx

Testemunhas:

_____
Nome: XXXXXX
RG: XXXXXX
CPF: XXXXXXX

_____
Nome: XXXXXXXXX
RG: XXXXXXX
CPF XXXXXX

Proc. Administrativo 12- 279/2024

De: CARLOS K. - AGCONT

Para: Envolvidos internos acompanhando

Data: 05/09/2024 às 09:42:33

Trago aos autos a minuta do Edital, bem como a portaria de nomeação da equipe de pregão.

_

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras

Anexos:

0_MINUTA_EDITAL_PREGAO_0x_24.pdf
portaria_presidencia_038_2024_assinado_versaoImpressao_1.pdf

PREGÃO ELETRÔNICO

03/2024
(90003/2024 no sistema compras.gov.br)

CONTRATANTE (UASG)

Câmara Municipal de Foz do Iguaçu (926470)

OBJETO

Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

VALOR TOTAL DA CONTRATAÇÃO

R$ 57.310,40 (Cinquenta e sete mil, trezentos e dez reais e quarenta centavos).

DATA DA SESSÃO PÚBLICA

Dia **08/10/2024** às **10h (horário de Brasília)**

CRITÉRIO DE JULGAMENTO:

Menor preço por item.

MODO DE DISPUTA:

Aberto e fechado

PREFERÊNCIA ME/EPP/EQUIPARADAS

SIM

Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

Sumário

Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

CÂMARA MUNICIPAL DE FOZ DO IGUAÇU

PREGÃO ELETRÔNICO Nº 03/2024.

(Processo Administrativo 1DOC n°180/2024)

Torna-se público que a Câmara Municipal de Foz do Iguaçu, por meio do Setor de Compras, sediada na Travessa Oscar Muxfeldt, nº 81, Centro, Foz do Iguaçu – PR, realizará licitação, para registro de preços, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021, do Atos da Presidência nº 131/2023 e nº 134/2023 demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. O objeto da presente licitação é a Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

1.2. A licitação será realizada em item único.

ITEM	DESCRIÇÃO	BENEFÍCIO ME/EPP	QNT	VALOR UNITÁRIO	VALOR TOTAL
1	Licença KASPERSKY NEXT EDR OPTIMUM 36 meses	Tratamento favorecido	160	R$ 358,19	R$ 57.310,40

2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

2.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

2.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

2.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

2.5. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015, bem como para bens e serviços

produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010

2.6. Não poderão disputar esta licitação:

2.6.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

2.6.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

2.6.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

2.6.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.6.5. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

2.6.6. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

2.6.7. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.6.8. agente público do órgão ou entidade licitante;

2.6.9. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

2.6.10. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.

2.7. O impedimento de que trata o item 2.6.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.8. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.6.2 e 2.6.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

2.9. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

2.10. O disposto nos itens 2.6.2 e 2.6.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

2.11. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da

contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133/2021.

2.12. A vedação de que trata o item 2.6.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

3.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

3.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

3.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 7.1.1 e 7.11.1 deste Edital.

3.4. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

3.4.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

3.4.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

3.4.3. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

3.4.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

3.5. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

3.6. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

3.6.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

3.6.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

3.7. A falsidade da declaração de que trata os itens 3.4 ou 3.6 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

3.8. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

3.9. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

3.10. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

3.11. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

3.11.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

3.11.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

3.12. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

3.12.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

3.12.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.

3.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 3.11 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

3.14. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

3.15. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

4. DO PREENCHIMENTO DA PROPOSTA

4.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

4.1.1. Valor unitário e total do item;

4.1.2. Marca;

4.1.3. Fabricante;

4.1.4. Quantidade cotada, devendo respeitar o mínimo para cada item.

4.2. Todas as especificações do objeto contidas na proposta aceita pela Administração vinculam o licitante.

4.2.1. O licitante NÃO poderá oferecer proposta em quantitativo inferior ao previsto para a contratação.

4.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

4.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

4.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

4.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

4.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, quando devidamente aceita pela administração, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

4.7.1. O prazo de validade da proposta **não será inferior a 90 (noventa)** dias**,** a contar da data de sua apresentação, independentemente do prazo indicado no documento encaminhado.

4.7.2. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

4.8. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

5.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

5.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

5.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

5.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

5.5. O lance deverá ser ofertado pelo valor unitário do item

5.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

5.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

5.8. O intervalo mínimo de diferença de valores, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 1,00 (Um real).

5.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.10. O procedimento seguirá de acordo com o modo de disputa aberto e fechado.

5.11. Para o envio de lances no pregão eletrônico o modo de disputa "aberto e fechado", os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

5.11.1. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

5.11.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.11.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

5.11.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.11.5. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.12. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.13. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

5.14. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

5.15. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

5.16. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

5.17. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

5.18. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

5.18.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

5.18.2. A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

5.18.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

5.18.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

5.19. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

5.19.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

5.19.1.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

5.19.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

5.19.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

5.19.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

5.19.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

5.19.2.1. empresas estabelecidas no território do Estado do Paraná;

5.19.2.2. empresas brasileiras;

5.19.2.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

5.19.2.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

5.19.3. Se, mesmo após a aplicação dos procedimentos previstos nos itens acima, ainda persistir o empate, será realizado sorteio público para fins de desempate;

5.19.3.1. Será informado no chat da sessão pública, a data, hora e local do sorteio, a ser realizado no site sorteio.com (ou outro compatível), com transmissão ao vivo no Youtube ou outra plataforma de streaming;

5.19.3.2. Haverá lavratura de ata de sorteio, com presença de testemunhas, que será incluída no processo administrativo.

5.20. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro deverá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.20.1. Não será admitida a previsão de preços diferentes em razão de local de entrega ou de acondicionamento, tamanho de lote ou qualquer outro motivo.

5.20.2. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

5.20.3. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

5.20.4. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

5.20.5. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

5.20.6. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

5.21. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

6. DA FASE DE JULGAMENTO

6.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 2.5 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.1.1. SICAF;

6.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

6.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

6.1.4. Cadastro de restrições ao direito de contratar com a Administração Pública (https://crcap.tce.pr.gov.br/ConsultarImpedidos.aspx)

6.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

6.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

6.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

6.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação.

6.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

6.4. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

6.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com os itens 3.5.1 e 4.6 deste edital.

6.6. Verificadas as condições de participação, o pregoeiro examinará a proposta final ajustada, ofertada pela empresa classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 27 a 33 do Ato da Presidência nº 134/2023.

6.7. Será desclassificada a proposta vencedora que:

6.7.1. contiver vícios insanáveis;

6.7.2. não obedecer às especificações técnicas contidas no Termo de Referência;

6.7.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

6.7.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.7.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

6.8. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

6.8.1. A inexequibilidade, na hipótese de que trata o **caput**, só será considerada após diligência do pregoeiro, que comprove:

6.8.1.1. que o custo do licitante ultrapassa o valor da proposta; e

6.8.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.8.2. Será desclassificada a proposta que não tiver sua exequibilidade demonstrada, quando exigido pela Administração.

6.9. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

6.10. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante ou da área especializada no objeto.

7. DA FASE DE HABILITAÇÃO

7.1. Os documentos previstos neste item, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

7.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

7.2. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

7.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor

juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

7.4. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, por cópia ou original e cópia simples para autenticação pela Equipe de Pregão e posterior devolução.

7.5. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

7.6. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

7.7. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

7.8. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

7.9. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

7.9.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

7.10. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (IN nº 3/2018, art. 7º, *caput*).

7.10.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. (IN nº 3/2018, art. 7º, parágrafo único).

7.11. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

7.11.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de DUAS HORAS, prorrogável por igual período, contado da solicitação do pregoeiro.

7.12. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

7.12.1. Os documentos relativos à regularidade fiscal somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

7.13. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e Ato da Presidência nº 134/2023, art. 35, §4º):

7.13.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

7.13.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

7.14. Na análise dos documentos de habilitação, a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.15. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital.

7.16. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

7.17. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

7.18. Serão exigidos os seguintes documentos para a habilitação:

7.18.1. Habilitação jurídica nos termos do art. 66 da Lei nº 14.133/2021;

7.18.2. Prova da inexistência de fato impeditivo para licitar ou contratar com a Administração Pública, mediante a juntada de pesquisa realizada junto ao Tribunal de Contas da União e ao Tribunal de Contas do Estado do Paraná;

7.18.3. Habilitação fiscal, social e trabalhista, nos termos do Art. 68 da Lei nº 14-133/2021;

7.18.4. Habilitação econômico-financeira, mediante o fornecimento de Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante;

8. DOS RECURSOS

8.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

8.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

8.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

8.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

8.3.1.1. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

8.3.2. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

8.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

8.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

8.6. Os recursos interpostos fora do prazo não serão conhecidos.

8.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

8.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

8.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

8.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico https://www.fozdoiguacu.pr.leg.br/transparencia/licitacoes/2024/pregao-eletronico-003-2024/

9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

9.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

9.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

9.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

9.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

9.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

9.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

9.1.2.4. deixar de apresentar amostra;

9.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

9.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

9.1.3.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

9.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação

9.1.5. fraudar a licitação

9.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

9.1.6.1. agir em conluio ou em desconformidade com a lei;

9.1.6.2. induzir deliberadamente a erro no julgamento;

9.1.6.3. apresentar amostra falsificada ou deteriorada;

9.1.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

9.1.8. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

9.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

9.2.1. advertência;

9.2.2. multa;

9.2.3. impedimento de licitar e contratar e

9.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

9.3. Na aplicação das sanções serão considerados:

9.3.1. a natureza e a gravidade da infração cometida.

9.3.2. as peculiaridades do caso concreto

9.3.3. as circunstâncias agravantes ou atenuantes

9.3.4. os danos que dela provierem para a Administração Pública

9.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor da proposta, recolhida no prazo máximo de **15 (quinze) dias** úteis, a contar da comunicação oficial.

9.4.1. Para as infrações previstas nos itens 9.1.1, 9.1.2 e 9.1.3, a multa será de 5% do valor total da proposta.

9.4.2. Para as infrações previstas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, a multa será de 30% do valor total da proposta.

9.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

9.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

9.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 9.1.1, 9.1.2 e 9.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

9.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, bem como pelas infrações administrativas previstas nos itens 9.1.1, 9.1.2 e 9.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

9.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 9.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

9.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

9.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida,

que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

9.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

9.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

9.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

10.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

10.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

10.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, pelos *seguintes meios*: protocolo digital através do sistema 1doc através do link https://fozdoiguacu.1doc.com.br/b.php?pg=wp/wp&itd=12 ou envio através do email licitacao@fozdoiguacu.pr.leg.br.

10.4. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

10.4.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.

10.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

11. DAS DISPOSIÇÕES GERAIS

11.1. Será divulgada ata da sessão pública no sistema eletrônico.

11.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

11.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

11.4. A homologação do resultado desta licitação não implicará direito à contratação.

11.5. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

11.6. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

11.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

11.8. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

11.9. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

11.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico https://www.fozdoiguacu.pr.leg.br/transparencia/licitacoes/2024/pregao-eletronico-003-2024.

11.11. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

11.11.1. ANEXO I - Termo de Referência

11.11.2. ANEXO II – Estudo Técnico Preliminar

11.11.3. ANEXO III - Minuta de Termo de Contrato

11.11.4. ANEXO IV – Modelo da Proposta de Preços

JOÃO MORALES

PRESIDENTE DA CÂMARA MUNICIPAL DO IGUAÇU

TERMO DE REFERÊNCIA

1) DEFINIÇÃO DO OBJETO

Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

Item	CAT/MAT	Descrição	Prazo	SKU	Quantidade	Valor
1	350949	KASPERSKY NEXT EDR OPTIMUM 36 meses	36 meses	KL4066KASTJ	160	R$ 57.310,40

2) FUNDAMENTAÇÃO DA CONTRATAÇÃO

Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".
Considerando que esta casa de leis realiza a utilização da solução de segurança, sem ressalvas e visa proteger seu investimento, assegurar a padronização e compatibilidade com o ambiente computacional. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para, no mínimo, manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.
Com a iminente expiração da licença, torna-se necessária a renovação e aquisição para assegurar a proteção atualizada contra as ameaças virtuais mais recentes.
Sendo a demanda prevista no PAC, conforme documento de estudo técnico preliminar - ETP.

3) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução de segurança deve atender a necessidade de evolução e adequação desta casa em relação a suas ferramentas de proteção, esta casa de leis possui dois contratos ativos de licença da ferramenta KESB Select da desenvolvedora Kaspersky Global, em um deles possui o quantitativo de 130 licenças a expirar em 22/09/2024 e o outro de 20 licenças a expirar em 01/10/2024. Sendo assim, a solução apresentada deve fornecer 10 novas licenças e 150 em formato de renovação, adequada à nova linha de produtos das soluções de segurança com incremento de, no mínimo, EDR, bem como sua ativação. Referente a possibilidade de parcelamento, deve seguir de acordo com o ETP, por se tratar de uma solução integrada.

Custo Inicial Reduzido: Ao optar pela renovação, a empresa evita os altos custos iniciais de compra e instalação de novas soluções, permitindo a alocação de recursos para outras áreas críticas do negócio.

- **Suporte e atualizações:** Fornecimento dos serviços de suporte técnico, bem como atualizações, asseguram o perfeito funcionamento da solução.
- **Gestão Simplificada:** Por se tratar de uma solução integrada a gestão centralizada, permite aos profissionais maior autonomia e melhor condição de adaptação, visto que a equipe é reduzida.

Os itens da presente solução devem ser contratados em conjunto tendo em vista a necessidade de completa compatibilidade para o correto funcionamento.

a) Proteção antivírus de Arquivos;

b) Proteção antivírus da Web;

c) Firewall local de cada máquina;

d) Bloqueador de Ataques da Rede;

e) Inspeção do Sistema;

f) Inspeção avançada de dispositivos portáteis (pen drive, cartão de memória, etc);

g) Monitoramento de Vulnerabilidades.

4) REQUISITOS DA CONTRATAÇÃO

4.1. Do módulo de proteção de endpoint

a. A solução proposta deverá proteger os sistemas operacionais abaixo:

i. Windows 7
ii. Windows 8
iii. Windows 8.1
iv. Windows 10
v. Windows 11

b. Servidores

i. Windows Small Business Server 2011
ii. Windows MultiPoint Server 2011
iii. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

c. Servidores de terminal Microsoft

i. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

d. Sistemas operacionais Linux de 32 bits:

i. CentOS 6.7 e posterior
ii. Debian GNU/Linux 11.0 e posterior
iii. Debian GNU/Linux 12.0 e posterior
iv. Red Hat Enterprise Linux 6.7 e posterior

e. Sistemas operacionais Linux de 64 bits:

i. Amazon Linux 2.
ii. CentOS 6.7 e mais tarde
iii. CentOS 7.2 e posterior.
iv. CentOS Stream 8.
v. CentOS Stream 9.
vi. Debian GNU/Linux 11.0 e posterior.
vii. Debian GNU/Linux 12.0 e posterior.
viii. Linux Mint 20.3 e superior.
ix. Linux Mint 21.1 e posterior.
x. openSUSE Leap 15.0 e posterior.
xi. Oracle Linux 7.3 e posterior.
xii. Oracle Linux 8.0 e posterior.
xiii. Oracle Linux 9.0 e posterior.
xiv. Red Hat Enterprise Linux 6.7 e posterior
xv. Red Hat Enterprise Linux 7.2 e posterior.

xvi. Red Hat Enterprise Linux 8.0 e posterior.
xvii. Red Hat Enterprise Linux 9.0 e posterior.
xviii. Rocky Linux 8.5 e posterior.
xix. Rocky Linux 9.1.
xx. SUSE Linux Enterprise Server 12.5 ou posterior.
xxi. SUSE Linux Enterprise Server 15 ou posterior.
xxii. Ubuntu 20.04 LTS.
xxiii. Ubuntu 22.04 LTS.
xxiv. Sistemas operacionais Arm de 64 bits:
xxv. CentOS Stream 9.
xxvi. SUSE Linux Enterprise Server 15.
xxvii. Ubuntu 22.04 LTS.

f. Sistemas operacionais MAC OS:
i. macOS 12 – 14

g. Ferramentas de virtualização MAC OS:
i. Parallels Desktop 16 para Mac Business Edition
ii. VMware Fusion 11.5 Profissional
iii. VMware Fusion 12 Profissional

h. A solução proposta deverá suportar as seguintes plataformas virtuais:
i. VMware Workstation 17.0.2 Pro
ii. VMware ESXi 8.0 Update 2
iii. Microsoft Hyper-V Server 2019
iv. Citrix Virtual Apps e Desktop 7 2308
v. Citrix Provisioning 2308
vi. Citrix Hypervisor 8.2 Update 1

4.2. Do módulo de gerenciamento avançado

a. A solução proposta deve suportar arquitetura cloud-native e on-premisse;
b. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
i. Amazon Web Services
ii. Microsoft Azure
c. A solução proposta deve incluir as seguintes opções de integração SIEM:
i. HP (Microfoco) ArcSight
ii. IBM QRadar
iii. Splunk
iv. Kaspersky KUMA
d. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.
e. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;
f. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.
g. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.
h. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

i. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

j. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

k. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

l. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.

m. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

n. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:

i. Status do dispositivo
ii. Tag
iii. Diretório ativo
iv. Proprietários de dispositivos
v. Hardware

o. A solução proposta deve suportar os seguintes canais de entrega de notificação:

i. E-mail
ii. Registro de sistema
iii. SMS

p. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:

i. Atributos de rede
ii. Nome
iii. Domínio e/ou Sufixo de Domínio
iv. Endereço de IP
v. Endereço IP para servidor de gerenciamento
vi. Localização no Active Directory
vii. Unidade organizacional
viii. Grupo
ix. Sistema operacional
x. Número do pacote de serviço
xi. Arquitetura Virtual
xii. Registro de aplicativos
xiii. Nome da Aplicação
xiv. Versão do aplicativo
xv. Fabricante
xvi. Tipo e versão
xvii. Arquitetura

q. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

r. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

s. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

i. Dispositivos Desktop/Servidores
ii. Dispositivos móveis
iii. Dispositivos de rede
iv. Dispositivos virtuais
v. Componentes OEM
vi. Periféricos de computador
vii. Dispositivos IoT conectados
viii. Telefones VoIP
ix. Repositórios de rede

t. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

i. Nome da Aplicação
ii. Caminho do aplicativo
iii. Metadados do aplicativo
iv. Aplicativo Certificado digital
v. Categorias de aplicativos predefinidas pelo fornecedor
vi. SHA256 e MD5

u. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

i. Bluetooth
ii. Dispositivos móveis
iii. Modems externos
iv. CD/DVD
v. Câmeras e scanners
vi. MTPs
vii. E a transferência de dados para dispositivos móveis

v. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

w. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

x. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

i. Estruturas de domínios e grupos de trabalho do Windows
ii. Estruturas de grupos do Active Directory
iii. Conteúdo de um arquivo de texto criado manualmente pelo administrador

y. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

z. A solução proposta deve permitir realizar as seguintes ações para endpoints:

i. Verificação manual;
ii. Verificação no acesso;
iii. Verificação por demanda;
iv. Verificação de arquivos compactados
v. Verificação de arquivos individuais, pastas e unidades;
vi. Bloqueio e verificação de scripts

vii. Proteção contra alteração de registros;
viii. Proteção contra estouro de buffer;
ix. Verificação em segundo plano/inativa

1.1. Verificação de unidade removível na conexão com o sistema;
1.2. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.
1.3. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.
1.4. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.
1.5. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.
1.6. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.
1.7. A solução proposta deve suportar Windows Failover Cluster.
1.8. A solução proposta deve ter um recurso de clustering integrado.
1.9. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.
1.10. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.
1.11. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.
1.12. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.
1.13. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.
1.14. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.
1.15. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.
1.16. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.
1.17. A solução proposta deverá possuir controles para download de DLL e drivers.
1.18. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão.
1.19. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.
1.20. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).
1.21. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.
1.22. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir

as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.
1.23. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.
1.24. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.
1.25. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.
1.26. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.
1.27. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.
1.28. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.
1.29. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.
1.30. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.
1.31. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. .
1.32. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.
1.33. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.
1.34. A solução proposta deve permitir ao administrador personalizar relatórios.
1.35. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.
1.36. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.
1.37. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.
1.38. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.
1.39. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.

1.40. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.
1.41. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;
1.42. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.
1.43. A solução proposta deve suportar integração com solução APT.
1.44. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.
1.45. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:
1.45.1. Windows
1.45.2. Linux
1.46. A solução proposta deverá suportar os seguintes servidores de banco de dados:
1.46.1.1. Windows:
1.46.1.2. Microsoft SQL Server
1.46.1.3. Microsoft Banco de dados SQL do Azure
1.46.1.4. MySQL Standard e Enterprise
1.46.1.5. MariaDB
1.46.1.6. PostgreSQL
1.46.2. Linux:
1.46.2.1. MySQL
1.46.2.2. MariaDB
1.46.2.3. PostgreSQL
1.47. A solução proposta deverá suportar as seguintes plataformas virtuais:
1.47.1.1. Windows:
1.47.1.2. VMware vSphere 6.7 e 7.0
1.47.1.3. Estação de trabalho VMware 16 Pro
1.47.1.4. Servidor Microsoft Hyper-V 2012 de 64 bits
1.47.1.5. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
1.47.1.6. Microsoft Servidor Hyper -V 2016 de 64 bits
1.47.1.7. Servidor Microsoft Hyper-V 2019 de 64 bits
1.47.1.8. Servidor Microsoft Hyper-V 2022 de 64 bits
1.47.1.9. Citrix XenServer 7.1 LTSR
1.47.1.10. Citrix XenServer 8.x
1.47.1.11. Oracle VM VirtualBox 6.x
1.47.2. Linux:
1.47.2.1. VMware vSphere 6.7, 7.0 e 8.0
1.47.2.2. VMware Desktop 16 Pro e 17 Pro
1.47.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits
1.47.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
1.47.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits
1.47.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits
1.47.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits
1.47.2.8. Citrix XenServer 7.1 e 8.x

1.47.2.9. Oracle VM VirtualBox 6.x e7.x
1.48. A solução proposta deve suportar criptografia em vários níveis:
1.48.1. Criptografia completa do disco – incluindo disco do sistema
1.48.2. Criptografia de arquivos e pastas
1.48.3. Criptografia de mídia removível
1.48.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2
1.49. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:
1.49.1. A criptografia de arquivos em unidades de computador locais.
1.49.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.
1.49.3. A criação de listas criptografadas de pastas em unidades de computador locais.
1.50. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:
1.50.1. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.
1.50.2. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.
1.51. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:
1.51.1. A criptografia de todos os arquivos armazenados em unidades removíveis.
1.51.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.
1.52. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia
1.53. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.
1.54. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.
1.55. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.
1.56. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.
1.57. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.
1.58. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.

1.59. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.
1.60. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.
1.61. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.
1.62. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.
1.63. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.
1.64. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.
1.65. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário.
1.66. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.
1.67. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.
1.68. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:
1.68.1. Uso do Trusted Platform Module e configurações de senha.
1.68.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.
1.69. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).
1.70. A solução proposta deve suportar criptografia em Microsoft Surface Tablets.
1.71. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
1.71.1. Instalação remota de software de terceiros
1.71.2. Relatórios sobre software e hardware existentes
1.71.3. Monitoramento para instalação de software não autorizado
1.71.4. Remoção de software não autorizado
1.72. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.
1.73. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.
1.74. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.
1.75. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.
1.76. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.

1.77. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.
1.78. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.
1.79. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança
1.80. A solução proposta deve permitir ao administrador aprovar atualizações.
1.81. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.
1.82. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.
1.83. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.
1.84. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.
1.85. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.
1.86. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).
1.87. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.
1.88. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.
1.89. A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’.
1.90. A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”.
1.91. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.
1.92. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.
1.93. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.
1.94. A solução proposta deve apoiar a implantação do sistema operacional.
1.95. A solução proposta deve suportar Wake-on LAN e UEFI.
1.96. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.
1.97. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.
1.98. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.
1.99. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.
1.100. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.

1.101. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.
1.102. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.
1.103. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.
1.104. A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.
1.105. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:
1.105.1. Inicie a instalação ao reiniciar ou desligar o computador.
1.105.2. Instale o gerador necessário todos os pré-requisitos do sistema.
1.105.3. Permitir a instalação de novas versões de aplicativos durante as atualizações.
1.105.4. Baixe atualizações para o dispositivo sem instalá-las.
1.106. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.
1.107. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.
1.108. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:
1.108.1. CEF;
1.108.2. LEEF;
1.109. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.
1.110. O relatório da solução proposta deve conter informações CVE.
1.111. A solução proposta deve suportar instalação de aplicações e software de terceiros;

4.3. Do módulo de gerenciamento simplificado

1.112. A solução proposta deve suportar arquitetura cloud;
1.113. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.
1.114. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.
1.115. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.
1.116. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.
1.117. A solução proposta deve atender as condições apontadas no item e subintes 6.
1.118. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.
1.119. A solução proposta deve incluir informações do endpoint:
1.119.1. IP público de internet;
1.119.2. IP interno do dispositivo;
1.119.3. Versão do agente de proteção;

1.119.4. Ultima comunicação com a console, contendo data e hora;
1.119.5. Informações do sistema operacional;
1.120. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.
1.121. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.
1.122. A solução proposta deve incluir treinamento em segurança cibernética.

4.4. Requisitos gerais

1.123. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
1.123.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.
1.124. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
1.125. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).
1.126. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.
1.127. A solução proposta deve suportar o subsistema Linux no Windows.
1.128. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
1.128.1. Proteção contra ameaças sem arquivos (Fileless);
1.128.2. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;
1.129. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;
1.130. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.
1.131. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.
1.132. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.
1.133. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.
1.134. A solução proposta deve fornecer análise comportamental baseada em machine learning.
1.135. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.
1.136. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
1.136.1. Controles de aplicativos,
1.136.2. Controle web e dispositivos
1.136.3. HIPS e Firewall
1.136.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;

1.136.5. Gerenciamento de criptografia de arquivos e discos;
1.136.6. Controle adaptativo para detecção de anomalias;
1.137. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.
1.138. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.
1.139. A solução proposta deve ter bancos de dados de reputação locais e globais.
1.140. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.
1.141. A solução proposta deve incluir um módulo capaz, no mínimo, de:
1.141.1. Bloqueio de aplicativos com base em sua categorização.
1.141.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.
1.141.3. A adição de sub-redes e a modificação de permissões de atividade.
1.142. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.
1.143. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.
1.144. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.
1.145. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
1.145.1. Modo silencioso;
1.145.2. Discos rígidos e dispositivos removíveis;
1.145.3. De todos as contas de usuários do dispositivo.
1.146. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:
1.146.1. Exclusão imediata de dados;
1.146.2. Exclusão de dados adiada.
1.147. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:
1.147.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
1.147.2. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.
1.148. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.
1.149. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.
1.150. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.
1.151. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

1.152. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.
1.153. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.
1.154. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.
1.155. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;
1.156. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;
1.157. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.
1.158. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.
1.159. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.
1.160. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.
1.161. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.
1.162. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.
1.163. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.
1.164. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.
1.165. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.
1.166. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.
1.167. A solução proposta deve ter categoria de detecção para bloquear banners de sites.
1.168. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;
1.169. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.
1.170. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.
1.171. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.
1.172. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

1.173. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.
1.174. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.
1.175. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.
1.176. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.
1.177. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.
1.178. A solução proposta deve suportar o controle de scripts executados em PowerShell.
1.179. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.
1.180. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.
1.181. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.
1.182. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.
1.183. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.
1.184. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.
1.185. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
1.185.1. Filtro de anexos.
1.185.2. Verificação de mensagens de email ao receber, ler e enviar.
1.186. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.
1.187. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;
1.188. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);
1.189. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.
1.190. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.
1.191. A solução proposta deve incluir suporte ao protocolo IPv6.
1.192. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.
1.193. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
1.194. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.

1.195. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.
1.196. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.
1.197. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.
1.198. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.
1.199. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.
1.200. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.
1.201. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.
1.202. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.
1.203. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.
1.204. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.
1.205. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.
1.206. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.
1.207. A solução proposta deve suportar endereços IPv6.
1.208. A solução proposta deve suportar verificação em duas etapas (autenticação).
1.209. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.
1.210. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.
1.211. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.
1.212. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.
1.213. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.
1.214. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.
1.215. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.
1.216. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.

1.217. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.
1.218. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.
1.219. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.
1.220. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.
1.221. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.
1.222. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.
1.223. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.
1.224. A solução proposta deve ter a capacidade de excluir atualizações baixadas.
1.225. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.
1.226. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.
1.227. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.
1.228. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.
1.229. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.
1.230. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.
1.231. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.
1.232. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.
1.233. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
1.233.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.
1.233.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.
1.234. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.
1.235. A solução proposta deve gerar relatoiros de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

4.5. Do modulo de gerenciamento de dispositivos móveis

1.236. O modulo deve ser integrado a console de gerenciamento;
1.237. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
1.237.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)

1.238. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
1.238.1. iOS 10–17 ou iPadOS 13–17
1.239. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.
1.240. A solução proposta deve suportar dispositivos iOS supervisionados.
1.241. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.
1.242. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.
1.243. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.
1.244. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).
1.245. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.
1.246. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.
1.247. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.
1.248. A solução proposta deve ter recursos de conteinerização para dispositivos Android.
1.249. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:
1.249.1. Dados em contêineres
1.249.2. Contas de e-mail corporativo
1.249.3. Configurações para conexão à rede Wi-Fi corporativa e VPN
1.249.4. Nome do ponto de acesso (APN)
1.249.5. Perfil do Android for Work
1.249.6. Recipiente KNOX
1.249.7. Chave do gerenciador de licença KNOX
1.250. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
1.250.1. Todos os perfis de configuração instalados
1.250.2. Todos os perfis de provisionamento
1.250.3. O perfil iOS MDM
1.251. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas
1.252. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo .
1.253. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:
1.253.1. Critérios de verificação do dispositivo;

1.253.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;
1.254. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.
1.255. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:
1.255.1. Cartões de memória e outras unidades removíveis
1.255.2. Câmera do dispositivo
1.255.3. Conexões Wi-Fi
1.255.4. Conexões Bluetooth
1.255.5. Porta de conexão infravermelha
1.255.6. Ativação do ponto de acesso Wi-Fi
1.255.7. Conexão de área de trabalho remota
1.255.8. Sincronização de área de trabalho
1.255.9. Definir configurações da caixa de correio do Exchange
1.255.10. Configurar caixa de e-mail em dispositivos iOS MDM
1.255.11. Configure contêineres Samsung KNOX.
1.255.12. Definir as configurações do perfil do Android for Work
1.255.13. Configurar e-mail/calendário/contatos
1.255.14. Defina as configurações de restrição de conteúdo de mídia.
1.255.15. Definir configurações de proxy no dispositivo móvel
1.255.16. Configurar certificados e SCEP
1.256. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay .
1.257. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:
1.257.1. Google Play, Huawei App Gallery e Apple App Store
1.257.2. Portal de inscrição móvel KNOX
1.257.3. Pacotes de instalação pré-configurados independentes
1.258. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.
1.259. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.
1.260. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
1.260.1. VMware AirWatch 9.3 ou posterior
1.260.2. MobileIron 10.0 ou posterior
1.260.3. IBM MaaS360 10.68 ou posterior
1.260.4. Microsoft Intune 1908 ou posterior
1.260.5. SOTI MobiControl 14.1.4 (1693) ou posterior
1.261. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.
1.262. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:
1.262.1. Google Play
1.262.2. Galeria de aplicativos Huawei

1.262.3. Loja de aplicativos da Apple
1.263. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.
1.264. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.
1.265. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.
1.266. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.
1.267. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.
1.268. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.
1.269. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.
1.270. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.
1.271. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.
1.272. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.
1.273. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.
1.274. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.
1.275. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
1.276. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

4.6. Do módulo de EDR

4.6.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
4.6.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
4.6.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
4.6.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
4.6.5. Deve apresentar informações detalhadas contendo:
4.6.5.1.Usuário que executou a ação;
4.6.5.2.Informações acesso privilegiado;
4.6.6. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.
4.6.7. A solução proposta deve suportar integração com serviço de reputação em nuvem.
4.6.8. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)

4.6.9. O agente EDR deve ter integração com o aplicativo de proteção de endpoint(agente único).
4.6.10. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;
4.6.11. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.
4.6.12. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.
4.6.13. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.
4.6.14. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.
4.6.15. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.
4.6.16. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.
4.6.17. A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.
4.6.18. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.
4.6.19. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.
4.6.20. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:
4.6.21. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).
4.6.22. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.
4.6.23. Informações gerais sobre a detecção, incluindo modo de detecção.
4.6.24. Alterações no registro associadas à detecção.
4.6.25. Histórico da presença de arquivos no dispositivo.
4.6.26. Ações de resposta executadas pela aplicação.
4.6.27. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.
4.6.28. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:
4.6.29. Processo
4.6.30. Conexões de rede
4.6.31. Alterações no registro
4.6.32. Detalhes do download de objeto
4.6.33. A solução proposta deve fornecer orientação de resposta (resposta guiada).
4.6.34. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente

4.6.35. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
4.6.36. Impedir a execução de objetos
4.6.37. Isolamento de host
4.6.38. Excluir objeto do host ou grupo de hosts
4.6.39. Encerrar um processo no dispositivo
4.6.40. Colocar um objeto em quarentena
4.6.41. Execute a verificação do sistema
4.6.42. Execução remota de programa/processo/comando
4.6.43. Iniciar a varredura IoC para um grupo de hosts.

4.1. Requisitos para documentação da solução.
4.1.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:
4.1.2. Ajuda on-line para administradores
4.1.3. Ajuda on-line para melhores práticas de implementação
4.1.4. Ajuda on-line para proteção de servidores de administração
4.1.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.
4.2. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

5. PRAZO DE GARANTIA

5.1. As empresas licitantes deverão indicar o prazo da garantia do Software ou licença, que deverá ser de 36 meses oferecido diretamente ou com a autorização e responsabilidade do fabricante, sendo este o período em que se obrigam a prestar a manutenção e assistência técnica gratuita, nos termos regulados na minuta do contrato.

5.2. Serão desclassificadas as propostas que não ofereçam prazo de garantia ou abaixo do mínimo estipulado. As empresas licitantes indicarão, SOB PENA DE DESCLASSIFICAÇÃO, informações relacionadas à PADRONIZAÇÃO e COMPATIBILIDADE da solução, conforme detalhamento no ETP.

6. OBRIGAÇÕES DA CONTRATANTE

6.1. Comunicar à Contratada quaisquer irregularidades nos equipamentos, para adoção das providências cabíveis;

6.2. Designar funcionário para acompanhar/fiscalizar a entrega;

6.3. Efetuar os pagamentos relativos ao presente contrato em moeda corrente quando da apresentação da fatura de serviços executados respeitando os prazos de vencimentos;

6.4. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;

6.5. Qualquer alteração deste, somente deverá ser com o aval dos gestores do contrato;

6.6. Aplicar a contratada as sanções administrativas regulamentares e contratuais cabíveis;

7. OBRIGAÇÕES DA CONTRATADA

7.1. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

7.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do contrato, inerentes à execução do objeto contratual;

7.3. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

7.4. É de responsabilidade da CONTRATADA, manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

8. DA SUBCONTRATAÇÃO

8.1. Não será admitida a subcontratação do objeto.

9. MODELO DE EXECUÇÃO DO OBJETO

Em até, 30 dias, a contar da assinatura do contrato, as novas licenças deverão ser fornecidas e registradas em nome de CÂMARA MUNICIPAL DE FOZ DO IGUAÇU, nome fantasia PODER LEGISLATIVO, CNPJ 75.914.051/0001-28, atreladas a conta suporte@fozdoiguacu.pr.leg.br , dentro da plataforma da desenvolvedora Kaspersky Global.
Quando que realizada a disponibilização da licença, notificar via e-mail os responsáveis técnicos, sanches@fozdoiguacu.pr.leg.br e rodrigo@fozdoiguacu.pr.leg.br com detalhes do acesso.

10. MODELO DE GESTÃO DO CONTRATO E CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

A execução do objeto seguirá a seguinte dinâmica:

6.1 A contratante indicará Fiscal de contratos que irá acompanhar a execução do contrato em conformidade com este termo de referência.

6.2 O Contrato terá o prazo de 3 (três) anos, podendo ser prorrogado.

6.3 A Contratada formalizará a designação do preposto da empresa, especificando os poderes e responsabilidades relacionados à execução do objeto contratado.

6.4 Toda comunicação entre a Contratante e a Contratada deverá ser formalizada por escrito especialmente quando exigido por lei, podendo ser realizada por meio de mensagem eletrônica quando aplicável.

6.5 A execução será realizada de forma parcelada formalizada pelo envio da ordem de compra.

6.6 Os prazos e critérios para recebimento e pagamento estão detalhados nos itens 7.3 a 7.4.

6.7 Considera-se ocorrido o recebimento da nota fiscal quando a Gestão de contratos atestar a execução do objeto do contrato através do termo de recebimento definitivo.

6.8 Não haverá exigência de garantia contratual da execução, devido às características da

contratação.

6.9 A apresentação da Nota Fiscal/fatura é indispensável a cada fornecimento de bem ou serviço, para fins de liquidação e pagamento da despesa, emitida ao destinatário: Razão social: CÂMARA MUNICIPAL DE FOZ DO IGUACU; CNPJ: 75.914.051/0001-28; Endereço: Travessa Oscar Muxfeldt, nº 81, Centro, na cidade de Foz do Iguaçu-Paraná, CEP 85.851-490. Telefone: (45) 3521-8100.

6.10 Antes de cada pagamento à Contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

6.11 Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se- á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

6.12 Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

6.13 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

6.14 Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 20 (vinte) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da Contratante.

6.15 Persistindo a irregularidade, a Contratante deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa.

6.16 Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso a Contratada não regularize sua situação junto ao SICAF.

6.17 O prazo desta contratação será de 36 meses, contados da assinatura do contrato.

6.18 Pagamento:

6.18.1 Os pagamentos serão efetuados até o 10° (décimo) dia após o recebimento definitivo dos bens, condicionado a apresentação da Nota Fiscal/Fatura, bem como os documentos de regularidade

fiscal, social e trabalhista exigidos pelo art. 68 da Lei n° 14.133/2021

6.18.2 Na eventualidade de ocorrer atraso no pagamento, o valor será atualizado pela variação acumulada do IPCA/IBGE, ocorrida entre a data de seu adimplemento e a do efetivo pagamento, calculada pro rata tempore.

7 Sanções:

7.1 Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei n° 14.133, de 2021, quais sejam:

7.2 Dar causa à inexecução parcial do contrato;

7.3 Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

7.4 Dar causa à inexecução total do contrato;

7.5 Deixar de entregar a documentação exigida para o certame;

7.6 Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

7.7 Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

7.8 Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

7.9 Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

7.10 Fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

7.11 Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

7.12 Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

7.13 Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;

7.14 O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Multa de até 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor,

b) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver

c) aplicado a sanção, pelo prazo máximo de 3 (três) anos.

d) Direta, quando não se justificar a imposição de penalidade mais grave;

e) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 8.9 a bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

8 A fiscalização do contrato será realizada pelo servidor(a) designado:

9 A gestão do contrato será realizada pelo servidor (a) designado:

11. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço.

Tratamento diferenciado e favorecido a ser dispensado às microempresas, às empresas de pequeno porte e aos microempreendedores individuais conforme definido pelo documento de estudo técnico preliminar (ETP).

12. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

As quantidades previstas a serem adquiridas, conforme os itens descritos, são:

Item	Descrição	SKU	Quantidade	Valor Unit.	Valor
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160	R$ 358,19	R$ 57.310,40

A pesquisa de preço foi realizada considerando os parâmetros dispostos da Lei 14.133 no art. 23 § inciso IV – *"pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital"*. Do qual optou-se pelo menor preço ofertado.

Quanto à não utilização dos parâmetros dos § Incisos I e II do Art. 23, consultas no portal PNCP (Inciso I) e contratações similares feitas pela Administração Pública (II), conforme descrito no parágrafo anterior, torna-se ineficaz e escassa a busca por contratações similares em outros órgãos. Regendo-se pela economicidade, melhor tecnologia e melhores resultados pretendidos pelo órgão, a consulta aos fornecedores torna-se mais eficaz.

13. ADEQUAÇÃO ORÇAMENTÁRIA

ITEM	DOTAÇÃO
1	01.01.01.031.0001.2002.3.3.90.40.99.05 - AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: ABC5-0F02-498C-9F1A

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

RODRIGO NISHIMORI (CPF 007.XXX.XXX-01) em 07/08/2024 11:21:12 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://fozdoiguacu.1doc.com.br/verificacao/ABC5-0F02-498C-9F1A

ESTUDO TÉCNICO PRELIMINAR

1) DESCRIÇÃO DA NECESSIDADE

1.1. Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

1.2. A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

1.3. Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

1.4. Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

1.5. Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

1.6. Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

1.7. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.

2) REQUISITOS DA CONTRATAÇÃO

Item	Descriçao	SKU	Quantidade
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160

3) LEVANTAMENTO DE MERCADO

Considerando que a Câmara Municipal de Foz do Iguaçu já dispõe de um sistema de antivírus, foram avaliadas duas alternativas sendo uma delas a renovação e upgrade de versão do sistema e a outra a aquisição de um sistema integrado com o nosso sistema de Firewall.

Mantendo os investimentos já realizados, tendo em vista de que além da aquisição do sistema, foi também realizado a contratação de uma empresa especializada para nos auxiliar na configuração recomendadas pelo fabricante, e com base nas pesquisa de preços e estudo entre outras soluções, optou-se pela renovação e upgrade da versão já utilizada do licenciamento da solução Kaspersky e aquisição de novas licenças para contemplar a necessidade do parque computacional da CMFI, levando em consideração a ampliação do nosso parque computacional que ocorreu nesses últimos anos.

4) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

As especificações do objeto desta licitação deverão estar detalhadas no termo de referência elaborado com base neste estudo técnico preliminar e de acordo com a solicitação elaborada pelo setor demandante.

5) ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

Item	Descrição	SKU	Quantidade	Valor
1	KASPERSKY NEXT EDR OPTIMUM 36 meses	KL4066KASTJ	160	R$ 57.310,40

Descrição Item 1

A solução deve incluir treinamento em segurança cibernética

Do módulo de proteção de endpoint

Compatibilidade com diferentes sistemas operacionais, MAC OS, Linux de 32 e 64 bits (CentOS, Red Hat Enterprise, Debian, Ubuntu, Oracle Linux), Windows 7, 8, 8.1, 10,11 para desktops, para servidores S.O Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022, Windows Small Business Server 2011, Servidores de terminal Microsoft (Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022).

Módulo de gerenciamento avançado

A solução deve suportar arquitetura cloud-native e on-premisse, a solução deve incluir suporte para implantação baseada em nuvem (Amazon Web Services e/ou Microsoft Azure. Integração nativa com as seguintes opções de SIEM (HP (Microfoco) ArcSight, IBM QRadar, Splunk, Kaspersky KUMA). 2.4.

A solução deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

A solução deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

A solução deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

A solução deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

O servidor de gerenciamento primário da solução deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

A solução deve suportar os seguintes canais de entrega de notificação, E-mail, registro de sistema e SMS ou equivalente.

A solução deve ter a capacidade de etiquetar/marcar computadores com base em Atributos de rede, Nome, Domínio e/ou Sufixo de Domínio, Endereço de IP, Endereço IP para servidor de gerenciamento, Localização no Active Directory, Unidade organizacional, Grupo, Sistema operacional, Número do pacote de serviço, Arquitetura Virtual, Registro de aplicativos, Nome da Aplicação, Versão do aplicativo, Fabricante, Tipo e versão, Arquitetura.

A solução deverá permitir especificamente o bloqueio dos seguintes dispositivos, Bluetooth, Dispositivos móveis, Modems externos, CD/DVD, Câmeras e scanners.

A solução deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

A solução deve permitir realizar as seguintes ações para endpoints, verificação manual, verificação no acesso, verificação por demanda, verificação de arquivos compactados, verificação de arquivos individuais, pastas e unidades, bloqueio e verificação de scripts, proteção contra alteração de registros, proteção contra estouro de buffer, verificação em segundo plano/inativa.

A solução deverá suportar os seguintes servidores de banco de dados:

Windows,

- Microsoft SQL Server
- Microsoft Banco de dados SQL do Azure
- MySQL Standard e Enterprise
- MariaDB
- PostgreSQL

Linux:

- MySQL
- MariaDB
- PostgreSQL

A solução deverá suportar as seguintes plataformas virtuais:

Windows:

- VMware vSphere 6.7 e 7.0

- Estação de trabalho VMware 16 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Oracle VM VirtualBox 6.x

2.74.2. Linux:

- VMware vSphere 6.7, 7.0 e 8.0
- VMware Desktop 16 Pro e 17 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 e 8.x

Do módulo de gerenciamento simplificado

A solução deve suportar arquitetura cloud;

A solução deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

A solução deve permitir ao administrador gerar relatórios pré-definidos.

A solução deve incluir informações do endpoint, IP público de internet, IP interno do dispositivo, Versão do agente de proteção, ultima comunicação com a console, contendo data e hora, informações do sistema operacional;

Requisitos gerais

A solução deve ser capaz de detectar os seguintes tipos de ameaças:

Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

A solução deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.

A solução deve ter capacidade de integração com a central de segurança do Windows Defender.

A solução deve suportar o subsistema Linux no Windows.

A solução deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

- Proteção contra ameaças sem arquivos (Fileless);
- Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

Do modulo de gerenciamento de dispositivos móveis

O modulo deve ser integrado a console de gerenciamento;

A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

- Android 5.0 ou posterior (incluindo Android 12L)

A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

- iOS 10–17 ou iPadOS 13–17

A solução deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

Do módulo de EDR

Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.

A solução deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;

Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;

Deve apresentar informações detalhadas contendo:

- Usuário que executou a ação;
- Informações acesso privilegiado;

A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas. O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único).

6) IMPACTOS AMBIENTAIS

Não foram identificados impactos ambientes nesta contratação

7) JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Não se aplica

8) CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

Não se identificou contratações interdependentes e/ou correlatas, sendo que a prestação dos serviços depende exclusivamente do presente procedimento.

9) ALINHAMENTO COM PAC – PLANO ANUAL DE CONTRATAÇÕES

A demanda em questão encontra-se prevista no plano anual de contratações.

10) RESULTADOS PRETENDIDOS

- Garantir um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;
- Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo estações de trabalho e notebooks comprometidos;
- Evitar, mitigar e conter a propagação de pragas digitais (vírus/malwares/spywares, spam, entre outros) com a administração centralizada da solução de proteção;
- Permitir o controle de acesso à rede por dispositivos computacionais, permitindo gerenciamento destes dispositivos;
- Possibilitar análise pormenorizada de arquivos, discos rígidos, unidades móveis, mensagens de e-mail e anexos, viabilizando detecção de ameaças, com intento de salvaguardar a estrutura tecnológica de ataques com teor e objetivo malicioso;
- Possibilitar o controle de acesso e tráfego de informações aos dispositivos e serviços operacionais na rede, através de gerenciamento centralizado, o que vem

a complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;

- Aprimorar a segurança de TIC da CMFI frente a ameaças sofisticadas.

11) PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Tendo em vista que nosso ambiente de tecnologia já possui uma solução de firewall, não será necessária nenhuma providência prévia.

12) VIABILIDADE DA CONTRATAÇÃO

Esta equipe de TI declara viável esta contratação

13) TRATAMENTO DIFERENCIADO E FAVORECIDO A SER DISPENSADO ÀS MICROEMPRESAS, ÀS EMPRESAS DE PEQUENO PORTE E AOS MICROEMPREENDEDORES INDIVIDUAIS

Após diversas tentativas de localização e contato com empresas qualificadas como microempresas (ME) e empresas de pequeno porte (EPP) na região de Foz do Iguaçu para fornecimento das licenças, constatou-se a inexistência, inclusive pelo embasamento da pesquisa na base de de empresas credenciadas junto ao portal do desenvolvedor, acessado na data de 10/06/2024 às 09:38. Durante o processo de prospecção, entramos em contato direto com diversas empresas locais, incluindo aquelas registradas como ME e EPP, para verificar a capacidade técnica e a disponibilidade para fornecimento do serviço requerido. Nenhuma das ME/EPP contactadas demonstrou capacidade técnica ou interesse em participar do certame.

Diante dessas circunstâncias, a manutenção da exclusividade do certame para ME e EPP pode inviabilizar a contratação, comprometendo a eficiência e a continuidade dos serviços públicos dependentes de uma conexão estável e de alta velocidade, eis que há sério risco da licitação ser deserta. Ressalta-se, porém, que as ME/EPP ainda poderão participar do certame com vantagens sobre os demais concorrentes conforme versa a legislação pátria.

Portanto, justifica-se o afastamento da exclusividade de participação de microempresas e empresas de pequeno porte neste certame específico, com base na inexistência de fornecedores locais qualificados e na necessidade imperiosa de garantir a prestação adequada e contínua dos serviços públicos.

14) RESPONSÁVEIS PELA ELABORAÇÃO DO ETP

Jeverson Siqueira
Cargo: Tecnico de Informatica
Matrícula: 202.045
Setor: Diretoria de Tecnologia

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: 86AC-350E-D424-A918

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

JEVERSON SIQUEIRA (CPF 080.XXX.XXX-74) em 07/08/2024 13:42:46 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://fozdoiguacu.1doc.com.br/verificacao/86AC-350E-D424-A918

M I N U T A

CONTRATO Nº XX/2024

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS, QUE FAZEM ENTRE SI A CÂMARA MUNICIPAL DE FOZ DO IGUAÇU E A EMPRESA XXXXXXXXXXXXXXXXXX.

A **Câmara Municipal de Foz do Iguaçu**, pessoa jurídica de direito público, com sede em Foz do Iguaçu, Estado do Paraná, situada na Travessa Oscar Muxfeldt, 81, Centro, inscrita no CNPJ/MF sob o nº 75.914.051/0001-28, neste ato representada por seu Presidente, João José Arce Rodrigues, consoante competência originária prevista no art. 17 do Regimento Interno da Câmara Municipal de Foz do Iguaçu, daqui para frente denominada simplesmente de **CONTRATANTE,** e, de outro lado, a empresa XXXXXXXXXXXXXXXXXXXXXX, inscrita no CNPJ/MF sob o nº XXXXXXXXX/XXXX-XX, situado na XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, cidade de XXXXXXXXXX, Estado XXXXXXXXX, CEP: XX.XXX-XXX, representada por seu representante legal XXXXXXXXXXXXXXXXXXXX, inscrito junto ao CPF/MF sob n. XXXXXXXXXX, a seguir denominada simplesmente **CONTRATADA**, firmam o presente contrato, sujeitando-se às cláusulas a seguir expostas e às normas da Lei n. 14.133/2021, têm entre si justo e contratado o que segue:

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O objeto do presente contratação de empresa especializada e tecnicamente qualificada para o fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 meses, de acordo com as características e especificações técnicas e, quantitativos descritos em termo de referência, bem como em seus anexos, conforme descrição a seguir:

ITEM	CAT/MAT	DESCRIÇÃO	QUANT.	UNIDADE	VALOR UNIT.	VALOR TOTAL
1	350949	KASPERSKY NEXT EDR OPTIMUM	160	Uni	R$ XXXXX,XX	R$ XXXXXX,XX
TOTAL						R$ XXXXXX,XX

2. CLÁUSULA SEGUNDA – DA VINCULAÇÃO

2.1. Os Contraentes reconhecem a vinculação desta contratação aos termos do Pregão Eletrônico n. XX/XXXX, emitido pela CONTRATANTE e à respectiva proposta que for vencedora, sendo que as

especificações técnicas mínimas do objeto, a fundamentação da contratação, a descrição da solução como um todo, as condições da garantia, os requisitos de habilitação, qualificação, técnica e capacidade operacional e de fornecimento, os requisitos da contratação, dentre outras informações, estão constantes em Termo de Referência, que é parte integrante deste Contrato independentemente de sua transcrição, ao qual também se declaram vinculados os contraentes.

3. CLÁUSULA TERCEIRA – DA LEGISLAÇÃO APLICÁVEL E DOS CASOS OMISSOS

3.1. Aplica-se a Lei n. 14.133/2021 à execução deste Contrato, sendo esta também a legislação a ser aplicadas aos casos omissos.

4. CLÁUSULA QUARTA – DO REGIME DE EXECUÇÃO

4.1. Os serviços serão executados sob o regime de execução indireta.

4.2. A execução dos serviços especificados neste Contrato e em Termo de Referência deverá ter início em até 30 dias, contados da assinatura do contrato, mediante fornecimento das licenças registradas em nome da CÂMARA MUNICIPAL DE FOZ DO IGUAÇU, nome fantasia PODER LEGISLATIVO, CNPJ n. 75.914.051/0001-28, atreladas a conta suporte@fozdoiguacu.pr.leg.br, dentro da plataforma da desenvolvedora Karpersky Global.

4.2. Quando realizada a disponibilização da licença, notificar via e-mail os responsáveis técnicos, sanches@fozdoiguacu.pr.leg.br e rodrigo@fozdoiguacu.pr.leg.br com detalhes do acesso.

4.3. Os serviços de instalação e manutenção deverão ser realizados na sede administrativa da CONTRATANTE, no endereço Travessa Oscar Muxfeldt, 81 - Centro, Foz do Iguaçu - PR, 85851-490

4.4. Os serviços a serem contratados constituem-se em atividades materiais acessórias, instrumentais ou complementares à área de competência legal da CONTRATANTE, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

4.5. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e a Administração, vedando-se qualquer relação entre elas que caracterize pessoalidade e subordinação direta.

4.6. Os serviços contratados são enquadrados como continuados, tendo em vista a sua necessidade permanente para a CONTRATANTE.

5. CLÁUSULA QUINTA – PREÇO

5.1. Em contra partida aos serviços prestados a CONTRATANTE pagará à CONTRATADA o valor mensal de até R$ XXXXX, totalizando estimativa de pagamento anual de até R$ XXXXX, conforme descrito na proposta apresentada pela empresa e constante no processo administrativo.

5.2. No valor indicado estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, seguro e outros necessários ao cumprimento integral do objeto da contratação.

6. CLÁUSULA SEXTA – DO REAJUSTE

6.1. Mediante expresso pedido da CONTRATADA, os valores contratados poderão ser reajustados a cada 12 (doze) meses, contados a partir da data da proposta apresentada pela CONTRATADA, com aplicação do índice de variação do IPCA para o mesmo período ou outro índice que o substitua.
6.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de 12 (doze) meses para a próxima reajustamento, será contado a partir dos efeitos financeiros do último reajuste.
6.3. O reajuste previsto nesta cláusula poderá ser formalizado por Termo de Apostilamento.

7. CLÁUSULA SÉTIMA – DOS CRITÉRIOS DE MEDIÇÃO
7.1. Os Materiais entreguem dever estar em conformidade com as quantidades solicitadas dos itens já descritos neste documento;
7.2. A qualidade exigida dos equipamentos e materiais utilizados tem que estar de acordo com a qualidade de cada item, sendo vedada a utilização de materiais de qualidade inferior ou de não garantia.
7.3. Todos os pontos instalados devem ser certificados para assim constatar a qualidade do serviço e garantia de transmissão do mesmo.
7.4. Dos demais todos os itens devem ser novos seguidos rigidamente as especificações mínimas descritas na seção Requisitos da Contratação e amparados em seu prazo de garantia estabelecidos.

8. CLÁUSULA OITAVA – DO RECEBIMENTO
8.1. Os serviços serão recebidos provisoriamente no prazo de 05 (cinco) dias, para efeito de posterior verificação de sua conformidade com as especificações constantes na proposta;
8.2. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes na proposta, devendo ser substituídos no prazo de 10 (dez) dias, a contar da notificação da CONTRATANTE, às suas custas, sem prejuízo da aplicação das penalidades;
8.3. Na impossibilidade de realização dos serviços, a empresa vencedora deverá substituir o serviço por outro com especificações iguais ou superiores;
8.4. Os serviços serão recebidos definitivamente no prazo de 10 (dez) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação;
8.5. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo;
8.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

9. CLÁUSULA NONA – DO PAGAMENTO
9.1. Os pagamentos serão efetuados até o 10º (décimo) dia após o recebimento definitivo dos produtos/serviços, condicionado a apresentação da Nota Fiscal/Fatura, bem como os documentos de regularidade fiscal, social e trabalhista exigidos pelo art. 68 da Lei nº 14.133/2021.
9.2. Na eventualidade de ocorrer atraso no pagamento, o valor será atualizado pela variação acumulada do IPCA, ocorrida entre a data de seu adimplemento e a do efetivo pagamento, calculada pro rata tempore.
9.3. A apresentação da nota fiscal/fatura é indispensável a cada entrega de produtos ou prestação de

serviços, para fins de liquidação e pagamento da despesa, a ser emitida ao destinatário: Razão social: CÂMARA MUNICIPAL DE FOZ DO IGUACU; CNPJ: 75.914.051/0001-28; Endereço: Travessa Oscar Muxfeldt, nº 81, Centro, na cidade de Foz do Iguaçu-Paraná, CEP 85.851-490. Telefone: (45) 3521-8100.

9.4. Antes de cada pagamento à CONTRATADA, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

9.5. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se- á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.

9.6. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

9.7. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

9.8. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua notificação, por escrito, para que, no prazo de 15 (quinze) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.

9.9. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.

9.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso a CONTRATADA não regularize sua situação junto ao SICAF.

9.11. O prazo desta contratação será de 36 meses, contados da assinatura do contrato.

10. CLÁUSULA DÉCIMA – DO PRAZO PARA RESPOSTA AOS PEDIDOS DE REPACTUAÇÃO DE PREÇOS E RESTABELECIMENTO DO EQUILÍBRIO ECONÔMICO

10.1. Quando for o caso de repactuação de preços e/ou de restabelecimento do equilíbrio econômico deste Contrato, será de 30 dias úteis o prazo resposta da CONTRATANTE, a contar da data de formalização do pedido por parte da CONTRATADA.

11. CLÁUSULA DÉCIMA PRIMEIRA - DA INEXIGÊNCIA DE GARANTIAS À EXECUÇÃO DO CONTRATO

11.1. Dadas as características da contratação, não haverá exigência de garantia à execução do contrato.

12. CLÁUSULA DÉCIMA SEGUNDA – DA GARANTIA DOS PRODUTOS E SERVIÇOS

12.1. As empresas licitantes deverão indicar o prazo da garantia do Software ou licença, que deverá ser de 36 meses oferecido diretamente ou com a autorização e responsabilidade do fabricante, sendo este o período em que se obrigam a prestar a manutenção e assistência técnica gratuita, nos termos regulados em termo de referência.
12.2. Serão desclassificadas as propostas que não ofereçam prazo de garantia ou abaixo do mínimo estipulado. As empresas licitantes indicarão, SOB PENA DE DESCLASSIFICAÇÃO, informações relacionadas à PADRONIZAÇÃO e COMPATIBILIDADE da solução, conforme detalhamento no ETP.

13. CLÁUSULA DÉCIMA TERCEIRA – DOTAÇÃO ORÇAMENTÁRIA
13.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da Câmara Municipal, para o exercício de 2024 nas classificações: item 1 – 01.01.01.031.0001.2002.3.3.90.40.99.05 – AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE.
13.2. Nos exercícios seguintes, correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

14. CLÁUSULA DÉCIMA QUARTA – DAS OBRIGAÇÕES DA CONTRATANTE
14.1. A CONTRATANTE obriga-se a:
14.1.1. Comunicar à Contratada quaisquer irregularidades nos equipamentos, para adoção das providências cabíveis;
14.1.2. Designar funcionário para acompanhar/fiscalizar a entrega;
14.1.3. Efetuar os pagamentos relativos ao presente contrato em moeda corrente quando da apresentação da fatura de serviços executados respeitando os prazos de vencimentos;
14.1.4. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;
14.1.5. Qualquer alteração deste, somente deverá ser com o aval dos gestores do contrato;
14.1.6. Aplicar a contratada as sanções administrativas regulamentares e contratuais cabíveis.

15. CLÁUSULA DÉCIMA QUINTA – DAS OBRIGAÇÕES DA CONTRATADA
15.1. A CONTRATADA obriga-se a:
15.1.1. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;
15.1.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do contrato, inerentes à execução do objeto contratual;
15.1.3. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;
15.1.4. É de responsabilidade da CONTRATADA, manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

16. CLÁUSULA DÉCIMA SEXTA – DAS SANÇÕES ADMINISTRATIVAS

16.1. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei n° 14.133, de 2021, quais sejam:

16.1.1. Dar causa à inexecução parcial do contrato;

16.1.2. Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

16.1.3. Dar causa à inexecução total do contrato;

16.1.4. Deixar de entregar a documentação exigida para o certame;

16.1.5. Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

16.1.6. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

16.1.7. Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

16.1.8. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

16.1.9. Fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

16.1.10. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

16.1.11. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

16.1.12. Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;

16.1.13. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

16.1.13.1. Multa de até 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor;

16.1.15. Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, quando não se justificar a imposição de penalidade mais grave;

16.1.16. Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 16.1.8 e bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

16.2. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao fornecedor.

17. CLÁUSULA DÉCIMA SÉTIMA - DA OBRIGAÇÃO DE MANUTENÇÃO DAS CONDIÇÕES DE QUALIFICAÇÃO

17.1. A CONTRATADA obriga-se a manter, durante toda a execução do Contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições para a qualificação na contratação direta que precedeu a este instrumento;

18. CLÁUSULA DÉCIMA OITAVA - DA OBRIGAÇÃO DE RESERVA DE CARGOS PREVISTA EM LEI

18.1. A CONTRATADA, durante toda a execução do Contrato, obriga-se a cumprir as exigências de reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz.

19. CLÁUSULA DÉCIMA NONA – MODELO DE GESTÃO DO CONTRATO

19.1. A execução do objeto seguirá a seguinte dinâmica:

19.1.1. A contratante indicará Fiscal de contratos que irá acompanhar a execução do contrato em conformidade com este termo de referência.

19.1.2. O Contrato terá o prazo de 3 (três) anos, podendo ser prorrogado.

19.1.3. A Contratada formalizará a designação do preposto da empresa, especificando os poderes e responsabilidades relacionados à execução do objeto contratado.

19.1.4. Toda comunicação entre a Contratante e a Contratada deverá ser formalizada por escrito, especialmente quando exigido por lei, podendo ser realizada por meio de mensagem eletrônica, quando aplicável.

19.1.5. A execução será realizada de forma parcelada formalizada pelo envio da ordem de compra.

19.1.6. Os prazos e critérios para recebimento e pagamento estão detalhados nas cláusulas 7 a 9 retro.

19.1.7. Considera-se ocorrido o recebimento da nota fiscal quando a Gestão de contratos atestar a execução do objeto do contrato através do termo de recebimento definitivo.

19.1.8. Não haverá exigência de garantia contratual da execução, devido às características da contratação.

20. CLÁUSULA VIGÉSIMA – DA INEXECUÇÃO E DA EXTINÇÃO DO CONTRATO

20.1. A inexecução total ou parcial do contrato ensejará a sua extinção com as consequências contratuais e as previstas em lei, com fulcro no Título III, Capítulo VIII da Lei n. 14.133/2021, nos seguintes modos:

20.1.1. determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta;

20.1.2. consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração;

20.1.3. determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

20.2. Constituirão motivos para extinção do contrato, a qual deverá ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa, as seguintes situações:

20.2.1. não cumprimento ou cumprimento irregular de normas editalícias ou de cláusulas contratuais, de especificações, de projetos ou de prazos;

20.2.2. desatendimento das determinações regulares emitidas pela autoridade designada para acompanhar e fiscalizar sua execução ou por autoridade superior;

20.2.3. alteração social ou modificação da finalidade ou da estrutura da empresa que restrinja sua capacidade de concluir o contrato;

20.2.4. decretação de falência ou de insolvência civil, dissolução da sociedade ou falecimento do contratado;
20.2.5. caso fortuito ou força maior, regularmente comprovados, impeditivos da execução do contrato;
20.2.6. atraso na obtenção da licença ambiental, ou impossibilidade de obtê-la, ou alteração substancial do anteprojeto que dela resultar, ainda que obtida no prazo previsto;
20.2.7. atraso na liberação das áreas sujeitas a desapropriação, a desocupação ou a servidão administrativa, ou impossibilidade de liberação dessas áreas;
20.2.8. razões de interesse público, justificadas pela autoridade máxima do órgão ou da entidade CONTRATANTE.
20.3. O descumprimento, por parte da CONTRATADA, de suas obrigações legais e/ou contratuais assegurará ao CONTRATANTE o direito de extinguir o contrato a qualquer tempo, independentemente de aviso, interpelação judicial e/ou extrajudicial.
20.4. A extinção por ato unilateral do CONTRATANTE sujeitará a CONTRATADA à multa rescisória de até 10% (dez por cento) sobre o valor do saldo do contrato existente na data da extinção, independentemente de outras penalidades.
20.5. Caso o valor do prejuízo do CONTRATANTE advindo da extinção contratual por culpa da CONTRATADA exceder o valor da Cláusula Penal prevista no parágrafo anterior, esta valerá como mínimo de indenização, na forma do disposto no art. 416, parágrafo único, do Código Civil.
20.6. A extinção determinada por ato unilateral da Administração e a extinção consensual deverão ser precedidas de autorização escrita e fundamentada da autoridade competente e reduzidas a termo no respectivo processo.
20.7. A CONTRATANTE poderá rescindir o presente instrumento contratual, sem qualquer ônus à Administração, quando da conclusão de eventual novo procedimento de contratação de interesse público para objeto afim.

21. CLÁUSULA VIGÉSIMA PRIMEIRA – DA VIGÊNCIA

21.1. O presente Contrato terá validade de 36 (trinta e seis) meses, contados da data da assinatura, podendo ser prorrogado, a critério da Administração, conforme o disposto no art. 107, da Lei n. 14.133/2021 e suas alterações posteriores.
21.2. A prorrogação deste contrato deverá ser promovida mediante celebração de termo aditivo.

22. CLÁUSULA VIGÉSIMA SEGUNDA – DA FISCALIZAÇÃO

22.1. O acompanhamento e a fiscalização da execução das obrigações oriundas deste contrato ficarão a cargo do Gestor José Marceo Nicoletti Teixeira, e do Fiscal de Contratos, Jeverson Siqueira, e consiste na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais representantes da CONTRATANTE, especialmente designados, na forma do art. 117 da Lei nº 14.133/2021.
22.2. O fiscal do contrato deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 117 da Lei nº 14.133/2021.

22.3. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela CONTRATADA ensejará a aplicação de sanções administrativas, previstas neste Termo de Contrato e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 156 e 137 da Lei nº 14.133/2021.
22.4. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da CONTRATANTE ou de seus agentes e prepostos, de conformidade com art. 120 da Lei nº 14.133/2021.

23. CLÁUSULA VIGÉSIMA TERCEIRA – DA SUBCONTRATAÇÃO
23.1. É vedada a subcontratação total ou parcial do objeto deste Termo de Contrato.

24. CLÁUSULA VIGÉSIMA QUARTA – DAS VEDAÇÕES
24.1. É vedado à CONTRATADA:
24.1.1. Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;
24.1.2. Interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

25. CLÁUSULA VIGÉSIMA QUINTA – DAS ALTERAÇÕES
25.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos art. 124 a 136 da Lei n. 14.133/2021.

26. CLÁUSULA VIGÉSIMA SEXTA – DA PUBLICAÇÃO
26.1. A CONTRATANTE providenciará a publicação deste contrato no Diário Oficial do Município de Foz do Iguaçu, na página da Câmara Municipal de Foz do Iguaçu nos termos do art. 174 da Lei n. 14.133/2021 e no Portal Nacional de Contratações Públicas (PNCP), para fins de garantia a ampla publicidade.

27. CLÁUSULA VIGÉSIMA SÉTIMA – DO FORO
27.1. Fica eleito o foro desta cidade de Foz do Iguaçu, Estado do Paraná, para dirimir toda e qualquer questão que derivar deste contrato.

E por estarem justas e acordadas, assinam as partes o presente instrumento, na presença de duas testemunhas, que também o subscrevem, para que surtam todos os efeitos jurídicos e legais.

Foz do Iguaçu, xx de xxxxx de 2024.

CÂMARA MUNICIPAL DE FOZ DO IGUAÇU
João José Arce Morales

XXXXXXXXXXX
xxxxxxxxxxx

Testemunhas:

_____
Nome: XXXXXX
RG: XXXXXX
CPF: XXXXXXX

_____
Nome: XXXXXXXXX
RG: XXXXXXX
CPF XXXXXX

ANEXO IV - MODELO DE PROPOSTA DE PREÇOS
PREGÃO, NA FORMA ELETRÔNICA, Nº 03/2024

REF: PREGÃO, NA FORMA ELETRÔNICA, Nº 03/2024-TIPO MENOR PREÇO

A empresa _____, estabelecida na _____, no bairro _____, no Município de _____, no Estado de _____, no n.º _____, na Prefeitura sob o n.º_____ e no Estado sob o nº_____, CNPJ n.º_____, telefone n.º (____) _____ e e-mail _____, pela presente e consoante as especificações técnicas contidas no Edital, vem propor os valores abaixo para fornecimento de equipamentos de informática do Pregão, na forma Eletrônica, n° **03/2024**, conforme segue:

ITEM	DESCRIÇÃO	SKU	QNT	VALOR UNITÁRIO	VALOR TOTAL
1	Licença Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal license	KL4066KASTJ	160		

O **PREÇO TOTAL** apresentado na presente proposta é de R$ _____ (valor por extenso).

Nesta proposta de percentual de desconto e preço estão considerados obrigatoriamente:

a) **O atendimento às especificações detalhadas do objeto, consoante Anexo I deste Edital;**
b) **A inclusão de todas as despesas que influenciam nos custos, tais como despesas com custo, transporte e frete, tributos (impostos, taxas, emolumentos, contribuições fiscais e parafiscais), obrigações sociais, trabalhistas, fiscais, encargos comerciais ou de qualquer natureza e todos os ônus diretos e indiretos,**
c) **O prazo de validade da proposta é de 90 (noventa) dias, a contar da data da sessão do pregão, na forma eletrônica.**

Esta empresa declara que está ciente e cumprirá, integralmente, todas as cláusulas do EDITAL retro citado.

Foz do Iguaçu, _____ de _____ de _____.

_____

Assinatura do representante legal da empresa proponente
NOME:
RG:
CARGO:

PORTARIA DA PRESIDÊNCIA Nº 038/2024

O Presidente da Câmara Municipal de Foz do Iguaçu, Estado do Paraná, no uso de suas atribuições legais e considerando o Ato da Presidência nº 130/2023, de 11 de dezembro de 2023,

RESOLVE

Art. 1º Designar, a contar de 28 de janeiro de 2024, o servidor **CARLOS ALBERTO KASPER**, matrícula nº 201.489, ocupante do cargo efetivo de Analista Legislativo VI, como ***PREGOEIRO*** / **AGENTE DE CONTRATAÇÃO** da Câmara Municipal de Foz do Iguaçu.
Art. 2º Delegar ao Pregoeiro / Agente de Contratação, além das funções pertinentes, a coordenação da fase interna da licitação e a competência para firmar os respectivos atos e os instrumentos convocatórios, com exceção do Edital.
Art. 3º Designar os servidores abaixo relacionados como Equipe de Apoio para auxiliar o pregoeiro / agente de contratação na condução dos trabalhos:

- **CRISTINA ITO DE LIMA**, matrícula nº 201.752, Agente Administrativo IV;
- **RICARDO ANDRADE,** matrícula nº 200.552, Analista Legislativo VII;
- **CLÁUDIA CRISTINA DE ARAÚJO**, matrícula nº 201.500, Agente Administrativo V.

Art. 4º Esta Portaria terá vigência de 1 (um) ano, a contar de 28 de janeiro de 2024.
Art. 5º Revogar, a contar de 28 de janeiro de 2024, as Portarias da Presidências nºs 23, 24, 27, 199 e 200/2023.

Gabinete do Presidente da Câmara Municipal de Foz do Iguaçu, 06 de Fevereiro de 2024.

JOÃO MORALES
Presidente

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: 491D-962C-C88B-B6AF

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

JOAO JOSE ARCE MORALES (CPF 029.XXX.XXX-16) em 06/02/2024 14:13:07 (GMT-03:00)
Papel: Parte
Emitido por: AC SyngularID Multipla << AC SyngularID << Autoridade Certificadora Raiz Brasileira v5 (Assinatura ICP-Brasil)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://fozdoiguacu.1doc.com.br/verificacao/491D-962C-C88B-B6AF

Proc. Administrativo 13- 279/2024

De: CARLOS K. - AGCONT

Para: Envolvidos internos acompanhando

Data: 05/09/2024 às 13:52:37

Lista de Verificação

_

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras

Anexos:

CHECK_LIST_PREGAO_03.pdf

Assinado digitalmente (emissão + anexos) por:

Assinante	Data	Assinatura	
CARLOS ALBERTO KASPER	05/09/2024 13:53:09	1Doc	CARLOS ALBERTO KASPER CPF 061.XXX.XXX-20
Cristina Ito de Lima	06/09/2024 08:43:28	1Doc	CRISTINA ITO DE LIMA CPF 051.XXX.XXX-95

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **C1DC-880E-BF03-25B9**

LISTA DE VERIFICAÇÃO

VERIFICAÇÃO COMUM A TODAS AS CONTRATAÇÕES DE SOLUÇÃO DE TIC	Atende plenamente a exigência?	Indicação do local do processo em que foi atendida a exigência (doc. / fls. / SEI)
Houve abertura de processo administrativo?[1]	Sim	1DOC – PA279/2024
Foi adotada a forma eletrônica para o processo administrativo ou, caso adotada forma em papel, houve a devida justificativa?[2]	Sim	1DOC
A autoridade competente designou os agentes públicos responsáveis pelo desempenho das funções essenciais à contratação?[3]	Sim	Despacho 12 – Portaria da presidência nº 38/2024
Foi respeitado o princípio da segregação de funções? [4]	Sim	Despachos 5, 6, 8 e 12
A Administração registrou que a pretendida contratação está em consonância com o PDTIC?	Não	Não existe PDTIC
A pretendida contratação consta no Plano de Contratações Anual, ou é dispensada do referido registro? [5]	Sim	Despacho 2
Consta documento de formalização de demanda, elaborado pela área requisitante?[6] [7]	Sim	Abertura do processo
Foi certificado que objeto da contratação está compatível com as leis orçamentárias?[8]	Sim	Despacho 4
A Área de TIC avaliou o alinhamento da contratação ao PDTIC e ao Plano Anual de Contratações e indicou o Integrante Técnico para composição da Equipe de Planejamento da Contratação? [9]	Não	Não existe PDTIC
Após manifestação da área técnica, a autoridade competente da área administrativa indicou o Integrante Administrativo?	Não se aplica	
Foi elaborado o Estudo Técnico Preliminar da Contratação?	Sim	Despacho 5
O Estudo Técnico Preliminar contempla ao menos a descrição da necessidade, a estimativa do quantitativo, a estimativa do valor, a manifestação sobre o parcelamento e a manifestação sobre a viabilidade da contratação e, quanto aos demais elementos previstos no art. 18, §1º, da Lei nº 14.133/2021, estão contemplados ou há justificativa para sua ausência?[10]	Sim	Despacho 5
Houve manifestação justificando as exigências de práticas e/ou critérios de sustentabilidade ou sua dispensa no caso concreto?[11]	Sim	Despacho 5, ETP – item 6
Utilizou-se o Modelo de Termo de Referência previsto no Ato da Presidência nº 133/2023?	Sim	
Foi elaborado Termo de Referência?	Sim	Despacho 6
A definição do objeto da contratação foi feita de forma precisa, suficiente e clara, sem especificações que, por excessivas, irrelevantes ou desnecessárias, limitem ou frustrem a competição ou a realização do fornecimento da solução, e contém a indicação do prazo de duração do contrato e, se for o caso, a possibilidade de sua prorrogação? [12]	Sim	Despacho 6, TR, não compete à equipe de pregão julgar a justificativa apresentada
O objeto da contratação contempla, de forma detalhada, o quantitativo de bens e serviços necessários para sua composição, bem como o código do Catálogo de Materiais ou Serviços, disponível no Portal de Compras do Governo Federal? [13]	Sim	Despacho 6
Tratando-se de licitação para fornecimento de bens, em caso de indicação de uma ou mais marcas ou modelos, o que se admite apenas excepcionalmente, foi apresentado o estudo técnico, fundamentado nas alíneas do art. 41, I, da Lei nº 14.133/2021, que justifique essa opção?[14]	Sim	Despacho 6, TR, item 2, não compete à equipe de pregão julgar a justificativa apresentada
Há justificativa para o parcelamento ou não da solução de TIC? [15]	Não	Há apontamento “não se aplica”

		no item 7 do ETP (Despacho 5)
Em caso de licitação por preço global, foi observado que cada serviço ou produto do lote deve estar discriminado em itens separados nas propostas de preços, permitindo a identificação do preço individual e a eventual incidência das margens de preferência? [16]	Não se aplica	Item único
Há avaliação da viabilidade de permissão de consórcio ou subcontratação, com respectiva justificativa? [17]	Não	
Caso o TR contemple exigências de qualificação técnica ou econômica, elas foram justificadas no processo[18]?	Não se aplica	
Caso o TR contemple exigências de qualificação técnica, elas são específicas e objetivas?	Não se aplica	
Caso o TR contemple exigências de qualificação técnica ou econômica e o objeto licitatório refira-se a contratações para: a) entrega imediata; b) contratações em valores inferiores a 1/4 (um quarto) do limite para dispensa de licitação para compras em geral, ou; c) contratações de produto para pesquisa e desenvolvimento até o valor de R$324.122,46 (valor atualizado anualmente), houve justificativa para não dispensá-las?[19]	Não se aplica	
Foi elaborado Modelo de Execução do Contrato?	Sim	Despacho 6, TR, Itens 9/10 e Despacho 11, Termo de Contrato, cláusula 19ª
A forma de pagamento foi definida em função dos resultados?[20]	Não	
Em caso de contratação de serviços de TIC, o processo conta com Termo de Compromisso e Termo de Ciência?	Não se aplica	
Foram definidas as sanções administrativas?	Sim	Despacho 11, Termo de Contrato, Cláusula 16ª
Em caso de previsão de reajuste de preços por aplicação de índice, nas contratações de serviços de Tecnologia da Informação, foi previsto o índice de correção monetária ICTI (art. 24)?	Não	Despacho 11, cláusula 6ª da minuta de contrato
Caso tenha havido a opção por orçamento sigiloso, foi apresentada a competente justificativa? [21]	Não se aplica	
O Termo de Referência foi assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da área de TIC, com posterior aprovação pela autoridade competente?	Não	
Foi realizada análise de riscos, incluindo elaboração de Mapa de Gerenciamento de Riscos, devidamente assinado pela Equipe de Planejamento da Contratação, cujas informações podem ser utilizadas como insumos para a construção da Matriz de Alocação de Riscos?[22]	Não	
Os autos estão instruídos com o edital da licitação? [23]	Sim	Despacho 12, minuta de Edital
Foi utilizado modelo padronizado de edital ou justificada sua não utilização?	Não se aplica	Não existe modelo
Eventuais alterações implementadas nas minutas em relação aos modelos padronizados de Termo de Referência, Edital e Contrato foram destacadas no texto, e, se necessário, explicadas?	Não se aplica	
A Administração justificou o critério de julgamento adotado, inclusive para afastar ou não o critério de técnica e preço, considerando o disposto no art. 36 da Lei nº 14.133/2021? [24]	Sim	Despacho 12
Caso seja adotado o critério de julgamento por maior desconto, o preço estimado ou o máximo aceitável consta do edital da licitação? [25]	Não se aplica	
Caso o objeto contemple itens com valores inferiores a	Não	Despacho 5, ETP, Item12

R$80.000,00, eles foram destinados às ME/EPPs e entidades equiparadas ou foi justificada a não exclusividade? [26]		
Foi mantida no edital cláusula com índice de reajustamento de preços, com data-base vinculada à data do orçamento estimado? [27]	Sim	Despacho 11, cláusula 6ª da minuta de contrato
Caso tenha sido vedada a participação de cooperativas, consta justificativa nos autos? [28]	Não se aplica	
Caso tenha sido vedada a participação de consórcios, consta justificativa nos autos? [29]	Não se aplica	
Caso não conste minuta de contrato como anexo ao edital, a utilização de instrumento assemelhado foi justificada? [30]	Não se aplica	Despacho 12

VERIFICAÇÃO RELATIVA À PESQUISA DE PREÇOS E ÀS QUESTÕES ORÇAMENTÁRIAS PARA COMPRAS E SERVIÇOS EM GERAL	Atende plenamente a exigência?	Indicação do local do processo em que foi atendida a exigência (doc. / fls. / SEI)
Consta orçamento estimado com as composições detalhadas dos preços utilizados para sua formação?[31]	Sim	Despacho 8, RPP
Foi certificado que o valor previamente estimado da contratação está compatível com os valores praticados pelo mercado, considerados os preços constantes de bancos de dados públicos e as quantidades a serem contratadas, observadas a potencial economia de escala e as peculiaridades do local de execução do objeto? [32]	Não	Despacho 8, RPP
Foi certificado que o estimado preço foi obtido com base em pelo menos três preços ou houve justificativa pelo gestor responsável e aprovada pela autoridade competente para a hipótese excepcional em que não for respeitado referido número mínimo? [33]	Sim	Despacho 8, RPP
Caso o preço tenha sido obtido unicamente com base nos sistemas oficiais de governo, como Painel de Preços ou banco de preços em saúde, foi certificado que o valor estimado não é superior à mediana do item nos sistemas consultados? [34]	Não se aplica	
A pesquisa de preços contém, no mínimo, I - descrição do objeto a ser contratado; II - identificação do(s) agente(s) responsável(is) pela pesquisa ou, se for o caso, da equipe de planejamento; III - caracterização das fontes consultadas; IV - série de preços coletados; V - método estatístico aplicado para a definição do valor estimado; VI - justificativas para a metodologia utilizada, em especial para a desconsideração de valores inconsistentes, inexequíveis ou excessivamente elevados, se aplicável; VII - memória de cálculo do valor estimado e documentos que lhe dão suporte; e VIII - justificativa da escolha dos fornecedores, no caso da pesquisa direta	Sim	Despacho 8, RPP
Foi certificado que foram priorizados na pesquisa de preços os sistemas oficiais de governo, como Painel de Preços ou banco de preços em saúde, e contratações similares feitas pela Administração Pública, ou justificada a impossibilidade de utilização dessas fontes? [35]	Não	
Caso a pesquisa tenha se baseado em contratações similares feitas pela Administração Pública e já concluídas, a conclusão ocorreu em prazo inferior a 1 (um) ano à data da pesquisa de preços ou houve a devida justificativa para a utilização excepcional de preços de contratação concluída há mais de um ano? [36]	Não se aplica	
Nos casos de utilização de pesquisa direta com fornecedores, na hipótese em que ela for cabível, foi observado o número mínimo de consulta a três fornecedores ou foram instruídos os autos com as	Sim	Despacho 8, RPP

devidas justificativas? [37]		
Nos casos de utilização de pesquisa direta com fornecedores, foi certificada a observância de os orçamentos obtidos serem datados no máximo com 6 meses de antecedência da data prevista para divulgação do edital ou certificado que haverá a devida atualização caso ultrapassado esse prazo? [38]	Sim	Despacho 8, RPP
Caso realizada pesquisa direta com fornecedores, foi certificado que que o prazo de resposta concedido foi compatível com a complexidade do objeto da licitação?[39]	Sim	Despacho 8, RPP
Caso realizada pesquisa direta com fornecedores, foi certificado que os orçamentos contêm: a) descrição do objeto, valor unitário e total; b) número do Cadastro de Pessoa Física - CPF ou do Cadastro Nacional de Pessoa Jurídica - CNPJ do proponente; c) endereços físico e eletrônico e telefone de contato; d) data de emissão; e e) nome completo e identificação do responsável?[40]	Sim	Despacho 8, RPP
Caso realizada pesquisa direta com fornecedores, foi certificado que a consulta conteve informação das características da contratação, com vistas à melhor caracterização das condições comerciais praticadas para o objeto a ser contratado?	Sim	Despacho 8, RPP
Caso realizada pesquisa direta com fornecedores, consta dos autos a relação de fornecedores que foram consultados e não enviaram propostas como resposta à solicitação feita?[41]	Não	
Tratando-se de contratação que envolva a criação, expansão ou aperfeiçoamento de ação governamental que acarrete aumento da despesa, constam dos autos estimativa do impacto orçamentário-financeiro e declaração sobre adequação orçamentária e financeira?[42]	Não se aplica	

VERIFICAÇÃO ESPECÍFICA PARA <u>AQUISIÇÕES</u>	Atende plenamente a exigência?	Indicação do local do processo em que foi atendida a exigência (doc. / fls. / SEI etc.)
Se o objeto a ser contratado for bem de consumo, foi certificado que não se enquadra como bem de luxo? [43]	Não se aplica	
Há justificativa para não utilização de sistema de registro de preços?[44]	Não	
Foi certificado que a determinação do quantitativo a ser adquirido considerou a estimativa de consumo e utilização prováveis, com base em técnica adequada?[45]	Sim	Despacho 6, TR – item 3
Há manifestação sobre o atendimento do princípio da padronização?[46]	Sim	Despacho 6, TR – item 2
Há manifestação sobre o atendimento do princípio do parcelamento?[47]	Sim	Despacho 5, ETP – item 7
Caso o objeto contemple item de aquisição de bens de natureza divisível, com valor superior a R$80.000,00, foi prevista a cota reservada ou justificada sua não previsão?	Não	Despacho 5, ETP – item 13
No caso da cota reservada, a divisão do quantitativo destinado à cota procurou observar o limite percentual de até 25% do total, independentemente do valor da cota?	Não se aplica	
Há manifestação sobre a compatibilidade da despesa estimada com a prevista nas leis orçamentárias?[48]	Sim	Despacho 4

Consta informação do uso ou justificativa para não utilização de catálogo eletrônico de padronização?[49]	Sim	Despacho 6, TR – Item 1, utilização de CATMAT
Caso haja indicação de marca ou modelo, consta justificativa para a indicação?[50]	Sim	Despacho 6, não compete à equipe de pregão julgar a justificativa apresentada
Havendo vedação de determinada marca ou produto, foi indicada a existência de processo administrativo em que esteja comprovado que não atendem às necessidades da Administração?[51]	Não se aplica	
Há certificação no ETP ou nos autos de que a opção pela aquisição é mais vantajosa do que eventuais alternativas, como a locação de bens?[52]	Não se aplica	Licenciamento de software

Lista de Verificação preenchida por: Carlos Alberto Kasper

Lista de verificação conferida por: Cristina Ito de Lima

[1] ON-AGU 2/2009: "os instrumentos dos contratos, convênios e demais ajustes, bem como os respectivos aditivos, devem integrar um único processo administrativo, devidamente autuado em sequência cronológica, numerado, rubricado, contendo cada volume os respectivos termos de abertura e encerramento."

[2] Decreto nº 8.539/2015 e art. 12, VI, da Lei 14.133/21

[3] Art. 7º, *caput*, da Lei 14.133/21

[4] Art. 7º, §1º, da Lei 14.133/21. Art. 12 do Decreto 11.246/22.

[5] IN SGD nº 94/2022, art. 7º. Atentar para as exceções à obrigatoriedade de registro no Plano anual previstas no art. 1º, parágrafo único, e art. 7º, ambos do Decreto nº 10.947, de 25 de janeiro de 2022.

[6] O Documento de Formalização da Demanda (DFD) é documento obrigatório que deve constar em qualquer processo de contratação, conforme art. 12, VII, e art. 72, I, da Lei 14.133/21. A regra é que o DFD já tenha sido elaborado para os fins do PCA. Neste caso, é salutar que haja a juntada de sua cópia nos autos. Entretanto, nos casos previstos no art. 7º do Decreto nº 10.947/22, há a dispensa do registro da contratação no plano anual, o que implica na não elaboração, naquela oportunidade, do DFD. Então, nesta hipótese, o DFD constará apenas do processo de contratação direta, conforme art. 12, VII e §1º, da Lei 14.133/21 e art. 7º do Decreto 10.947/22, já citados.

[7] Art. 10. [...]

§ 1º O Documento de Formalização de Demanda a que se refere o inciso I deverá conter, no mínimo:

a) justificativa da necessidade da contratação;

b) descrição sucinta do objeto;

c) quantidade a ser contratada, quando couber, considerada a expectativa de consumo anual;

d) estimativa preliminar do valor da contratação, por meio de procedimento simplificado;

e) indicação da data pretendida para a conclusão da contratação, a fim de não gerar prejuízos ou descontinuidade das atividades do órgão ou da entidade;

f) grau de prioridade da compra ou da contratação em baixo, médio ou alto, de acordo com a metodologia estabelecida pelo órgão ou pela entidade contratante;

g) indicação de vinculação ou dependência com o objeto de outro documento de formalização de demanda para a sua execução, com vistas a determinar a sequência em que as contratações serão realizadas; e

h) nome da área requisitante ou técnica com a identificação do responsável.

[8] Art. 18 da Lei 14.133/21.

[9] IN SGD nº 94/2022, art. 10, II.

[10] Art. 18, §§ 1º e 2º, da Lei 14.133/21. Os incisos obrigatórios são:

"I - descrição da necessidade da contratação, considerado o problema a ser resolvido sob a perspectiva do interesse público;
[...]
IV - estimativas das quantidades para a contratação, acompanhadas das memórias de cálculo e dos documentos que lhes dão suporte, que considerem interdependências com outras contratações, de modo a possibilitar economia de escala;
[...]
VI - estimativa do valor da contratação, acompanhada dos preços unitários referenciais, das memórias de cálculo e dos documentos que lhe dão suporte, que poderão constar de anexo classificado, se a Administração optar por preservar o seu sigilo até a conclusão da licitação;
[...]
VIII - justificativas para o parcelamento ou não da contratação;
[...]
XIII - posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina.
§ 2º O estudo técnico preliminar deverá conter ao menos os elementos previstos nos incisos I, IV, VI, VIII e XIII do § 1º deste artigo e, quando não contemplar os demais elementos previstos no referido parágrafo, apresentar as devidas justificativas".

[11] Art. 5º e art. 11, I e IV, da Lei 14.133/21. Art. 16, I, "g", da IN SGD nº 94/2022.
Obs.: Recomenda-se a consulta ao "Guia Nacional de Licitações Sustentáveis", da CGU/AGU, que contém orientações indispensáveis para a contratação de determinados objetos.

[12] IN SGD nº 94/2022, art. 13.

[13] art. 12, II e 14 da IN SGD nº 94/2022.

[14] Art. 41. No caso de licitação que envolva o fornecimento de bens, a Administração poderá excepcionalmente:
I - indicar uma ou mais marcas ou modelos, desde que formalmente justificado, nas seguintes hipóteses:
a) em decorrência da necessidade de padronização do objeto;
b) em decorrência da necessidade de manter a compatibilidade com plataformas e padrões já adotados pela Administração;
c) quando determinada marca ou modelo comercializados por mais de um fornecedor forem os únicos capazes de atender às necessidades do contratante;
d) quando a descrição do objeto a ser licitado puder ser mais bem compreendida pela identificação de determinada marca ou determinado modelo aptos a servir apenas como referência;

[15] IN SGD nº 94/2022, art. 12, §§ 2º, I e 3º.

[16] IN SGD nº 94/2022, art. 12, §4º.

[17] IN SGD nº 94/2022, art. 12, § 2º, II.

[18] art. 18, inciso IX, da Lei nº 14.133, de 2021.

[19] O artigo art. 37, inciso XXI da Constituição Federal, preceitua que "o processo de licitação pública... somente permitirá as exigências de qualificação técnica e econômica indispensáveis à garantia do cumprimento das obrigações". Já o art. 70, III, da Lei nº 14.133/2021 estabelece que as exigências de habilitação poderão ser dispensadas nos casos especificados no item da lista de verificação. A combinação da disposição constitucional com a disposição legal resulta que as exigências de qualificação técnica e econômica nas situações retratadas no art. 70, III, deve ser excepcional e justificada.

[20] IN SGD nº 94/2022, art. 18, IV. Súmula TCU 269: Nas contratações para a prestação de serviços de tecnologia da informação, a remuneração deve estar vinculada a resultados ou ao atendimento de níveis de serviço, admitindo-se o pagamento por hora trabalhada ou por posto de serviço somente quando as características do objeto não o permitirem, hipótese em que a excepcionalidade deve estar prévia e adequadamente justificada nos respectivos processos administrativos.

[21] Art. 24 da Lei nº14.133/2021.

[22] IN SGD nº 94/2022, art. 38. Art. 18, X, da Lei nº 14.133/21. Cabe ressaltar que a análise de riscos não se confunde com a matriz de alocação de riscos, já que aquela é ato interno de planejamento da contratação, enquanto esta é cláusula contratual de pactuação de riscos com o contratado.
[23] Art. 18, V, da Lei 14.133/21.
[24] "Art. 36. O julgamento por técnica e preço considerará a maior pontuação obtida a partir da ponderação, segundo fatores objetivos previstos no edital, das notas atribuídas aos aspectos de técnica e de preço da proposta. § 1º O critério de julgamento de que trata o caput deste artigo será escolhido quando estudo técnico preliminar demonstrar que a avaliação e a ponderação da qualidade técnica das propostas que superarem os requisitos mínimos estabelecidos no edital forem relevantes aos fins pretendidos pela Administração nas licitações para contratação de:
I - serviços técnicos especializados de natureza predominantemente intelectual, caso em que o critério de julgamento de técnica e preço deverá ser preferencialmente empregado;
II - serviços majoritariamente dependentes de tecnologia sofisticada e de domínio restrito, conforme atestado por autoridades técnicas de reconhecida qualificação;
III - bens e serviços especiais de tecnologia da informação e de comunicação;
IV - obras e serviços especiais de engenharia;
V - objetos que admitam soluções específicas e alternativas e variações de execução, com repercussões significativas e concretamente mensuráveis sobre sua qualidade, produtividade, rendimento e durabilidade, quando essas soluções e variações puderem ser adotadas à livre escolha dos licitantes, conforme critérios objetivamente definidos no edital de licitação."
[25] Art. 24, par. ún., da Lei 14.133/21.
[26] art. 48, I, da Lei Complementar nº 123/2006.
[27] Art. 25, §7º, da Lei nº 14.133/21. Embora os modelos de editais devam trazer essa cláusula, o item da Lista é uma cautela para confirmar que a versão final manteve essa cláusula obrigatória.
[28] Art. 9º, I, "a", e art. 16 da Lei nº 14.133/21.
[29] Art. 9º, I, "a", e art. 15 da Lei nº 14.133/21.
[30] art. 95 da Lei 14.133/2021.
[31] Art. 18, IV, da Lei 14133/21. Art. 9º da IN Seges 65/21, c.c. art. 30, X, da IN Seges 5/2017;
[32] Art. 23 da Lei 14133/21.
[33] Art. 6º, §5º, da IN Seges nº 65/21.
[34] Art. 6º, §6º, da IN Seges nº 65/21.
[35] Art. 5º e §1º da IN Seges nº 65/21.
[36] Art. 5º, II, da IN Seges 65/21.
[37] Art. 5º, IV, e art. 6º, §5º, da IN Seges 65/21.
[38] Art. 5º, IV, da IN Seges 65/21.
[39] Art. 5º e §2º, inc. I, da IN Seges 65/21.
[40] Art. 5º e §2º, inc. II, da IN Seges 65/21.
[41] Art. 5º e §2º, inc. IV, da IN Seges 65/21.
[42] Art. 16, I e II, da LC 101/2000. Obs. 1: ON AGU 52/2014: "As despesas ordinárias e rotineiras da administração, já previstas no orçamento e destinadas à manutenção das ações governamentais preexistentes, dispensam as exigências previstas nos incisos I e II do art. 16 da Lei Complementar 101, de 2000".
[43] Art. 20 da Lei 14.133/21. Decreto nº 10818/21.
[44] Art. 40, II, da Lei 14.133/21
[45] Art. 40, III, da Lei 14.133/21
[46] Art. 40, V, "a", da Lei 14.133/21
[47] Art. 40, V, "b", da Lei 14.133/21
[48] Art. 40, V, "c", da Lei 14.133/21
[49] Art. 19, §2º, e art. 40, §1º, da Lei 14.133/21
[50] Art. 41, I, da Lei 14.133/21
[51] Art. 41, III, da Lei 14.133/21
[52] Art. 44 da Lei 14.133/21

Proc. Administrativo 14- 279/2024

De: CARLOS K. - AGCONT

Para: CMFI-DG-ATDG-DIRJUR - Diretoria Jurídica

Data: 05/09/2024 às 13:53:59

À diretoria jurídica para análise e parecer.

–

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras

Proc. Administrativo 15- 279/2024

De: Karla B. - CMFI-DG-ATDG-DIRJUR

Para: Envolvidos internos acompanhando

Data: 10/09/2024 às 09:42:25

Felipe Gomes Cabral - CMFI-PRESID-DG-ATDG-DIRJUR-EADJ

–

Karla Sales Balotin
Diretora Jurídica

Proc. Administrativo 16- 279/2024

De: Felipe C. - CMFI-PRESID-DG-ATDG-DIRJUR-EADJ

Para: AGCONT - Agente de contratação

Data: 10/09/2024 às 10:43:51

Vistos.

1. O procedimento deve ser adequado de forma a satisfazer os apontamentos que já constam da própria lista de verificação, sendo que tal documento consta com indicativos de itens não atendidos plenamente e sem a devida justificativa.
2. O levantamento de mercado do ETP justifica a indicação da marca em decorrência de que se trata de solução já aplicada à Câmara Municipal, inclusive, com necessidade de upgrade. Porém, não apresenta outras soluções ao gestor, como a contratação de nova solução e suas consequências, nem quais são todas as alternativas mercadológicas, o que exige a norma (art. 18, caput e §1º, V);
3. No TR, recomendo revisão do quadro de definição que consta do item 1, sendo especificadas as medidas de contagem e a natureza do valor exposto no quadro. Necessária correção do TR apresentado quanto à numeração do item, por exemplo, o item 4 que apresenta numeração até 1.276, e que depois da numeração do item 4,6 retorna ao item 4.1, o que pode ser objeto de apontamento.
4. A cotação não conta com fontes de bancos de preços, PNCP, contratações similares da Administração Pública ou fontes públicas, o que não atende a ordem prioritária do art. 23, §1º da L14133/21, demandando justificativa.

Oportuniza-se revisão da documentação apresentada. Após análise, retorne para parecer (art. 53, L14133/21).

–

Felipe Gomes Cabral – Consultor Jurídico, OAB/PR86944, mat. 202.053.

Documento assinado, datado e validado eletronicamente pelo sistema 1Doc, Sistema Eletrônico oficial da Câmara dos Vereadores de Foz do Iguaçu.

Proc. Administrativo 17- 279/2024

De: CARLOS K. - AGCONT

Para: CMFI-DG-DIRTEC - Diretoria de Tecnologia

Data: 12/09/2024 às 12:20:56

Segue para análise dos apontamentos da Diretoria Jurídica desta Casa.

–

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras

Proc. Administrativo 18- 279/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: Envolvidos internos acompanhando

Data: 12/09/2024 às 14:53:28

Termo de referencia versão ajustada.

_

Rafael Sanches
Diretoria de Tecnologia

Anexos:

1_Termo_de_Referencia_SolAntvir_v2.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Waldson de Almeida Dias	13/09/2024 11:04:37	1Doc	WALDSON DE ALMEIDA DIAS CPF 425.XXX.XXX-20

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **8D6E-2A15-90A9-AA4D**

TERMO DE REFERÊNCIA

1) DEFINIÇÃO DO OBJETO

Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

Item	CAT/ MAT	Descrição	SKU	Quantidade total	Valor Unit.	Valor Total
1	350949	Licença de uso individual da solução Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160	R$ 358,19	R$ 57.310,40

2) FUNDAMENTAÇÃO DA CONTRATAÇÃO

Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da

qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.
Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".
Considerando que esta casa de leis realiza a utilização da solução de segurança, sem ressalvas e visa proteger seu investimento, assegurar a padronização e compatibilidade com o ambiente computacional. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para, no mínimo, manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.
Com a iminente expiração da licença, torna-se necessária a renovação e aquisição para assegurar a proteção atualizada contra as ameaças virtuais mais recentes.
Sendo a demanda prevista no PAC, conforme documento de estudo técnico preliminar - ETP.

3) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução de segurança deve atender a necessidade de evolução e adequação desta casa em relação a suas ferramentas de proteção, esta casa de leis possui dois contratos ativos de licença da ferramenta KESB Select da desenvolvedora Kaspersky Global, em um deles possui o quantitativo de 130 licenças a expirar em 22/09/2024 e o outro de 20 licenças a expirar em 01/10/2024. Sendo assim, a solução apresentada deve fornecer 10 novas licenças e 150 em formato de renovação, adequada à nova linha de produtos das soluções de segurança com incremento de, no mínimo, EDR, bem como sua ativação. Referente a possibilidade de parcelamento, deve seguir de acordo com o ETP, por se tratar de uma solução integrada.

Custo Inicial Reduzido: Ao optar pela renovação, a empresa evita os altos custos iniciais de compra e instalação de novas soluções, permitindo a alocação de recursos para outras áreas críticas do negócio.

- **Suporte e atualizações:** Fornecimento dos serviços de suporte técnico, bem como atualizações, asseguram o perfeito funcionamento da solução.
- **Gestão Simplificada:** Por se tratar de uma solução integrada a gestão centralizada, permite aos profissionais maior autonomia e melhor condição de adaptação, visto que a equipe é reduzida.

Os itens da presente solução devem ser contratados em conjunto tendo em vista a necessidade de completa compatibilidade para o correto funcionamento.

a) Proteção antivírus de Arquivos;

b) Proteção antivírus da Web;

c) Firewall local de cada máquina;

d) Bloqueador de Ataques da Rede;

e) Inspeção do Sistema;

f) Inspeção avançada de dispositivos portáteis (pen drive, cartão de memória, etc);

g) Monitoramento de Vulnerabilidades.

4) REQUISITOS DA CONTRATAÇÃO

4.1. Do módulo de proteção de endpoint

a. A solução proposta deverá proteger os sistemas operacionais abaixo:
   i. Windows 7
   ii. Windows 8
   iii. Windows 8.1
   iv. Windows 10
   v. Windows 11
b. Servidores
   i. Windows Small Business Server 2011
   ii. Windows MultiPoint Server 2011
   iii. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022
c. Servidores de terminal Microsoft
   i. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022
d. Sistemas operacionais Linux de 32 bits:
   i. CentOS 6.7 e posterior
   ii. Debian GNU/Linux 11.0 e posterior
   iii. Debian GNU/Linux 12.0 e posterior
   iv. Red Hat Enterprise Linux 6.7 e posterior
e. Sistemas operacionais Linux de 64 bits:
   i. Amazon Linux 2.
   ii. CentOS 6.7 e mais tarde
   iii. CentOS 7.2 e posterior.
   iv. CentOS Stream 8.
   v. CentOS Stream 9.
   vi. Debian GNU/Linux 11.0 e posterior.
   vii. Debian GNU/Linux 12.0 e posterior.
   viii. Linux Mint 20.3 e superior.
   ix. Linux Mint 21.1 e posterior.
   x. openSUSE Leap 15.0 e posterior.
   xi. Oracle Linux 7.3 e posterior.

xii. Oracle Linux 8.0 e posterior.
xiii. Oracle Linux 9.0 e posterior.
xiv. Red Hat Enterprise Linux 6.7 e posterior
xv. Red Hat Enterprise Linux 7.2 e posterior.
xvi. Red Hat Enterprise Linux 8.0 e posterior.
xvii. Red Hat Enterprise Linux 9.0 e posterior.
xviii. Rocky Linux 8.5 e posterior.
xix. Rocky Linux 9.1.
xx. SUSE Linux Enterprise Server 12.5 ou posterior.
xxi. SUSE Linux Enterprise Server 15 ou posterior.
xxii. Ubuntu 20.04 LTS.
xxiii. Ubuntu 22.04 LTS.
xxiv. Sistemas operacionais Arm de 64 bits:
xxv. CentOS Stream 9.
xxvi. SUSE Linux Enterprise Server 15.
xxvii. Ubuntu 22.04 LTS.

f. Sistemas operacionais MAC OS:
    i. macOS 12 – 14
g. Ferramentas de virtualização MAC OS:
    i. Parallels Desktop 16 para Mac Business Edition
    ii. VMware Fusion 11.5 Profissional
    iii. VMware Fusion 12 Profissional
h. A solução proposta deverá suportar as seguintes plataformas virtuais:
    i. VMware Workstation 17.0.2 Pro
    ii. VMware ESXi 8.0 Update 2
    iii. Microsoft Hyper-V Server 2019
    iv. Citrix Virtual Apps e Desktop 7 2308
    v. Citrix Provisioning 2308
    vi. Citrix Hypervisor 8.2 Update 1

4.2. Do módulo de gerenciamento avançado

a. A solução proposta deve suportar arquitetura cloud-native e on-premisse;
b. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
    i. Amazon Web Services
    ii. Microsoft Azure
c. A solução proposta deve incluir as seguintes opções de integração SIEM:
    i. HP (Microfoco) ArcSight
    ii. IBM QRadar
    iii. Splunk
    iv. Kaspersky KUMA
d. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.
e. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

f. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.
g. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.
h. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.
i. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.
j. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.
k. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.
l. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.
m. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.
n. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:
    i. Status do dispositivo
    ii. Tag
    iii. Diretório ativo
    iv. Proprietários de dispositivos
    v. Hardware
o. A solução proposta deve suportar os seguintes canais de entrega de notificação:
    i. E-mail
    ii. Registro de sistema
    iii. SMS
p. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:
    i. Atributos de rede
    ii. Nome
    iii. Domínio e/ou Sufixo de Domínio
    iv. Endereço de IP
    v. Endereço IP para servidor de gerenciamento
    vi. Localização no Active Directory
    vii. Unidade organizacional
    viii. Grupo
    ix. Sistema operacional
    x. Número do pacote de serviço
    xi. Arquitetura Virtual
    xii. Registro de aplicativos
    xiii. Nome da Aplicação
    xiv. Versão do aplicativo
    xv. Fabricante

xvi. Tipo e versão
xvii. Arquitetura

q. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.
r. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.
s. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:
    i. Dispositivos Desktop/Servidores
    ii. Dispositivos móveis
    iii. Dispositivos de rede
    iv. Dispositivos virtuais
    v. Componentes OEM
    vi. Periféricos de computador
    vii. Dispositivos IoT conectados
    viii. Telefones VoIP
    ix. Repositórios de rede
t. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:
    i. Nome da Aplicação
    ii. Caminho do aplicativo
    iii. Metadados do aplicativo
    iv. Aplicativo Certificado digital
    v. Categorias de aplicativos predefinidas pelo fornecedor
    vi. SHA256 e MD5
u. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:
    i. Bluetooth
    ii. Dispositivos móveis
    iii. Modems externos
    iv. CD/DVD
    v. Câmeras e scanners
    vi. MTPs
    vii. E a transferência de dados para dispositivos móveis
v. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.
w. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.
x. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:
    i. Estruturas de domínios e grupos de trabalho do Windows
    ii. Estruturas de grupos do Active Directory
    iii. Conteúdo de um arquivo de texto criado manualmente pelo administrador

y. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.
z. A solução proposta deve permitir realizar as seguintes ações para endpoints:
    i. Verificação manual;
    ii. Verificação no acesso;
    iii. Verificação por demanda;
    iv. Verificação de arquivos compactados
    v. Verificação de arquivos individuais, pastas e unidades;
    vi. Bloqueio e verificação de scripts
    vii. Proteção contra alteração de registros;
    viii. Proteção contra estouro de buffer;
    ix. Verificação em segundo plano/inativa

1.1. Verificação de unidade removível na conexão com o sistema;
1.2. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.
1.3. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.
1.4. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.
1.5. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.
1.6. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.
1.7. A solução proposta deve suportar Windows Failover Cluster.
1.8. A solução proposta deve ter um recurso de clustering integrado.
1.9. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.
1.10. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.
1.11. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.
1.12. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.
1.13. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.
1.14. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.
1.15. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.
1.16. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.
1.17. A solução proposta deverá possuir controles para download de DLL e drivers.

1.18. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão.
1.19. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.
1.20. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).
1.21. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.
1.22. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.
1.23. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.
1.24. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.
1.25. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.
1.26. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.
1.27. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.
1.28. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.
1.29. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.
1.30. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.
1.31. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. .
1.32. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.
1.33. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante

um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.

1.34. A solução proposta deve permitir ao administrador personalizar relatórios.

1.35. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.

1.36. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.

1.37. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.

1.38. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.

1.39. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.

1.40. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.

1.41. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;

1.42. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.

1.43. A solução proposta deve suportar integração com solução APT.

1.44. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.

1.45. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:

1.45.1. Windows

1.45.2. Linux

1.46. A solução proposta deverá suportar os seguintes servidores de banco de dados:

1.46.1.1. Windows:

1.46.1.2. Microsoft SQL Server

1.46.1.3. Microsoft Banco de dados SQL do Azure

1.46.1.4. MySQL Standard e Enterprise

1.46.1.5. MariaDB

1.46.1.6. PostgreSQL

1.46.2. Linux:

1.46.2.1. MySQL

1.46.2.2. MariaDB

1.46.2.3. PostgreSQL

1.47. A solução proposta deverá suportar as seguintes plataformas virtuais:

1.47.1.1. Windows:

1.47.1.2. VMware vSphere 6.7 e 7.0

1.47.1.3. Estação de trabalho VMware 16 Pro

1.47.1.4. Servidor Microsoft Hyper-V 2012 de 64 bits

1.47.1.5. Servidor Microsoft Hyper-V 2012 R2 de 64 bits

1.47.1.6. Microsoft Servidor Hyper -V 2016 de 64 bits
1.47.1.7. Servidor Microsoft Hyper-V 2019 de 64 bits
1.47.1.8. Servidor Microsoft Hyper-V 2022 de 64 bits
1.47.1.9. Citrix XenServer 7.1 LTSR
1.47.1.10. Citrix XenServer 8.x
1.47.1.11. Oracle VM VirtualBox 6.x

1.47.2. Linux:

1.47.2.1. VMware vSphere 6.7, 7.0 e 8.0
1.47.2.2. VMware Desktop 16 Pro e 17 Pro
1.47.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits
1.47.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
1.47.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits
1.47.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits
1.47.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits
1.47.2.8. Citrix XenServer 7.1 e 8.x
1.47.2.9. Oracle VM VirtualBox 6.x e7.x

1.48. A solução proposta deve suportar criptografia em vários níveis:
1.48.1. Criptografia completa do disco – incluindo disco do sistema
1.48.2. Criptografia de arquivos e pastas
1.48.3. Criptografia de mídia removível
1.48.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2

1.49. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:
1.49.1. A criptografia de arquivos em unidades de computador locais.
1.49.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.
1.49.3. A criação de listas criptografadas de pastas em unidades de computador locais.

1.50. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:
1.50.1. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.
1.50.2. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.

1.51. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:
1.51.1. A criptografia de todos os arquivos armazenados em unidades removíveis.
1.51.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.

1.52. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia

1.53. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.

1.54. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.

1.55. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.

1.56. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.

1.57. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.

1.58. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.

1.59. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.

1.60. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.

1.61. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.

1.62. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.

1.63. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.

1.64. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.

1.65. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário.

1.66. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.

1.67. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.

1.68. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:

1.68.1. Uso do Trusted Platform Module e configurações de senha.

1.68.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.

1.69. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).
1.70. A solução proposta deve suportar criptografia em Microsoft Surface Tablets.
1.71. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
1.71.1. Instalação remota de software de terceiros
1.71.2. Relatórios sobre software e hardware existentes
1.71.3. Monitoramento para instalação de software não autorizado
1.71.4. Remoção de software não autorizado
1.72. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.
1.73. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.
1.74. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.
1.75. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.
1.76. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.
1.77. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.
1.78. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.
1.79. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança
1.80. A solução proposta deve permitir ao administrador aprovar atualizações.
1.81. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.
1.82. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.
1.83. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.
1.84. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.
1.85. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.
1.86. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).
1.87. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.
1.88. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.
1.89. A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’.

1.90. A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”.
1.91. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.
1.92. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.
1.93. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.
1.94. A solução proposta deve apoiar a implantação do sistema operacional.
1.95. A solução proposta deve suportar Wake-on LAN e UEFI.
1.96. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.
1.97. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.
1.98. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.
1.99. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.
1.100. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.
1.101. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.
1.102. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.
1.103. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.
1.104. A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.
1.105. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:
1.105.1. Inicie a instalação ao reiniciar ou desligar o computador.
1.105.2. Instale o gerador necessário todos os pré-requisitos do sistema.
1.105.3. Permitir a instalação de novas versões de aplicativos durante as atualizações.
1.105.4. Baixe atualizações para o dispositivo sem instalá-las.
1.106. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.
1.107. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.
1.108. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:
1.108.1. CEF;

1.108.2. LEEF;

1.109. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.

1.110. O relatório da solução proposta deve conter informações CVE.

1.111. A solução proposta deve suportar instalação de aplicações e software de terceiros;

4.3. Do módulo de gerenciamento simplificado

1.112. A solução proposta deve suportar arquitetura cloud;

1.113. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

1.114. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

1.115. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.

1.116. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.

1.117. A solução proposta deve atender as condições apontadas no item e subintes 6.

1.118. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.

1.119. A solução proposta deve incluir informações do endpoint:

1.119.1. IP público de internet;

1.119.2. IP interno do dispositivo;

1.119.3. Versão do agente de proteção;

1.119.4. Ultima comunicação com a console, contendo data e hora;

1.119.5. Informações do sistema operacional;

1.120. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.

1.121. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.

1.122. A solução proposta deve incluir treinamento em segurança cibernética.

4.4. Requisitos gerais

1.123. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:

1.123.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

1.124. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.

1.125. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).

1.126. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.

1.127. A solução proposta deve suportar o subsistema Linux no Windows.

1.128. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

1.128.1. Proteção contra ameaças sem arquivos (Fileless);

1.128.2. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

1.129. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;
1.130. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.
1.131. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.
1.132. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.
1.133. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.
1.134. A solução proposta deve fornecer análise comportamental baseada em machine learning.
1.135. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.
1.136. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
1.136.1. Controles de aplicativos,
1.136.2. Controle web e dispositivos
1.136.3. HIPS e Firewall
1.136.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;
1.136.5. Gerenciamento de criptografia de arquivos e discos;
1.136.6. Controle adaptativo para detecção de anomalias;
1.137. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.
1.138. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.
1.139. A solução proposta deve ter bancos de dados de reputação locais e globais.
1.140. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.
1.141. A solução proposta deve incluir um módulo capaz, no mínimo, de:
1.141.1. Bloqueio de aplicativos com base em sua categorização.
1.141.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.
1.141.3. A adição de sub-redes e a modificação de permissões de atividade.
1.142. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.
1.143. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.
1.144. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem

ser armazenados em um formato específico que garanta que não representem qualquer ameaça.

1.145. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
- 1.145.1. Modo silencioso;
- 1.145.2. Discos rígidos e dispositivos removíveis;
- 1.145.3. De todos as contas de usuários do dispositivo.

1.146. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:
- 1.146.1. Exclusão imediata de dados;
- 1.146.2. Exclusão de dados adiada.

1.147. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:
- 1.147.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
- 1.147.2. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.

1.148. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.

1.149. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.

1.150. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.

1.151. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

1.152. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.

1.153. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.

1.154. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.

1.155. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;

1.156. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;

1.157. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.

1.158. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.

1.159. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.

1.160. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.
1.161. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.
1.162. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.
1.163. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.
1.164. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.
1.165. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.
1.166. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.
1.167. A solução proposta deve ter categoria de detecção para bloquear banners de sites.
1.168. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;
1.169. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.
1.170. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.
1.171. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.
1.172. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;
1.173. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.
1.174. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.
1.175. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.
1.176. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.
1.177. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.
1.178. A solução proposta deve suportar o controle de scripts executados em PowerShell.
1.179. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.
1.180. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.
1.181. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.

1.182. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.
1.183. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.
1.184. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.
1.185. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
1.185.1. Filtro de anexos.
1.185.2. Verificação de mensagens de email ao receber, ler e enviar.
1.186. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.
1.187. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;
1.188. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);
1.189. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.
1.190. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.
1.191. A solução proposta deve incluir suporte ao protocolo IPv6.
1.192. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.
1.193. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
1.194. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.
1.195. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.
1.196. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.
1.197. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.
1.198. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.
1.199. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.
1.200. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.
1.201. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.

1.202. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.
1.203. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.
1.204. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.
1.205. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.
1.206. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.
1.207. A solução proposta deve suportar endereços IPv6.
1.208. A solução proposta deve suportar verificação em duas etapas (autenticação).
1.209. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.
1.210. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.
1.211. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.
1.212. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.
1.213. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.
1.214. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.
1.215. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.
1.216. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.
1.217. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.
1.218. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.
1.219. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.
1.220. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.
1.221. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.
1.222. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.

1.223. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.
1.224. A solução proposta deve ter a capacidade de excluir atualizações baixadas.
1.225. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.
1.226. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.
1.227. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.
1.228. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.
1.229. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.
1.230. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.
1.231. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.
1.232. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.
1.233. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
1.233.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.
1.233.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.
1.234. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.
1.235. A solução proposta deve gerar relatoiros de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

4.5. Do modulo de gerenciamento de dispositivos móveis

1.236. O modulo deve ser integrado a console de gerenciamento;
1.237. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
1.237.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)
1.238. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
1.238.1. iOS 10–17 ou iPadOS 13–17
1.239. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.
1.240. A solução proposta deve suportar dispositivos iOS supervisionados.
1.241. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.

1.242. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.

1.243. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.

1.244. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).

1.245. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.

1.246. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

1.247. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.

1.248. A solução proposta deve ter recursos de conteinerização para dispositivos Android.

1.249. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:

1.249.1. Dados em contêineres

1.249.2. Contas de e-mail corporativo

1.249.3. Configurações para conexão à rede Wi-Fi corporativa e VPN

1.249.4. Nome do ponto de acesso (APN)

1.249.5. Perfil do Android for Work

1.249.6. Recipiente KNOX

1.249.7. Chave do gerenciador de licença KNOX

1.250. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:

1.250.1. Todos os perfis de configuração instalados

1.250.2. Todos os perfis de provisionamento

1.250.3. O perfil iOS MDM

1.251. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas

1.252. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo .

1.253. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:

1.253.1. Critérios de verificação do dispositivo;

1.253.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;

1.254. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.

1.255. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:

1.255.1. Cartões de memória e outras unidades removíveis
1.255.2. Câmera do dispositivo
1.255.3. Conexões Wi-Fi
1.255.4. Conexões Bluetooth
1.255.5. Porta de conexão infravermelha
1.255.6. Ativação do ponto de acesso Wi-Fi
1.255.7. Conexão de área de trabalho remota
1.255.8. Sincronização de área de trabalho
1.255.9. Definir configurações da caixa de correio do Exchange
1.255.10. Configurar caixa de e-mail em dispositivos iOS MDM
1.255.11. Configure contêineres Samsung KNOX.
1.255.12. Definir as configurações do perfil do Android for Work
1.255.13. Configurar e-mail/calendário/contatos
1.255.14. Defina as configurações de restrição de conteúdo de mídia.
1.255.15. Definir configurações de proxy no dispositivo móvel
1.255.16. Configurar certificados e SCEP

1.256. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay .

1.257. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:
1.257.1. Google Play, Huawei App Gallery e Apple App Store
1.257.2. Portal de inscrição móvel KNOX
1.257.3. Pacotes de instalação pré-configurados independentes

1.258. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.

1.259. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.

1.260. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
1.260.1. VMware AirWatch 9.3 ou posterior
1.260.2. MobileIron 10.0 ou posterior
1.260.3. IBM MaaS360 10.68 ou posterior
1.260.4. Microsoft Intune 1908 ou posterior
1.260.5. SOTI MobiControl 14.1.4 (1693) ou posterior

1.261. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.

1.262. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:
1.262.1. Google Play
1.262.2. Galeria de aplicativos Huawei
1.262.3. Loja de aplicativos da Apple

1.263. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.

1.264. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.

1.265. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.
1.266. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.
1.267. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.
1.268. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.
1.269. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.
1.270. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.
1.271. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.
1.272. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.
1.273. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.
1.274. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.
1.275. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
1.276. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

4.6. Do módulo de EDR

4.6.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
4.6.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
4.6.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
4.6.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
4.6.5. Deve apresentar informações detalhadas contendo:
4.6.5.1. Usuário que executou a ação;
4.6.5.2. Informações acesso privilegiado;
4.6.6. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.
4.6.7. A solução proposta deve suportar integração com serviço de reputação em nuvem.
4.6.8. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado.

(Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)

4.6.9. O agente EDR deve ter integração com o aplicativo de proteção de endpoint(agente único).

4.6.10. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;

4.6.11. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.

4.6.12. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.

4.6.13. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.

4.6.14. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.

4.6.15. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.

4.6.16. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.

4.6.17. A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.

4.6.18. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.

4.6.19. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.

4.6.20. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:

4.6.21. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).

4.6.22. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.

4.6.23. Informações gerais sobre a detecção, incluindo modo de detecção.

4.6.24. Alterações no registro associadas à detecção.

4.6.25. Histórico da presença de arquivos no dispositivo.

4.6.26. Ações de resposta executadas pela aplicação.

4.6.27. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.

4.6.28. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:

4.6.29. Processo

4.6.30. Conexões de rede

4.6.31. Alterações no registro

4.6.32. Detalhes do download de objeto

4.6.33. A solução proposta deve fornecer orientação de resposta (resposta guiada).

4.6.34. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente
4.6.35. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
4.6.36. Impedir a execução de objetos
4.6.37. Isolamento de host
4.6.38. Excluir objeto do host ou grupo de hosts
4.6.39. Encerrar um processo no dispositivo
4.6.40. Colocar um objeto em quarentena
4.6.41. Execute a verificação do sistema
4.6.42. Execução remota de programa/processo/comando
4.6.43. Iniciar a varredura IoC para um grupo de hosts.

4.7. **Requisitos para documentação da solução.**

4.7.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:
4.7.2. Ajuda on-line para administradores
4.7.3. Ajuda on-line para melhores práticas de implementação
4.7.4. Ajuda on-line para proteção de servidores de administração
4.7.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.
4.7.6. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

04. PRAZO DE GARANTIA

a. As empresas licitantes deverão indicar o prazo da garantia do Software ou licença, que deverá ser de 36 meses oferecido diretamente ou com a autorização e responsabilidade do fabricante, sendo este o período em que se obrigam a prestar a manutenção e assistência técnica gratuita, nos termos regulados na minuta do contrato.

b. Serão desclassificadas as propostas que não ofereçam prazo de garantia ou abaixo do mínimo estipulado. As empresas licitantes indicarão, SOB PENA DE DESCLASSIFICAÇÃO, informações relacionadas à PADRONIZAÇÃO e COMPATIBILIDADE da solução, conforme detalhamento no ETP.

05. OBRIGAÇÕES DA CONTRATANTE

a. Comunicar à Contratada quaisquer irregularidades nos equipamentos, para adoção das providências cabíveis;

b. Designar funcionário para acompanhar/fiscalizar a entrega;

c. Efetuar os pagamentos relativos ao presente contrato em moeda corrente quando da apresentação da fatura de serviços executados respeitando os prazos de vencimentos;

d. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;

e. Qualquer alteração deste, somente deverá ser com o aval dos gestores do contrato;

f. Aplicar a contratada as sanções administrativas regulamentares e contratuais cabíveis;

06. OBRIGAÇÕES DA CONTRATADA

a. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

b. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do contrato, inerentes à execução do objeto contratual;

c. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

d. É de responsabilidade da CONTRATADA, manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

07. DA SUBCONTRATAÇÃO

a. Não será admitida a subcontratação do objeto.

08. MODELO DE EXECUÇÃO DO OBJETO

Em até, 30 dias, a contar da assinatura do contrato, as novas licenças deverão ser fornecidas e registradas em nome de CÂMARA MUNICIPAL DE FOZ DO IGUAÇU, nome fantasia PODER LEGISLATIVO, CNPJ 75.914.051/0001-28, atreladas a conta suporte@fozdoiguacu.pr.leg.br , dentro da plataforma da desenvolvedora Kaspersky Global.
Quando que realizada a disponibilização da licença, notificar via e-mail os responsáveis técnicos, sanches@fozdoiguacu.pr.leg.br e rodrigo@fozdoiguacu.pr.leg.br com detalhes do acesso.

09. MODELO DE GESTÃO DO CONTRATO E CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

A execução do objeto seguirá a seguinte dinâmica:

a. A contratante indicará Fiscal de contratos que irá acompanhar a execução do contrato em conformidade com este termo de referência.

b. O Contrato terá o prazo de 3 (três) anos, podendo ser prorrogado.

c. A Contratada formalizará a designação do preposto da empresa, especificando os poderes e responsabilidades relacionados à execução do objeto contratado.

d. Toda comunicação entre a Contratante e a Contratada deverá ser formalizada por escrito, especialmente quando exigido por lei, podendo ser realizada por meio de mensagem eletrônica, quando aplicável.

e. A execução será realizada de forma parcelada formalizada pelo envio da ordem de compra.

f. Os prazos e critérios para recebimento e pagamento estão detalhados nos itens 7.3 a 7.4.

g. Considera-se ocorrido o recebimento da nota fiscal quando a Gestão de contratos atestar a

execução do objeto do contrato através do termo de recebimento definitivo.

h. Não haverá exigência de garantia contratual da execução, devido às características da contratação.

i. A apresentação da Nota Fiscal/fatura é indispensável a cada fornecimento de bem ou serviço, para fins de liquidação e pagamento da despesa, emitida ao destinatário: Razão social: CÂMARA MUNICIPAL DE FOZ DO IGUACU; CNPJ: 75.914.051/0001-28; Endereço: Travessa Oscar Muxfeldt, nº 81, Centro, na cidade de Foz do Iguaçu-Paraná, CEP 85.851-490. Telefone: (45) 3521-8100.

j. Antes de cada pagamento à Contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

k. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se- á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

l. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

m. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

n. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 20 (vinte) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da Contratante.

o. Persistindo a irregularidade, a Contratante deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa.

p. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso a Contratada não regularize sua situação junto ao SICAF.

q. O prazo desta contratação será de 36 meses, contados da assinatura do contrato.

r. Pagamento:

i. Os pagamentos serão efetuados até o 10° (décimo) dia após o recebimento definitivo dos bens, condicionado a apresentação da Nota Fiscal/Fatura, bem como os documentos de regularidade fiscal, social e trabalhista exigidos pelo art. 68 da Lei n° 14.133/2021

ii. Na eventualidade de ocorrer atraso no pagamento, o valor será atualizado pela variação acumulada do IPCA/IBGE, ocorrida entre a data de seu adimplemento e a do efetivo pagamento, calculada pro rata tempore.

Sanções:

s. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei n° 14.133, de 2021, quais sejam:

t. Dar causa à inexecução parcial do contrato;

u. Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

v. Dar causa à inexecução total do contrato;

w. Deixar de entregar a documentação exigida para o certame;

x. Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

y. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

z. Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

aa. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

bb. Fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

cc. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

dd. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

ee. Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;

ff. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Multa de até 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor,

b) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver

c) aplicado a sanção, pelo prazo máximo de 3 (três) anos.

d) Direta, quando não se justificar a imposição de penalidade mais grave;

e) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 8.9 a bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

07. A fiscalização do contrato será realizada pelo servidor(a) designado:

08. A gestão do contrato será realizada pelo servidor (a) designado:

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço.

Tratamento diferenciado e favorecido a ser dispensado às microempresas, às empresas de pequeno porte e aos microempreendedores individuais conforme definido pelo documento de estudo técnico preliminar (ETP).

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

As quantidades previstas a serem adquiridas, conforme os itens descritos, são:

Item	Descrição	SKU	Quantidade	Valor Unit.	Valor
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160	R$ 358,19	R$ 57.310,40

A pesquisa de preço foi realizada considerando os parâmetros dispostos da Lei 14.133 no art. 23 § inciso IV – *"pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital"*. Do qual optou-se pelo menor preço ofertado.

Quanto à não utilização dos parâmetros dos § Incisos I e II do Art. 23, consultas no portal PNCP (Inciso I) e contratações similares feitas pela Administração Pública (II), conforme descrito no parágrafo anterior, torna-se ineficaz e escassa a busca por contratações similares em outros órgãos. Regendo-se pela economicidade, melhor tecnologia e melhores resultados pretendidos pelo órgão, a consulta aos fornecedores torna-se mais eficaz.

12. ADEQUAÇÃO ORÇAMENTÁRIA

ITEM	DOTAÇÃO

1	01.01.01.031.0001.2002.3.3.90.40.99.05 - AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE

Proc. Administrativo 19- 279/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: Envolvidos internos acompanhando

Data: 12/09/2024 às 14:54:34

Senhor Presidente da Câmara Municipal de Foz Do Iguaçu - CMFI-PRESID,

Considerando o despacho de número 16 contido no processo administrativo de número 279/2024, referente a renovação das licenças de antivírus desta casa de leis. Preliminarmente devemos avaliar os seguintes pontos.

Estão contidos nos autos os prazos de vigência da atual solução, por se tratar de uma ferramenta de segurança, torna-se evidente que **o vencimento destas licenças**, **incorre na interrupção do serviço, deixando toda infraestrutura de serviços e nossos usuários expostos as milhares de vulnerabilidades e riscos do mundo digital**, visando evitar todos esses problemas foi que esta diretoria instruiu o processo a mais de um mês. Em relação aos itens visando melhor interpretação dos fatos elencamos a mesma ordem do referido parecer, sendo assim, o primeiro item refere-se a um checklist realizado pela equipe de apoio em conjunto com o agente de contratações, sendo assim, os mesmos podem fazer manifestações, para tanto mencionamos o senhor CARLOS ALBERTO KASPER - AGCONT.

Quanto ao segundo item, esta diretoria esclarece que, conforme expresso nos autos, do ponto de vista técnico e econômico a melhor solução é a renovação, visando proteger o investimento anteriormente realizado, a atual solução já se encontra instalada, configurada e operante, já foram absorvidos custos de implantação treinamento e não menos importante é o conhecimento preexistente da equipe técnica, em virtude disto a busca não foi de uma nova solução, até mesmo por que não existe apontamentos que desabone a atual solução, afirmação da equipe técnica que compõe esta diretoria de Tecnologia.

O terceiro item aborda questões estruturais da redação, visando melhorar a escrita esta equipe técnica já realizou os ajustes sugeridos., esclarecemos ainda que o termo de referência foi assinado por outro membro da equipe em virtude da quantidade escassa de servidores que se encontram em férias e tratamento de saúde.

Por fim, o item de número quatro aponta ausência de justificativa quanto a metodologia aplicada na realização da pesquisa de preço, estando injustificada a pesquisa com fontes de banco de preços, nos causa estranheza pelo fato que o assunto é tratado no item 11 do TR, bem como no RPP.

–

Rafael Sanches
Diretoria de Tecnologia

Proc. Administrativo 20- 279/2024

De: CARLOS K. - CMFI-PRESID-DG-DIRFIN-COM-EC

Para: Envolvidos internos acompanhando

Data: 13/09/2024 às 10:17:00

Conforme requisitado no [Despacho 19] passo a relatar acerca da lista de verificação.

Trata-se de lista de verificação modelo obtida dos modelos da AGU para contratação de TIC. Foram removidas da lista menções a processos próprios do Governo Federal e mantidas apenas condições que se amoldam à rotina da Câmara Municipal e/ou tratam de boas praticas de contratações.
Passo a relatar apenas os itens identificados com "NÃO CUMPRE" na lista.

1. A Área de TIC avaliou o alinhamento da contratação ao PDTIC e ao Plano Anual de Contratações e indicou o Integrante Técnico para composição da Equipe de Planejamento da Contratação?
- Conforme identificado e já exaustivamente tratado, esta Casa de leis **não possui** PDTIC.

2. Há justificativa para o parcelamento ou não da solução de TIC?
- Conforme identificado na lista, há uma mera menção de que "não se aplica" o parcelamento no item 7 do ETP, não cumprindo a previsão do art. 4º do Ato da Presidência nº 133/2023

3. Há avaliação da viabilidade de permissão de consórcio ou subcontratação, com respectiva justificativa?
- Conforme modelo de ETP disponibilizado em 2023 pelo ato supra indicado, no item 7 devem: "Justificar eventual restrição de participação de empresas reunidas em consórcio e/ou cooperativas", não existindo menção no ETP disponibilizado. Registre-se que este item não possui natureza, até este momento, obrigatória pelos atos desta Casa de Leis, mas trata de rotina de boas práticas.

4. A forma de pagamento foi definida em função dos resultados?
- Trata-se de licenciamento de software, a forma de pagamento em função dos resultados, neste caso, não parece se aplicar.

5. Em caso de previsão de reajuste de preços por aplicação de índice, nas contratações de serviços de Tecnologia da Informação, foi previsto o índice de correção monetária ICTI (art. 24)
- O índice utilizado na minuta de contrato foi outro.

6. O Termo de Referência foi assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da área de TIC, com posterior aprovação pela autoridade competente?
- Trata-se de rotina de boas práticas visando o pleno atendimento da contratação com as tecnologias já implantadas na casa. Recomenda-se a ciência do senhor Diretor em todos os Termos de Referência envolvendo contratações de TI. A aprovação pela autoridade competente dar-se-á em momento oportuno.

7. Foi realizada análise de riscos, incluindo elaboração de Mapa de Gerenciamento de Riscos, devidamente assinado pela Equipe de
Planejamento da Contratação, cujas informações podem ser utilizadas como insumos para a construção da Matriz de Alocação de Riscos?
- Previsão do art. 18, X da Lei nº 14.133, não constando nenhuma análise de risco da contratação no ETP.
RESSALTO que o item possui natureza OPCIONAL no presente caso, devendo porém constar que a análise de riscos foi dispensada.

8. Caso o objeto contemple itens com valores inferiores a R$80.000,00, eles foram destinados às ME/EPPs e entidades equiparadas ou foi justificada a não exclusividade?
- Há justificativa apresentada para o NÃO neste item.

9. Foi certificado que foram priorizados na pesquisa de preços os sistemas oficiais de governo, como Painel de Preços ou banco de
preços em saúde, e contratações similares feitas pela Administração Pública, ou justificada a impossibilidade de utilização dessas fontes?
- Exigência do art. 6º, §1º do Ato da Presidência 136/2023

10.Caso realizada pesquisa direta com fornecedores, consta dos autos a relação de fornecedores que foram consultados e não enviaram propostas como resposta à solicitação feita?
- Art. 6º, §4º, IV do Ato da Presidência nº 136/2023

11. Há justificativa para não utilização de sistema de registro de preços?
- Previsão do art. 40, II da Lei nº 14133/2023

12. Caso o objeto contemple item de aquisição de bens de natureza divisível, com valor superior a R$80.000,00, foi prevista a cota
reservada ou justificada sua não previsão?
- Há justificativa identificada para o NÃO neste item.

São as considerações para o momento.

_

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras

Proc. Administrativo 21- 279/2024

De: CARLOS K. - CMFI-PRESID-DG-DIRFIN-COM-EC

Para: Envolvidos internos acompanhando

Data: 13/09/2024 às 10:22:12

Oportunamente, ressalto que o item 9 do despacho retro parece estar cumprido, porém, em instrumento diverso do qual deveria estar (Relatório de Pesquisa de Preços) eis que o Termo de Referência identificou a inviabilidade de utilização.

–

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras

Memorando 5.640/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: CMFI-PRESID - Presidência

Data: 02/10/2024 às 09:30:17

Prezado Presidente,

Informamos que o licenciamento da solução de proteção denominada antivírus expirou no dia 30 de setembro de 2024. No entanto, a Diretoria de Tecnologia tomou as providências necessárias e já realizou um pedido ao desenvolvedor da solução para o fornecimento de uma chave temporária, a qual terá validade até o dia 25 de outubro de 2024.

Adicionalmente, ressaltamos que a Diretoria de Tecnologia já instruiu o processo em 16/07/2024 para a renovação definitiva da solução de proteção, garantindo que todas as etapas necessárias estão sendo seguidas.

É importante destacar que, caso a renovação não seja efetivada até o término da validade da chave temporária, esta Casa de Leis estará vulnerável às ameaças do mundo virtual, o que pode comprometer a integridade das informações e a segurança dos dados tratados.

Permanecemos à disposição para quaisquer esclarecimentos.

Atenciosamente,

–

Rafael Sanches
Diretoria de Tecnologia

Assinado digitalmente (emissão) por:

Assinante	Data	Assinatura	
Rafael Sanches Alencar	02/10/2024 09:31:03	1Doc	RAFAEL SANCHES ALENCAR CPF 006.XXX.XXX-96
Rodrigo Nishimori	02/10/2024 09:33:27	1Doc	RODRIGO NISHIMORI CPF 007.XXX.XXX-01
Jeverson Siqueira	02/10/2024 09:48:15	1Doc	JEVERSON SIQUEIRA CPF 080.XXX.XXX-74
Robson Gregório	02/10/2024 09:58:20	1Doc	ROBSON GREGÓRIO CPF 784.XXX.XXX-53
Waldson de Almeida Dias	02/10/2024 11:16:34	1Doc	WALDSON DE ALMEIDA DIAS CPF 425.XXX.XXX-20

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **4859-F753-63DE-B001**

Memorando 1- 5.640/2024

De: Presidente I. - CMFI-PRESID

Para: CMFI-PRESID-DG - Assistente Técnico Diretoria Geral

Data: 02/10/2024 às 09:37:22

Ciente. Para ciência e providências.

_

João Morales

Presidente da Câmara Municipal de Foz do Iguaçu

Memorando 2- 5.640/2024

De: FABIANO B. - CMFI-PRESID-DG

Para: Envolvidos internos acompanhando

Data: 02/10/2024 às 10:20:13

Ciente. A demanda será tratada diretamente no Proc. Administrativo 279/2024 - PL - Fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 meses

Att,

–

Fabiano Borghetti

Assistente Técnico da Direção Geral

Proc. Administrativo 22- 279/2024

De: FABIANO B. - CMFI-PRESID-DG

Para: CMFI-DG-DIRTEC - Diretoria de Tecnologia

Data: 02/10/2024 às 13:03:37

Setores (CC):

CMFI-DG-DIRTEC, CMFI-PRESID-DG-DIRFIN-COM, CMFI-PRESID-DG-DIRFIN-GESTCON

Ciente. Trata-se de demanda para a contratação de empresa para a renovação de licenças de antivírus com *upgrade,* visando melhorias.

O Processo Administrativo nº 243/2024, iniciado em 16/07/2024, foi instruído e, posteriormente substituído pelo presente Processo Administrativo nº 279/2024, datado de 06/08/2024.

Após a instrução, com a confecção, retificação e ratificação de documentos necessários para a contratação, resultando na tramitação em 21 despachos, além de outras movimentações internas, o processo chega para o Assistente Técnico da Direção Geral e para a Presidência da Câmara de Vereadores de Foz do Iguaçu para análise e considerações, diante das ressalvas apontadas.

É breve a síntese do processo.

Preliminarmente, com relação ao encaminhamento à Direção Geral, saliento que se trata de demanda estratégica da gestão que, apesar de não finalizado o planejamento estratégico deste órgão, nem mesmo o Plano Diretor de Tecnologia da Informação (PDTI), em virtude da alta demanda e de todas as mudanças implementadas nestes últimos 21 (vinte e um) meses, têm se dedicado a modernização do Poder Legislativo, inclusive com a melhoria dos serviços prestados à Casa de Leis, visando dar estrutura adequada de trabalho aos Vereadores, Assessores e Servidores.

No #Memorando nº 5.640/2024 a Diretoria de Tecnologia cientifica a preocupação com a não contratação e continuidade do referido processo, assim manifestando:

"*Informamos que o licenciamento da solução de proteção denominada antivírus expirou no dia 30 de setembro de 2024. No entanto, a Diretoria de Tecnologia tomou as providências necessárias e já realizou um pedido ao desenvolvedor da solução para o fornecimento de uma chave temporária, a qual terá validade até o dia 25 de outubro de 2024.*

Adicionalmente, ressaltamos que a Diretoria de Tecnologia já instruiu o processo em 16/07/2024 para a renovação definitiva da solução de proteção, garantindo que todas as etapas necessárias estão sendo seguidas.

É importante destacar que, caso a renovação não seja efetivada até o término da validade da chave temporária, esta Casa de Leis estará vulnerável às ameaças do mundo virtual, o que pode comprometer a integridade das informações e a segurança dos dados tratados."

Sabedores são os Servidores da Casa de Leis que já sofreram ataque cibernético e tiveram diversos dados e documentos danificados e perdidos, o que gerou um transtorno incalculável em todos os setores.

Com relação ao processo, este foi devidamente instruído, restando pendente algumas adequações solicitadas pela Diretoria Jurídica, conforme Despacho 16, de 10/09/2024, itens 1 a 4.

No Despacho 19 foram analisados e justificados os itens 2 a 4 do Despacho 16.

Ainda, no Despacho 20, foram justificados item a item os apontamentos da lista de verificação.

Dadas as observações, a Direção Geral entende conveniente a manutenção da contratação, pelo que passamos a expor:

Como mencionado, atualmente a CMFI conta com diversos softwares e é totalmente dependente do ambiente virtual, que ficaram inoperantes em caso de ataques, ou seja, em caso de invasão todos os trabalhos ficam inoperantes e o prejuízo poderá ser irreversível. Destacada a importância de tal serviço, vale mencionar que atualmente o quadro de pessoas que utilizam esse mesmo serviço conta com 15 Vereadores, 60 Assessores, 8 Cargos em Comissão, 52 Servidores Efetivos, 6 Estagiários e 16 terceirizados diariamente. A estrutura física atual (sem mencionar eventuais ampliações) atende em torno de 100 equipamentos de informática fixos, sem contabilizar os dispositivos móveis.

Insta mencionar, também, que a Diretoria de Tecnologia, área especializada, é detentora de capacidade técnica para dimensionar a demanda e as necessidades atuais e futuras e, diante disso, a melhor alternativa para a solução e atendimento, o que deve ser considerado.

Ainda, amplamente dissertado e debatido é que a melhor contratação para os órgãos públicos não são aquelas com o menor preço, mas sim, aquelas que efetivamente atendam a necessidade da demanda que se pretende suprir com a compra/contratação.

Diante do exposto, após reunião com as áreas envolvidas, Encaminho o processo à Diretoria demandante para retificação dos documentos, ao Gestor de Contratos e após ao Setor de Compras para as mesmas providências, com sequência de encaminhamento à Diretoria Jurídica, observando a URGÊNCIA que o caso requer.

Por fim, ressalto que não foram apontados irregularidades ou ilegalidades, mas sim ressalvas de ordem formal, merecendo o prosseguimento.

Att,

–

Fabiano Borghetti

Assistente Técnico da Direção Geral

Proc. Administrativo (Nota interna 02/10/2024 13:35) 279/2024

De: José T. - CMFI-PRESID-DG-DIRFIN-GESTCON

Para: Envolvidos internos acompanhando

Data: 02/10/2024 às 13:35:43

Segue uma via atualizada do Termo de Contrato, conforme despacho 22.

_

José Marcelo Nicoletti Teixeira,
Consultor Técnico Legislativo.

Anexos:

Minuta_Contrato_XX_2024_antivirus.pdf

M I N U T A

CONTRATO Nº 19/2024

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS, QUE FAZEM ENTRE SI A CÂMARA MUNICIPAL DE FOZ DO IGUAÇU E A EMPRESA XXXXXXXXXXXXXXXXXX.

A **Câmara Municipal de Foz do Iguaçu**, pessoa jurídica de direito público, com sede em Foz do Iguaçu, Estado do Paraná, situada na Travessa Oscar Muxfeldt, 81, Centro, inscrita no CNPJ/MF sob o nº 75.914.051/0001-28, neste ato representada por seu Presidente, João José Arce Rodrigues, consoante competência originária prevista no art. 17 do Regimento Interno da Câmara Municipal de Foz do Iguaçu, daqui para frente denominada simplesmente de **CONTRATANTE,** e, de outro lado, a empresa XXXXXXXXXXXXXXXXXXXXXX, inscrita no CNPJ/MF sob o nº XXXXXXXXX/XXXX-XX, situado na XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, cidade de XXXXXXXXXX, Estado XXXXXXXXX, CEP: XX.XXX-XXX, representada por seu representante legal XXXXXXXXXXXXXXXXXXXXX, inscrito junto ao CPF/MF sob n. XXXXXXXXXX, a seguir denominada simplesmente **CONTRATADA**, firmam o presente contrato, sujeitando-se às cláusulas a seguir expostas e às normas da Lei n. 14.133/2021, têm entre si justo e contratado o que segue:

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O objeto do presente contratação de empresa especializada e tecnicamente qualificada para o fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 meses, de acordo com as características e especificações técnicas e, quantitativos descritos em termo de referência, bem como em seus anexos, conforme descrição a seguir:

ITEM	CAT/MAT	DESCRIÇÃO	QUANT.	UNIDADE	VALOR UNIT.	VALOR TOTAL
1	350949	KASPERSKY NEXT EDR OPTIMUM	160	Uni	R$ XXXXX,XX	R$ XXXXXX,XX
TOTAL						R$ XXXXXX,XX

2. CLÁUSULA SEGUNDA – DA VINCULAÇÃO

2.1. Os Contraentes reconhecem a vinculação desta contratação aos termos do Pregão Eletrônico n. XX/XXXX, emitido pela CONTRATANTE e à respectiva proposta que for vencedora, sendo que as

especificações técnicas mínimas do objeto, a fundamentação da contratação, a descrição da solução como um todo, as condições da garantia, os requisitos de habilitação, qualificação, técnica e capacidade operacional e de fornecimento, os requisitos da contratação, dentre outras informações, estão constantes em Termo de Referência, que é parte integrante deste Contrato independentemente de sua transcrição, ao qual também se declaram vinculados os contraentes.

3. CLÁUSULA TERCEIRA – DA LEGISLAÇÃO APLICÁVEL E DOS CASOS OMISSOS

3.1. Aplica-se a Lei n. 14.133/2021 à execução deste Contrato, sendo esta também a legislação a ser aplicadas aos casos omissos.

4. CLÁUSULA QUARTA – DO REGIME DE EXECUÇÃO

4.1. Os serviços serão executados sob o regime de execução indireta.

4.2. A execução dos serviços especificados neste Contrato e em Termo de Referência deverá ter início em até 30 dias, contados da assinatura do contrato, mediante fornecimento das licenças registradas em nome da CÂMARA MUNICIPAL DE FOZ DO IGUAÇU, nome fantasia PODER LEGISLATIVO, CNPJ n. 75.914.051/0001-28, atreladas a conta suporte@fozdoiguacu.pr.leg.br, dentro da plataforma da desenvolvedora Karpersky Global.

4.2. Quando realizada a disponibilização da licença, notificar via e-mail os responsáveis técnicos, sanches@fozdoiguacu.pr.leg.br e rodrigo@fozdoiguacu.pr.leg.br com detalhes do acesso.

4.3. Os serviços de instalação e manutenção deverão ser realizados na sede administrativa da CONTRATANTE, no endereço Travessa Oscar Muxfeldt, 81 - Centro, Foz do Iguaçu - PR, 85851-490

4.4. Os serviços a serem contratados constituem-se em atividades materiais acessórias, instrumentais ou complementares à área de competência legal da CONTRATANTE, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

4.5. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e a Administração, vedando-se qualquer relação entre elas que caracterize pessoalidade e subordinação direta.

4.6. Os serviços contratados são enquadrados como continuados, tendo em vista a sua necessidade permanente para a CONTRATANTE.

5. CLÁUSULA QUINTA – PREÇO

5.1. Em contra partida aos serviços prestados a CONTRATANTE pagará à CONTRATADA o valor mensal de até R$ XXXXX, totalizando estimativa de pagamento anual de até R$ XXXXX, conforme descrito na proposta apresentada pela empresa e constante no processo administrativo.

5.2. No valor indicado estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, seguro e outros necessários ao cumprimento integral do objeto da contratação.

6. CLÁUSULA SEXTA – DO REAJUSTE

6.1. Mediante expresso pedido da CONTRATADA, os valores contratados poderão ser reajustados a cada 12 (doze) meses, contados a partir da data da proposta apresentada pela CONTRATADA, com aplicação do índice de variação do ICTI – Índice de Custo da Tecnologia da Informação, calculado pelo IPEA, para o mesmo período ou outro índice que o substitua.
6.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de 12 (doze) meses para a próxima reajustamento, será contado a partir dos efeitos financeiros do último reajuste.
6.3. O reajuste previsto nesta cláusula poderá ser formalizado por Termo de Apostilamento.

7. CLÁUSULA SÉTIMA – DOS CRITÉRIOS DE MEDIÇÃO
7.1. Os Materiais entreguem dever estar em conformidade com as quantidades solicitadas dos itens já descritos neste documento;
7.2. A qualidade exigida dos equipamentos e materiais utilizados tem que estar de acordo com a qualidade de cada item, sendo vedada a utilização de materiais de qualidade inferior ou de não garantia.
7.3. Todos os pontos instalados devem ser certificados para assim constatar a qualidade do serviço e garantia de transmissão do mesmo.
7.4. Dos demais todos os itens devem ser novos seguidos rigidamente as especificações mínimas descritas na seção Requisitos da Contratação e amparados em seu prazo de garantia estabelecidos.

8. CLÁUSULA OITAVA – DO RECEBIMENTO
8.1. Os serviços serão recebidos provisoriamente no prazo de 05 (cinco) dias, para efeito de posterior verificação de sua conformidade com as especificações constantes na proposta;
8.2. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes na proposta, devendo ser substituídos no prazo de 10 (dez) dias, a contar da notificação da CONTRATANTE, às suas custas, sem prejuízo da aplicação das penalidades;
8.3. Na impossibilidade de realização dos serviços, a empresa vencedora deverá substituir o serviço por outro com especificações iguais ou superiores;
8.4. Os serviços serão recebidos definitivamente no prazo de 10 (dez) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação;
8.5. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo;
8.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

9. CLÁUSULA NONA – DO PAGAMENTO
9.1. Os pagamentos serão efetuados até o 10º (décimo) dia após o recebimento definitivo dos produtos/serviços, condicionado a apresentação da Nota Fiscal/Fatura, bem como os documentos de regularidade fiscal, social e trabalhista exigidos pelo art. 68 da Lei nº 14.133/2021.
9.2. Na eventualidade de ocorrer atraso no pagamento, o valor será atualizado pela variação acumulada do IPCA, ocorrida entre a data de seu adimplemento e a do efetivo pagamento, calculada pro rata tempore.

9.3. A apresentação da nota fiscal/fatura é indispensável a cada entrega de produtos ou prestação de serviços, para fins de liquidação e pagamento da despesa, a ser emitida ao destinatário: Razão social: CÂMARA MUNICIPAL DE FOZ DO IGUACU; CNPJ: 75.914.051/0001-28; Endereço: Travessa Oscar Muxfeldt, nº 81, Centro, na cidade de Foz do Iguaçu-Paraná, CEP 85.851-490. Telefone: (45) 3521-8100.
9.4. Antes de cada pagamento à CONTRATADA, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.
9.5. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se- á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.
9.6. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
9.7. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.
9.8. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua notificação, por escrito, para que, no prazo de 15 (quinze) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.
9.9. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.
9.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso a CONTRATADA não regularize sua situação junto ao SICAF.
9.11. O prazo desta contratação será de 36 meses, contados da assinatura do contrato.

10. CLÁUSULA DÉCIMA – DO PRAZO PARA RESPOSTA AOS PEDIDOS DE REPACTUAÇÃO DE PREÇOS E RESTABELECIMENTO DO EQUILÍBRIO ECONÔMICO

10.1. Quando for o caso de repactuação de preços e/ou de restabelecimento do equilíbrio econômico deste Contrato, será de 30 dias úteis o prazo resposta da CONTRATANTE, a contar da data de formalização do pedido por parte da CONTRATADA.

11. CLÁUSULA DÉCIMA PRIMEIRA - DA INEXIGÊNCIA DE GARANTIAS À EXECUÇÃO DO CONTRATO

11.1. Dadas as características da contratação, não haverá exigência de garantia à execução do contrato.

12. CLÁUSULA DÉCIMA SEGUNDA – DA GARANTIA DOS PRODUTOS E SERVIÇOS

12.1. As empresas licitantes deverão indicar o prazo da garantia do Software ou licença, que deverá ser de 36 meses oferecido diretamente ou com a autorização e responsabilidade do fabricante, sendo este o período em que se obrigam a prestar a manutenção e assistência técnica gratuita, nos termos regulados em termo de referência.

12.2. Serão desclassificadas as propostas que não ofereçam prazo de garantia ou abaixo do mínimo estipulado. As empresas licitantes indicarão, SOB PENA DE DESCLASSIFICAÇÃO, informações relacionadas à PADRONIZAÇÃO e COMPATIBILIDADE da solução, conforme detalhamento no ETP.

13. CLÁUSULA DÉCIMA TERCEIRA – DOTAÇÃO ORÇAMENTÁRIA

13.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da Câmara Municipal, para o exercício de 2024 nas classificações: item 1 – 01.01.01.031.0001.2002.3.3.90.40.99.05 – AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE.

13.2. Nos exercícios seguintes, correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

14. CLÁUSULA DÉCIMA QUARTA – DAS OBRIGAÇÕES DA CONTRATANTE

14.1. A CONTRATANTE obriga-se a:

14.1.1. Comunicar à Contratada quaisquer irregularidades nos equipamentos, para adoção das providências cabíveis;

14.1.2. Designar funcionário para acompanhar/fiscalizar a entrega;

14.1.3. Efetuar os pagamentos relativos ao presente contrato em moeda corrente quando da apresentação da fatura de serviços executados respeitando os prazos de vencimentos;

14.1.4. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;

14.1.5. Qualquer alteração deste, somente deverá ser com o aval dos gestores do contrato;

14.1.6. Aplicar a contratada as sanções administrativas regulamentares e contratuais cabíveis.

15. CLÁUSULA DÉCIMA QUINTA – DAS OBRIGAÇÕES DA CONTRATADA

15.1. A CONTRATADA obriga-se a:

15.1.1. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

15.1.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do contrato, inerentes à execução do objeto contratual;

15.1.3. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

15.1.4. É de responsabilidade da CONTRATADA, manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob

qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

16. CLÁUSULA DÉCIMA SEXTA – DAS SANÇÕES ADMINISTRATIVAS

16.1. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei n° 14.133, de 2021, quais sejam:

16.1.1. Dar causa à inexecução parcial do contrato;

16.1.2. Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

16.1.3. Dar causa à inexecução total do contrato;

16.1.4. Deixar de entregar a documentação exigida para o certame;

16.1.5. Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

16.1.6. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

16.1.7. Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

16.1.8. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

16.1.9. Fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

16.1.10. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

16.1.11. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

16.1.12. Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;

16.1.13. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

16.1.13.1. Multa de até 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor;

16.1.15. Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, quando não se justificar a imposição de penalidade mais grave;

16.1.16. Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 16.1.8 e bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

16.2. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao fornecedor.

17. CLÁUSULA DÉCIMA SÉTIMA - DA OBRIGAÇÃO DE MANUTENÇÃO DAS CONDIÇÕES DE QUALIFICAÇÃO

17.1. A CONTRATADA obriga-se a manter, durante toda a execução do Contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições para a qualificação na contratação direta que precedeu a este instrumento;

18. CLÁUSULA DÉCIMA OITAVA - DA OBRIGAÇÃO DE RESERVA DE CARGOS PREVISTA EM LEI

18.1. A CONTRATADA, durante toda a execução do Contrato, obriga-se a cumprir as exigências de reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz.

19. CLÁUSULA DÉCIMA NONA – MODELO DE GESTÃO DO CONTRATO

19.1. A execução do objeto seguirá a seguinte dinâmica:

19.1.1. A contratante indicará Fiscal de contratos que irá acompanhar a execução do contrato em conformidade com este termo de referência.

19.1.2. O Contrato terá o prazo de 3 (três) anos, podendo ser prorrogado.

19.1.3. A Contratada formalizará a designação do preposto da empresa, especificando os poderes e responsabilidades relacionados à execução do objeto contratado.

19.1.4. Toda comunicação entre a Contratante e a Contratada deverá ser formalizada por escrito, especialmente quando exigido por lei, podendo ser realizada por meio de mensagem eletrônica, quando aplicável.

19.1.5. A execução será realizada de forma parcelada formalizada pelo envio da ordem de compra.

19.1.6. Os prazos e critérios para recebimento e pagamento estão detalhados nas cláusulas 7 a 9 retro.

19.1.7. Considera-se ocorrido o recebimento da nota fiscal quando a Gestão de contratos atestar a execução do objeto do contrato através do termo de recebimento definitivo.

19.1.8. Não haverá exigência de garantia contratual da execução, devido às características da contratação.

20. CLÁUSULA VIGÉSIMA – DA INEXECUÇÃO E DA EXTINÇÃO DO CONTRATO

20.1. A inexecução total ou parcial do contrato ensejará a sua extinção com as consequências contratuais e as previstas em lei, com fulcro no Título III, Capítulo VIII da Lei n. 14.133/2021, nos seguintes modos:

20.1.1. determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta;

20.1.2. consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração;

20.1.3. determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

20.2. Constituirão motivos para extinção do contrato, a qual deverá ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa, as seguintes situações:

20.2.1. não cumprimento ou cumprimento irregular de normas editalícias ou de cláusulas contratuais, de especificações, de projetos ou de prazos;

20.2.2. desatendimento das determinações regulares emitidas pela autoridade designada para acompanhar e fiscalizar sua execução ou por autoridade superior;
20.2.3. alteração social ou modificação da finalidade ou da estrutura da empresa que restrinja sua capacidade de concluir o contrato;
20.2.4. decretação de falência ou de insolvência civil, dissolução da sociedade ou falecimento do contratado;
20.2.5. caso fortuito ou força maior, regularmente comprovados, impeditivos da execução do contrato;
20.2.6. atraso na obtenção da licença ambiental, ou impossibilidade de obtê-la, ou alteração substancial do anteprojeto que dela resultar, ainda que obtida no prazo previsto;
20.2.7. atraso na liberação das áreas sujeitas a desapropriação, a desocupação ou a servidão administrativa, ou impossibilidade de liberação dessas áreas;
20.2.8. razões de interesse público, justificadas pela autoridade máxima do órgão ou da entidade CONTRATANTE.
20.3. O descumprimento, por parte da CONTRATADA, de suas obrigações legais e/ou contratuais assegurará ao CONTRATANTE o direito de extinguir o contrato a qualquer tempo, independentemente de aviso, interpelação judicial e/ou extrajudicial.
20.4. A extinção por ato unilateral do CONTRATANTE sujeitará a CONTRATADA à multa rescisória de até 10% (dez por cento) sobre o valor do saldo do contrato existente na data da extinção, independentemente de outras penalidades.
20.5. Caso o valor do prejuízo do CONTRATANTE advindo da extinção contratual por culpa da CONTRATADA exceder o valor da Cláusula Penal prevista no parágrafo anterior, esta valerá como mínimo de indenização, na forma do disposto no art. 416, parágrafo único, do Código Civil.
20.6. A extinção determinada por ato unilateral da Administração e a extinção consensual deverão ser precedidas de autorização escrita e fundamentada da autoridade competente e reduzidas a termo no respectivo processo.
20.7. A CONTRATANTE poderá rescindir o presente instrumento contratual, sem qualquer ônus à Administração, quando da conclusão de eventual novo procedimento de contratação de interesse público para objeto afim.

21. CLÁUSULA VIGÉSIMA PRIMEIRA – DA VIGÊNCIA

21.1. O presente Contrato terá validade de 36 (trinta e seis) meses, contados da data da assinatura, podendo ser prorrogado, a critério da Administração, conforme o disposto no art. 107, da Lei n. 14.133/2021 e suas alterações posteriores.
21.2. A prorrogação deste contrato deverá ser promovida mediante celebração de termo aditivo.

22. CLÁUSULA VIGÉSIMA SEGUNDA – DA FISCALIZAÇÃO

22.1. O acompanhamento e a fiscalização da execução das obrigações oriundas deste contrato ficarão a cargo do Gestor José Marceo Nicoletti Teixeira, e do Fiscal de Contratos, Jeverson Siqueira, e consiste na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais

representantes da CONTRATANTE, especialmente designados, na forma do art. 117 da Lei nº 14.133/2021.

22.2. O fiscal do contrato deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 117 da Lei nº 14.133/2021.

22.3. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela CONTRATADA ensejará a aplicação de sanções administrativas, previstas neste Termo de Contrato e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 156 e 137 da Lei nº 14.133/2021.

22.4. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da CONTRATANTE ou de seus agentes e prepostos, de conformidade com art. 120 da Lei nº 14.133/2021.

23. CLÁUSULA VIGÉSIMA TERCEIRA – DA SUBCONTRATAÇÃO

23.1. É vedada a subcontratação total ou parcial do objeto deste Termo de Contrato.

24. CLÁUSULA VIGÉSIMA QUARTA – DAS VEDAÇÕES

24.1. É vedado à CONTRATADA:

24.1.1. Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;

24.1.2. Interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

25. CLÁUSULA VIGÉSIMA QUINTA – DAS ALTERAÇÕES

25.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos art. 124 a 136 da Lei n. 14.133/2021.

26. CLÁUSULA VIGÉSIMA SEXTA – DA PUBLICAÇÃO

26.1. A CONTRATANTE providenciará a publicação deste contrato no Diário Oficial do Município de Foz do Iguaçu, na página da Câmara Municipal de Foz do Iguaçu nos termos do art. 174 da Lei n. 14.133/2021 e no Portal Nacional de Contratações Públicas (PNCP), para fins de garantia a ampla publicidade.

27. CLÁUSULA VIGÉSIMA SÉTIMA – DO FORO

27.1. Fica eleito o foro desta cidade de Foz do Iguaçu, Estado do Paraná, para dirimir toda e qualquer questão que derivar deste contrato.

E por estarem justas e acordadas, assinam as partes o presente instrumento, na presença de duas testemunhas, que também o subscrevem, para que surtam todos os efeitos jurídicos e legais.

Foz do Iguaçu, xx de xxxxx de 2024.

CÂMARA MUNICIPAL DE FOZ DO IGUAÇU
João José Arce Morales

XXXXXXXXXXX
xxxxxxxxxxx

Testemunhas:

_____
Nome: XXXXXX
RG: XXXXXX
CPF: XXXXXXX

_____
Nome: XXXXXXXXX
RG: XXXXXXX
CPF XXXXXX

Proc. Administrativo 23- 279/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: Envolvidos internos acompanhando

Data: 02/10/2024 às 15:32:06

O despacho foi cancelado em 03/10/2024 08:03:10 por Rafael Sanches Alencar (CPF 006.XXX.XXX-96).
A justificativa do cancelamento consta no despacho proc. administrativo 25- 279/2024

Proc. Administrativo 23- 279/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: Envolvidos internos acompanhando

Data: 02/10/2024 às 15:32:06

Documento ETP atualizado para assinatura.

–

Rafael Sanches
Diretoria de Tecnologia

ESTUDO TÉCNICO PRELIMINAR

1) DESCRIÇÃO DA NECESSIDADE

1.1. Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

1.2. A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

1.3. Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

1.4. Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

1.5. Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

1.6. Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

1.7. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.

2) REQUISITOS DA CONTRATAÇÃO

Item	Descriçao	SKU	Quantidade
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160

3) LEVANTAMENTO DE MERCADO

Considerando que a Câmara Municipal de Foz do Iguaçu já dispõe de um sistema de antivírus, foram avaliadas duas alternativas sendo uma delas a renovação e upgrade de versão do sistema e a outra a aquisição de um sistema integrado com o nosso sistema de Firewall.

Mantendo os investimentos ocorridos no ano de 2018 (R$ 11.635) e 2021 (R$ 31.217,00 (Preço médio)) e já realizados, tendo em vista de que além da aquisição do sistema, foi também realizada no ano de 2023 (R$ 6.980,00) a contratação de uma empresa especializada para nos auxiliar na configuração recomendadas pelo fabricante, e com base nas pesquisa de preços e estudo entre outras soluções, por medida de economicidade optou-se pela renovação com upgrade da versão já utilizada do licenciamento da solução Kaspersky e aquisição de novas licenças de acordo com a

necessidade da CMFI , levando em consideração a ampliação do parque computacional que ocorreu nesses últimos anos e demandas futuras.

Notou-se ainda que a linha de produtos do desenvolvedor da solução passou por atualizações entregando novas versões de sua solução bem como mais recursos, a título de exemplo temos, portais de capacitação na solução, canais de suporte e a adoção da inteligência artificial para detecção e mitigação de vulnerabilidades.

4) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

As especificações do objeto desta licitação deverão estar detalhadas no termo de referência elaborado com base neste estudo técnico preliminar e de acordo com a solicitação elaborada pelo setor demandante.

5) ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

Item	Descrição	SKU	Quantidade	Valor
1	KASPERSKY NEXT EDR OPTIMUM 36 meses	KL4066KASTJ	160	R$ 57.310,40

Descrição Item 1

A solução deve incluir treinamento em segurança cibernética

Do módulo de proteção de endpoint

Compatibilidade com diferentes sistemas operacionais, MAC OS, Linux de 32 e 64 bits (CentOS, Red Hat Enterprise, Debian, Ubuntu, Oracle Linux), Windows 7, 8, 8.1, 10,11 para desktops, para servidores S.O Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022, Windows Small Business Server 2011, Servidores de terminal Microsoft (Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022).

Módulo de gerenciamento avançado

A solução deve suportar arquitetura cloud-native e on-premisse, a solução deve incluir suporte para implantação baseada em nuvem (Amazon Web Services e/ou Microsoft Azure. Integração nativa com as seguintes opções de SIEM (HP (Microfoco) ArcSight, IBM QRadar, Splunk, Kaspersky KUMA). 2.4.

A solução deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

A solução deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

A solução deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.
A solução deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.
O servidor de gerenciamento primário da solução deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.
A solução deve suportar os seguintes canais de entrega de notificação, E-mail, registro de sistema e SMS ou equivalente.
A solução deve ter a capacidade de etiquetar/marcar computadores com base em
Atributos de rede, Nome, Domínio e/ou Sufixo de Domínio, Endereço de IP, Endereço IP para servidor de gerenciamento, Localização no Active Directory, Unidade organizacional, Grupo, Sistema operacional, Número do pacote de serviço, Arquitetura Virtual, Registro de aplicativos, Nome da Aplicação, Versão do aplicativo, Fabricante, Tipo e versão, Arquitetura.
A solução deverá permitir especificamente o bloqueio dos seguintes dispositivos, Bluetooth, Dispositivos móveis, Modems externos, CD/DVD, Câmeras e scanners.
A solução deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.
A solução deve permitir realizar as seguintes ações para endpoints, verificação manual, verificação no acesso, verificação por demanda, verificação de arquivos compactados, verificação de arquivos individuais, pastas e unidades, bloqueio e verificação de scripts, proteção contra alteração de registros, proteção contra estouro de buffer, verificação em segundo plano/inativa.

A solução deverá suportar os seguintes servidores de banco de dados:
Windows,

- Microsoft SQL Server
- Microsoft Banco de dados SQL do Azure
- MySQL Standard e Enterprise
- MariaDB
- PostgreSQL

Linux:

- MySQL
- MariaDB

- PostgreSQL

A solução deverá suportar as seguintes plataformas virtuais:

Windows:

- VMware vSphere 6.7 e 7.0
- Estação de trabalho VMware 16 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Oracle VM VirtualBox 6.x

2.74.2. Linux:

- VMware vSphere 6.7, 7.0 e 8.0
- VMware Desktop 16 Pro e 17 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 e 8.x

Do módulo de gerenciamento simplificado

A solução deve suportar arquitetura cloud;

A solução deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

A solução deve permitir ao administrador gerar relatórios pré-definidos.

A solução deve incluir informações do endpoint, IP público de internet, IP interno do dispositivo, Versão do agente de proteção, ultima comunicação com a console, contendo data e hora, informações do sistema operacional;

Requisitos gerais

A solução deve ser capaz de detectar os seguintes tipos de ameaças:
Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.
A solução deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
A solução deve ter capacidade de integração com a central de segurança do Windows Defender.
A solução deve suportar o subsistema Linux no Windows.
A solução deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

- Proteção contra ameaças sem arquivos (Fileless);
- Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

Do modulo de gerenciamento de dispositivos móveis

O modulo deve ser integrado a console de gerenciamento;
A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

- Android 5.0 ou posterior (incluindo Android 12L)

A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

- iOS 10–17 ou iPadOS 13–17

A solução deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

Do módulo de EDR

Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
A solução deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;

Deve apresentar informações detalhadas contendo:

- Usuário que executou a ação;
- Informações acesso privilegiado;

A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.

O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único).

6) IMPACTOS AMBIENTAIS

Não foram identificados impactos ambientes nesta contratação

7) JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Não se aplica, trata-se de um único item.

8) CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

Não se identificou contratações interdependentes e/ou correlatas, sendo que a prestação dos serviços depende exclusivamente do presente procedimento.

9) ALINHAMENTO COM PAC – PLANO ANUAL DE CONTRATAÇÕES

A demanda em questão encontra-se prevista no plano anual de contratações. Considerando que o mapa de gerenciamento de riscos tem natureza opcional, conforme previsto na NLL 14.133 e ato da presidência 133/2023.

10) RESULTADOS PRETENDIDOS

- Garantir um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;
- Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo estações de trabalho e notebooks comprometidos;
- Evitar, mitigar e conter a propagação de pragas digitais (vírus/malwares/spywares, spam, entre outros) com a administração centralizada da solução de proteção;

- Permitir o controle de acesso à rede por dispositivos computacionais, permitindo gerenciamento destes dispositivos;
- Possibilitar análise pormenorizada de arquivos, discos rígidos, unidades móveis, mensagens de e-mail e anexos, viabilizando detecção de ameaças, com intento de salvaguardar a estrutura tecnológica de ataques com teor e objetivo malicioso;
- Possibilitar o controle de acesso e tráfego de informações aos dispositivos e serviços operacionais na rede, através de gerenciamento centralizado, o que vem a complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;
- Aprimorar a segurança de TIC da CMFI frente a ameaças sofisticadas.

11) PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Tendo em vista que nosso ambiente de tecnologia já possui uma solução de firewall, não será necessária nenhuma providência prévia.

12) VIABILIDADE DA CONTRATAÇÃO

Esta equipe de TI declara viável esta contratação

13) TRATAMENTO DIFERENCIADO E FAVORECIDO A SER DISPENSADO ÀS MICROEMPRESAS, ÀS EMPRESAS DE PEQUENO PORTE E AOS MICROEMPREENDEDORES INDIVIDUAIS

Após diversas tentativas de localização e contato com empresas qualificadas como microempresas (ME) e empresas de pequeno porte (EPP) na região de Foz do Iguaçu para fornecimento das licenças, constatou-se a inexistência, inclusive pelo embasamento da pesquisa na base de de empresas credenciadas junto ao portal do desenvolvedor, acessado na data de 10/06/2024 às 09:38. Durante o processo de prospecção, entramos em contato direto com diversas empresas locais, incluindo aquelas registradas como ME e EPP, para verificar a capacidade técnica e a disponibilidade para fornecimento do serviço requerido. Nenhuma das ME/EPP contactadas demonstrou capacidade técnica ou interesse em participar do certame.

Diante dessas circunstâncias, a manutenção da exclusividade do certame para ME e EPP pode inviabilizar a contratação, comprometendo a eficiência e a continuidade dos serviços públicos dependentes de uma conexão estável e de alta velocidade, eis que

há sério risco da licitação ser deserta. Ressalta-se, porém, que as ME/EPP ainda poderão participar do certame com vantagens sobre os demais concorrentes conforme versa a legislação pátria.

Portanto, justifica-se o afastamento da exclusividade de participação de microempresas e empresas de pequeno porte neste certame específico, com base na inexistência de fornecedores locais qualificados e na necessidade imperiosa de garantir a prestação adequada e contínua dos serviços públicos.

14) RESPONSÁVEIS PELA ELABORAÇÃO DO ETP

Jeverson Siqueira
Cargo: Tecnico de Informatica
Matrícula: 202.045
Setor: Diretoria de Tecnologia

Proc. Administrativo 24- 279/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: Envolvidos internos acompanhando

Data: 02/10/2024 às 15:34:14

O despacho foi cancelado em 03/10/2024 08:03:32 por Rafael Sanches Alencar (CPF 006.XXX.XXX-96).
A justificativa do cancelamento consta no despacho proc. administrativo 26- 279/2024

Proc. Administrativo 24- 279/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: Envolvidos internos acompanhando

Data: 02/10/2024 às 15:34:14

Documento RPP atualizado para assinatura.

–

Rafael Sanches
Diretoria de Tecnologia

RELATÓRIO DE PESQUISA DE PREÇOS, PLANILHA COMPARATIVA E DOCUMENTAÇÃO COMPROBATÓRIA

INTRODUÇÃO

O presente relatório é resultado da pesquisa de preços abaixo discriminada em cumprimento ao determinado na Lei nº 14.133/2021 em conformidade com o Ato da Presidência nº 136/2023.

AGENTE RESPONSÁVEL PELA PESQUISA: Rafael Sanches Alencar

OBJETO: Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses

MÉTODO ESTATÍSTICO APLICADO COM JUSTIFICATIVAS PARA A METODOLOGIA UTILIZADA, EM ESPECIAL PARA A DESCONSIDERAÇÃO DE VALORES INCONSISTENTES, INEXEQUÍVEIS OU EXCESSIVAMENTE ELEVADOS, SE APLICÁVEL: Os valores foram com base em orçamentos obtidos em mercado, no qual se optou pelo menor preço, a fim de satisfazer as demandas desta casa de leis.

CARACTERIZAÇÃO DAS FONTES DE PESQUISA CONSULTADAS: Foram realizadas pesquisas de preços utilizando-se dos seguintes parâmetros estabelecidos no Ato da Presidência nº 136/2023, no qual Art. 6º

> "A pesquisa de preços para fins de determinação do preço estimado na contratação direta para a aquisição de bens e contratação de serviços em geral, consolidada em mapa comparativo, terá prazo de validade de 6 (seis) meses e será realizada mediante a utilização dos seguintes parâmetros, **de forma combinada ou não"**.

No qual foi utilizada IV – pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos orçamentos com mais de 6 (seis) meses de antecedência da data da pesquisa de preço;

JUSTIFICATIVA DAS FONTES CONSULTADAS: Foram priorizados na pesquisa de preços os sistemas oficiais de governo, no entanto, a busca não foi satisfatória, pois não apresentou resultados de produtos com a mesma especificação, um ponto que pode ter contribuído foi a mudança da linha de produtos do fabricante da solução. Sendo assim, considerando que o desenvolvedor da solução possui uma rede de empresas autorizadas, consultou-se as mesmas visando a obtenção de propostas, por meio eletrônico de, no mínimo, 3 (três) fornecedores.

PERÍODO DE REALIZAÇÃO DA PESQUISA DE PREÇOS: Junho de 2024.

Abaixo relatório detalhado identificando cada um dos itens e seus valores obtidos:

PESQUISA DE MERCADO						
LOTE I - ITEM 1 - Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License						
FORNECEDOR	**MARCA**	**C/D**	**ART. 7º §4º**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL**
OPTIMUS DATA TECHNOLOGY LTDA		C	Exequível	160	R$ 358,19	R$ 57.310,40
Avant		C	Exequível	160	R$ 445,94	R$ 71.350,40
Solo Network		C	Exequível	160	R$ 411,26	R$ 65.801,60
		C		0		R$ 0,00
	-	C		1		R$ 0,00
	-	C		1		R$ 0,00
	-	C		1		R$ 0,00
MENOR PREÇO/FORNECEDOR					**R$ 57.310,40**	**#N/D**

VALOR TOTAL R$57.310,40 (Cinquenta e sete mil, trezentos e dez reais com quarenta centavos).

Eu, Rafael Sanches Alencar, declaro que efetuei a pesquisa de preços, na forma dos incisos I do artigo 23° da Lei n° 14.133/2021, em conformidade com o Ato da Presidência nº 136/2023 e que os preços aqui apresentados condizem com os praticados no mercado.

Proc. Administrativo 25- 279/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: Envolvidos internos acompanhando

Data: 03/10/2024 às 08:03:10

Proc. Administrativo 23- 279/2024 cancelado por **Rafael Sanches Alencar**, com a seguinte justificativa:

Arquivo disponibilizado para assinatura necessita de ajuste do signatário.

Proc. Administrativo 26- 279/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: Envolvidos internos acompanhando

Data: 03/10/2024 às 08:03:32

Proc. Administrativo 24- 279/2024 cancelado por **Rafael Sanches Alencar**, com a seguinte justificativa:

Arquivo disponibilizado para assinatura necessita de ajuste do signatário.

Proc. Administrativo 27- 279/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: Envolvidos internos acompanhando

Data: 03/10/2024 às 08:18:33

Relatorio de Pesquisa de Preço atualizado, com ajustes na justificativa das fontes consultadas.

_

Rafael Sanches
Diretoria de Tecnologia

Anexos:

RELATORIA_PESQUISA_DE_PRECOS_docx_1_.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Rafael Sanches Alencar	03/10/2024 08:18:47	1Doc	RAFAEL SANCHES ALENCAR CPF 006.XXX.XXX-96

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **3173-3EF6-2F8B-CFFA**

RELATÓRIO DE PESQUISA DE PREÇOS, PLANILHA COMPARATIVA E DOCUMENTAÇÃO COMPROBATÓRIA

INTRODUÇÃO

O presente relatório é resultado da pesquisa de preços abaixo discriminada em cumprimento ao determinado na Lei nº 14.133/2021 em conformidade com o Ato da Presidência nº 136/2023.

AGENTE RESPONSÁVEL PELA PESQUISA: Rafael Sanches Alencar

OBJETO: Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses

MÉTODO ESTATÍSTICO APLICADO COM JUSTIFICATIVAS PARA A METODOLOGIA UTILIZADA, EM ESPECIAL PARA A DESCONSIDERAÇÃO DE VALORES INCONSISTENTES, INEXEQUÍVEIS OU EXCESSIVAMENTE ELEVADOS, SE APLICÁVEL: Os valores foram com base em orçamentos obtidos em mercado, no qual se optou pelo menor preço, a fim de satisfazer as demandas desta casa de leis.

CARACTERIZAÇÃO DAS FONTES DE PESQUISA CONSULTADAS: Foram realizadas pesquisas de preços utilizando-se dos seguintes parâmetros estabelecidos no Ato da Presidência nº 136/2023, no qual Art. 6º

> "A pesquisa de preços para fins de determinação do preço estimado na contratação direta para a aquisição de bens e contratação de serviços em geral, consolidada em mapa comparativo, terá prazo de validade de 6 (seis) meses e será realizada mediante a utilização dos seguintes parâmetros, **de forma combinada ou não"**.

No qual foi utilizada IV – pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos orçamentos com mais de 6 (seis) meses de antecedência da data da pesquisa de preço;

JUSTIFICATIVA DAS FONTES CONSULTADAS: Foram priorizados na pesquisa de preços os sistemas oficiais de governo, no entanto, a busca não foi satisfatória, pois não apresentou resultados de produtos com a mesma especificação, um ponto que pode ter contribuído foi a mudança da linha de produtos do fabricante da solução. Sendo assim, considerando que o desenvolvedor da solução possui uma rede de empresas autorizadas, consultou-se as mesmas visando a obtenção de propostas, por meio eletrônico de, no mínimo, 3 (três) fornecedores.

PERÍODO DE REALIZAÇÃO DA PESQUISA DE PREÇOS: Junho de 2024.

Abaixo relatório detalhado identificando cada um dos itens e seus valores obtidos:

PESQUISA DE MERCADO						
LOTE I - ITEM 1 - Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License						
FORNECEDOR	**MARCA**	**C/D**	**ART. 7º §4º**	**QTD**	**VALOR UNITÁRIO**	**VALOR TOTAL**
OPTIMUS DATA TECHNOLOGY LTDA		C	Exequível	160	R$ 358,19	R$ 57.310,40
Avant		C	Exequível	160	R$ 445,94	R$ 71.350,40
Solo Network		C	Exequível	160	R$ 411,26	R$ 65.801,60
		C		0		R$ 0,00
	-	C		1		R$ 0,00
	-	C		1		R$ 0,00
	-	C		1		R$ 0,00
MENOR PREÇO/FORNECEDOR					**R$ 57.310,40**	**#N/D**

VALOR TOTAL R$57.310,40 (Cinquenta e sete mil, trezentos e dez reais com quarenta centavos).

Eu, Rafael Sanches Alencar, declaro que efetuei a pesquisa de preços, na forma dos incisos I do artigo 23° da Lei n° 14.133/2021, em conformidade com o Ato da Presidência nº 136/2023 e que os preços aqui apresentados condizem com os praticados no mercado.

Proc. Administrativo 28- 279/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: Envolvidos internos acompanhando

Data: 03/10/2024 às 08:21:40

Documento ETP atualizado;

_

Rafael Sanches
Diretoria de Tecnologia

Anexos:

ETP_docx_1_.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Jeverson Siqueira	03/10/2024 08:41:10	1Doc	JEVERSON SIQUEIRA CPF 080.XXX.XXX-74

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **AD30-E329-B4EC-1FF9**

ESTUDO TÉCNICO PRELIMINAR

1) DESCRIÇÃO DA NECESSIDADE

1.1. Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

1.2. A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

1.3. Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

1.4. Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

1.5. Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

1.6. Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

1.7. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.

2) REQUISITOS DA CONTRATAÇÃO

Item	Descriçao	SKU	Quantidade
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160

3) LEVANTAMENTO DE MERCADO

Considerando que a Câmara Municipal de Foz do Iguaçu já dispõe de um sistema de antivírus, foram avaliadas duas alternativas sendo uma delas a renovação e upgrade de versão do sistema e a outra a aquisição de um sistema integrado com o nosso sistema de Firewall.

Mantendo os investimentos ocorridos no ano de 2018 (R$ 11.635) e 2021 (R$ 31.217,00 (Preço médio)) e já realizados, tendo em vista de que além da aquisição do sistema, foi também realizada no ano de 2023 (R$ 6.980,00) a contratação de uma empresa especializada para nos auxiliar na configuração recomendadas pelo fabricante, e com base nas pesquisa de preços e estudo entre outras soluções, por medida de economicidade optou-se pela renovação com upgrade da versão já utilizada do licenciamento da solução Kaspersky e aquisição de novas licenças de acordo com a

necessidade da CMFI , levando em consideração a ampliação do parque computacional que ocorreu nesses últimos anos e demandas futuras.

Notou-se ainda que a linha de produtos do desenvolvedor da solução passou por atualizações entregando novas versões de sua solução bem como mais recursos, a título de exemplo temos, portais de capacitação na solução, canais de suporte e a adoção da inteligência artificial para detecção e mitigação de vulnerabilidades.

4) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

As especificações do objeto desta licitação deverão estar detalhadas no termo de referência elaborado com base neste estudo técnico preliminar e de acordo com a solicitação elaborada pelo setor demandante.

5) ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

Item	Descrição	SKU	Quantidade	Valor
1	KASPERSKY NEXT EDR OPTIMUM 36 meses	KL4066KASTJ	160	R$ 57.310,40

Descrição Item 1

A solução deve incluir treinamento em segurança cibernética

Do módulo de proteção de endpoint

Compatibilidade com diferentes sistemas operacionais, MAC OS, Linux de 32 e 64 bits (CentOS, Red Hat Enterprise, Debian, Ubuntu, Oracle Linux), Windows 7, 8, 8.1, 10,11 para desktops, para servidores S.O Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022, Windows Small Business Server 2011, Servidores de terminal Microsoft (Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022).

Módulo de gerenciamento avançado

A solução deve suportar arquitetura cloud-native e on-premisse, a solução deve incluir suporte para implantação baseada em nuvem (Amazon Web Services e/ou Microsoft Azure. Integração nativa com as seguintes opções de SIEM (HP (Microfoco) ArcSight, IBM QRadar, Splunk, Kaspersky KUMA). 2.4.

A solução deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

A solução deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

A solução deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.
A solução deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.
O servidor de gerenciamento primário da solução deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.
A solução deve suportar os seguintes canais de entrega de notificação, E-mail, registro de sistema e SMS ou equivalente.
A solução deve ter a capacidade de etiquetar/marcar computadores com base em
Atributos de rede, Nome, Domínio e/ou Sufixo de Domínio, Endereço de IP, Endereço IP para servidor de gerenciamento, Localização no Active Directory, Unidade organizacional, Grupo, Sistema operacional, Número do pacote de serviço, Arquitetura Virtual, Registro de aplicativos, Nome da Aplicação, Versão do aplicativo, Fabricante, Tipo e versão, Arquitetura.
A solução deverá permitir especificamente o bloqueio dos seguintes dispositivos, Bluetooth, Dispositivos móveis, Modems externos, CD/DVD, Câmeras e scanners.
A solução deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.
A solução deve permitir realizar as seguintes ações para endpoints, verificação manual, verificação no acesso, verificação por demanda, verificação de arquivos compactados, verificação de arquivos individuais, pastas e unidades, bloqueio e verificação de scripts, proteção contra alteração de registros, proteção contra estouro de buffer, verificação em segundo plano/inativa.

A solução deverá suportar os seguintes servidores de banco de dados:
Windows,

- Microsoft SQL Server
- Microsoft Banco de dados SQL do Azure
- MySQL Standard e Enterprise
- MariaDB
- PostgreSQL

Linux:

- MySQL
- MariaDB

- PostgreSQL

A solução deverá suportar as seguintes plataformas virtuais:

Windows:

- VMware vSphere 6.7 e 7.0
- Estação de trabalho VMware 16 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Oracle VM VirtualBox 6.x

2.74.2. Linux:

- VMware vSphere 6.7, 7.0 e 8.0
- VMware Desktop 16 Pro e 17 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 e 8.x

Do módulo de gerenciamento simplificado

A solução deve suportar arquitetura cloud;

A solução deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

A solução deve permitir ao administrador gerar relatórios pré-definidos.

A solução deve incluir informações do endpoint, IP público de internet, IP interno do dispositivo, Versão do agente de proteção, ultima comunicação com a console, contendo data e hora, informações do sistema operacional;

Requisitos gerais

A solução deve ser capaz de detectar os seguintes tipos de ameaças:
Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.
A solução deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
A solução deve ter capacidade de integração com a central de segurança do Windows Defender.
A solução deve suportar o subsistema Linux no Windows.
A solução deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

- Proteção contra ameaças sem arquivos (Fileless);
- Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

Do modulo de gerenciamento de dispositivos móveis

O modulo deve ser integrado a console de gerenciamento;
A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

- Android 5.0 ou posterior (incluindo Android 12L)

A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

- iOS 10–17 ou iPadOS 13–17

A solução deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

Do módulo de EDR

Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
A solução deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;

Deve apresentar informações detalhadas contendo:

- Usuário que executou a ação;
- Informações acesso privilegiado;

A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.

O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único).

6) IMPACTOS AMBIENTAIS

Não foram identificados impactos ambientes nesta contratação

7) JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Não se aplica, trata-se de um único item.

8) CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

Não se identificou contratações interdependentes e/ou correlatas, sendo que a prestação dos serviços depende exclusivamente do presente procedimento.

9) ALINHAMENTO COM PAC – PLANO ANUAL DE CONTRATAÇÕES

A demanda em questão encontra-se prevista no plano anual de contratações. Considerando que o mapa de gerenciamento de riscos tem natureza opcional, conforme previsto na NLL 14.133 e ato da presidência 133/2023.

10) RESULTADOS PRETENDIDOS

- Garantir um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;
- Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo estações de trabalho e notebooks comprometidos;
- Evitar, mitigar e conter a propagação de pragas digitais (vírus/malwares/spywares, spam, entre outros) com a administração centralizada da solução de proteção;

- Permitir o controle de acesso à rede por dispositivos computacionais, permitindo gerenciamento destes dispositivos;
- Possibilitar análise pormenorizada de arquivos, discos rígidos, unidades móveis, mensagens de e-mail e anexos, viabilizando detecção de ameaças, com intento de salvaguardar a estrutura tecnológica de ataques com teor e objetivo malicioso;
- Possibilitar o controle de acesso e tráfego de informações aos dispositivos e serviços operacionais na rede, através de gerenciamento centralizado, o que vem a complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;
- Aprimorar a segurança de TIC da CMFI frente a ameaças sofisticadas.

11) PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Tendo em vista que nosso ambiente de tecnologia já possui uma solução de firewall, não será necessária nenhuma providência prévia.

12) VIABILIDADE DA CONTRATAÇÃO

Esta equipe de TI declara viável esta contratação

13) TRATAMENTO DIFERENCIADO E FAVORECIDO A SER DISPENSADO ÀS MICROEMPRESAS, ÀS EMPRESAS DE PEQUENO PORTE E AOS MICROEMPREENDEDORES INDIVIDUAIS

Após diversas tentativas de localização e contato com empresas qualificadas como microempresas (ME) e empresas de pequeno porte (EPP) na região de Foz do Iguaçu para fornecimento das licenças, constatou-se a inexistência, inclusive pelo embasamento da pesquisa na base de de empresas credenciadas junto ao portal do desenvolvedor, acessado na data de 10/06/2024 às 09:38. Durante o processo de prospecção, entramos em contato direto com diversas empresas locais, incluindo aquelas registradas como ME e EPP, para verificar a capacidade técnica e a disponibilidade para fornecimento do serviço requerido. Nenhuma das ME/EPP contactadas demonstrou capacidade técnica ou interesse em participar do certame.

Diante dessas circunstâncias, a manutenção da exclusividade do certame para ME e EPP pode inviabilizar a contratação, comprometendo a eficiência e a continuidade dos serviços públicos dependentes de uma conexão estável e de alta velocidade, eis que

há sério risco da licitação ser deserta. Ressalta-se, porém, que as ME/EPP ainda poderão participar do certame com vantagens sobre os demais concorrentes conforme versa a legislação pátria.

Portanto, justifica-se o afastamento da exclusividade de participação de microempresas e empresas de pequeno porte neste certame específico, com base na inexistência de fornecedores locais qualificados e na necessidade imperiosa de garantir a prestação adequada e contínua dos serviços públicos.

14) RESPONSÁVEIS PELA ELABORAÇÃO DO ETP

Jeverson Siqueira
Cargo: Tecnico de Informatica
Matrícula: 202.045
Setor: Diretoria de Tecnologia

Proc. Administrativo 29- 279/2024

De: CARLOS K. - AGCONT

Para: Envolvidos internos acompanhando

Data: 15/10/2024 às 08:40:23

Trago aos autos a minuta do Edital com os documentos atualizados

–

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras

Anexos:

MINUTA_EDITAL_PREGAO_0x_24_COMPLETO.pdf

PREGÃO ELETRÔNICO

0x/2024
(9000x/2024 no sistema compras.gov.br)

CONTRATANTE (UASG)

Câmara Municipal de Foz do Iguaçu (926470)

OBJETO

Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

VALOR TOTAL DA CONTRATAÇÃO

R$ 57.310,40 (Cinquenta e sete mil, trezentos e dez reais e quarenta centavos).

DATA DA SESSÃO PÚBLICA

Dia **xx/11/2024** às **10h (horário de Brasília)**

CRITÉRIO DE JULGAMENTO:

Menor preço por item.

MODO DE DISPUTA:

Aberto e fechado

PREFERÊNCIA ME/EPP/EQUIPARADAS

SIM

Baixe o APP Compras.gov.br
e apresente sua proposta!

Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

Sumário

CÂMARA MUNICIPAL DE FOZ DO IGUAÇU

PREGÃO ELETRÔNICO Nº 0x/2024.

(Processo Administrativo 1DOC n°180/2024)

Torna-se público que a Câmara Municipal de Foz do Iguaçu, por meio do Setor de Compras, sediada na Travessa Oscar Muxfeldt, nº 81, Centro, Foz do Iguaçu – PR, realizará licitação, para registro de preços, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021, do Atos da Presidência nº 131/2023 e nº 134/2023 demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. O objeto da presente licitação é a Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

1.2. A licitação será realizada em item único.

ITEM	DESCRIÇÃO	BENEFÍCIO ME/EPP	QNT	VALOR UNITÁRIO	VALOR TOTAL
1	Licença KASPERSKY NEXT EDR OPTIMUM 36 meses	Tratamento favorecido	160	R$ 358,19	R$ 57.310,40

2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

2.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

2.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

2.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

2.5. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015, bem como para bens e serviços

produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010

2.6. Não poderão disputar esta licitação:

2.6.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

2.6.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

2.6.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

2.6.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.6.5. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

2.6.6. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

2.6.7. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.6.8. agente público do órgão ou entidade licitante;

2.6.9. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

2.6.10. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.

2.7. O impedimento de que trata o item 2.6.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.8. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.6.2 e 2.6.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

2.9. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

2.10. O disposto nos itens 2.6.2 e 2.6.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

2.11. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da

contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133/2021.

2.12. A vedação de que trata o item 2.6.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

3.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

3.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

3.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 7.1.1 e 7.11.1 deste Edital.

3.4. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

3.4.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

3.4.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

3.4.3. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

3.4.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

3.5. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

3.6. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

3.6.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

3.6.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

3.7. A falsidade da declaração de que trata os itens 3.4 ou 3.6 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

3.8. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

3.9. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

3.10. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

3.11. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

3.11.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

3.11.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

3.12. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

3.12.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

3.12.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.

3.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 3.11 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

3.14. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

3.15. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

4. DO PREENCHIMENTO DA PROPOSTA

4.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

4.1.1. Valor unitário e total do item;

4.1.2. Marca;

4.1.3. Fabricante;

4.1.4. Quantidade cotada, devendo respeitar o mínimo para cada item.

4.2. Todas as especificações do objeto contidas na proposta aceita pela Administração vinculam o licitante.

4.2.1. O licitante NÃO poderá oferecer proposta em quantitativo inferior ao previsto para a contratação.

4.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

4.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

4.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

4.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

4.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, quando devidamente aceita pela administração, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

4.7.1. O prazo de validade da proposta **não será inferior a 90 (noventa)** dias**,** a contar da data de sua apresentação, independentemente do prazo indicado no documento encaminhado.

4.7.2. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

4.8. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

5.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

5.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

5.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

5.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

5.5. O lance deverá ser ofertado pelo valor unitário do item

5.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

5.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

5.8. O intervalo mínimo de diferença de valores, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 1,00 (Um real).

5.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.10. O procedimento seguirá de acordo com o modo de disputa aberto e fechado.

5.11. Para o envio de lances no pregão eletrônico o modo de disputa "aberto e fechado", os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

5.11.1. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

5.11.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.11.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

5.11.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.11.5. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.12. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.13. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

5.14. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

5.15. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

5.16. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

5.17. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

5.18. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

5.18.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

5.18.2. A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

5.18.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

5.18.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

5.19. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

5.19.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

5.19.1.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

5.19.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

5.19.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

5.19.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

5.19.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

5.19.2.1. empresas estabelecidas no território do Estado do Paraná;

5.19.2.2. empresas brasileiras;

5.19.2.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

5.19.2.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

5.19.3. Se, mesmo após a aplicação dos procedimentos previstos nos itens acima, ainda persistir o empate, será realizado sorteio público para fins de desempate;

5.19.3.1. Será informado no chat da sessão pública, a data, hora e local do sorteio, a ser realizado no site sorteio.com (ou outro compatível), com transmissão ao vivo no Youtube ou outra plataforma de streaming;

5.19.3.2. Haverá lavratura de ata de sorteio, com presença de testemunhas, que será incluída no processo administrativo.

5.20. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro deverá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.20.1. Não será admitida a previsão de preços diferentes em razão de local de entrega ou de acondicionamento, tamanho de lote ou qualquer outro motivo.

5.20.2. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

5.20.3. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

5.20.4. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

5.20.5. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

5.20.6. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

5.21. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

6. DA FASE DE JULGAMENTO

6.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 2.5 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.1.1. SICAF;

6.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

6.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

6.1.4. Cadastro de restrições ao direito de contratar com a Administração Pública (https://crcap.tce.pr.gov.br/ConsultarImpedidos.aspx)

6.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

6.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

6.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

6.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação.

6.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

6.4. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

6.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com os itens 3.5.1 e 4.6 deste edital.

6.6. Verificadas as condições de participação, o pregoeiro examinará a proposta final ajustada, ofertada pela empresa classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 27 a 33 do Ato da Presidência nº 134/2023.

6.7. Será desclassificada a proposta vencedora que:

6.7.1. contiver vícios insanáveis;

6.7.2. não obedecer às especificações técnicas contidas no Termo de Referência;

6.7.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

6.7.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.7.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

6.8. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

6.8.1. A inexequibilidade, na hipótese de que trata o **caput**, só será considerada após diligência do pregoeiro, que comprove:

6.8.1.1. que o custo do licitante ultrapassa o valor da proposta; e

6.8.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.8.2. Será desclassificada a proposta que não tiver sua exequibilidade demonstrada, quando exigido pela Administração.

6.9. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

6.10. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante ou da área especializada no objeto.

7. DA FASE DE HABILITAÇÃO

7.1. Os documentos previstos neste item, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

7.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

7.2. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

7.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor

juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

7.4. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, por cópia ou original e cópia simples para autenticação pela Equipe de Pregão e posterior devolução.

7.5. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

7.6. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

7.7. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

7.8. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

7.9. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

7.9.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

7.10. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (IN nº 3/2018, art. 7º, *caput*).

7.10.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. (IN nº 3/2018, art. 7º, parágrafo único).

7.11. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

7.11.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de DUAS HORAS, prorrogável por igual período, contado da solicitação do pregoeiro.

7.12. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

7.12.1. Os documentos relativos à regularidade fiscal somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

7.13. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e Ato da Presidência nº 134/2023, art. 35, §4º):

7.13.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

7.13.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

7.14. Na análise dos documentos de habilitação, a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.15. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital.

7.16. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

7.17. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

7.18. Serão exigidos os seguintes documentos para a habilitação:

7.18.1. Habilitação jurídica nos termos do art. 66 da Lei nº 14.133/2021;

7.18.2. Prova da inexistência de fato impeditivo para licitar ou contratar com a Administração Pública, mediante a juntada de pesquisa realizada junto ao Tribunal de Contas da União e ao Tribunal de Contas do Estado do Paraná;

7.18.3. Habilitação fiscal, social e trabalhista, nos termos do Art. 68 da Lei nº 14-133/2021;

7.18.4. Habilitação econômico-financeira, mediante o fornecimento de Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante;

8. DOS RECURSOS

8.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

8.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

8.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

8.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

8.3.1.1. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

8.3.2. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

8.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

8.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

8.6. Os recursos interpostos fora do prazo não serão conhecidos.

8.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

8.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

8.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

8.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico https://www.fozdoiguacu.pr.leg.br/transparencia/licitacoes/2024/pregao-eletronico-003-2024/

9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

9.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

9.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

9.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

9.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

9.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

9.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

9.1.2.4. deixar de apresentar amostra;

9.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

9.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

9.1.3.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

9.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação

9.1.5. fraudar a licitação

9.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

9.1.6.1. agir em conluio ou em desconformidade com a lei;

9.1.6.2. induzir deliberadamente a erro no julgamento;

9.1.6.3. apresentar amostra falsificada ou deteriorada;

9.1.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

9.1.8. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

9.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

9.2.1. advertência;

9.2.2. multa;

9.2.3. impedimento de licitar e contratar e

9.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

9.3. Na aplicação das sanções serão considerados:

9.3.1. a natureza e a gravidade da infração cometida.

9.3.2. as peculiaridades do caso concreto

9.3.3. as circunstâncias agravantes ou atenuantes

9.3.4. os danos que dela provierem para a Administração Pública

9.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor da proposta, recolhida no prazo máximo de **15 (quinze) dias** úteis, a contar da comunicação oficial.

9.4.1. Para as infrações previstas nos itens 9.1.1, 9.1.2 e 9.1.3, a multa será de 5% do valor total da proposta.

9.4.2. Para as infrações previstas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, a multa será de 30% do valor total da proposta.

9.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

9.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

9.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 9.1.1, 9.1.2 e 9.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

9.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, bem como pelas infrações administrativas previstas nos itens 9.1.1, 9.1.2 e 9.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

9.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 9.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

9.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

9.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida,

que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

9.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

9.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

9.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

10.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

10.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

10.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, pelos *seguintes meios*: protocolo digital através do sistema 1doc através do link https://fozdoiguacu.1doc.com.br/b.php?pg=wp/wp&itd=12 ou envio através do email licitacao@fozdoiguacu.pr.leg.br.

10.4. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

10.4.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.

10.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

11. DAS DISPOSIÇÕES GERAIS

11.1. Será divulgada ata da sessão pública no sistema eletrônico.

11.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

11.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

11.4. A homologação do resultado desta licitação não implicará direito à contratação.

11.5. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

11.6. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

11.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

11.8. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

11.9. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

11.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico https://www.fozdoiguacu.pr.leg.br/transparencia/licitacoes/2024/pregao-eletronico-00x-2024.

11.11. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

11.11.1. ANEXO I - Termo de Referência

11.11.2. ANEXO II – Estudo Técnico Preliminar

11.11.3. ANEXO III - Minuta de Termo de Contrato

11.11.4. ANEXO IV – Modelo da Proposta de Preços

JOÃO MORALES

PRESIDENTE DA CÂMARA MUNICIPAL DO IGUAÇU

TERMO DE REFERÊNCIA

1) DEFINIÇÃO DO OBJETO

Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

Item	CAT/MAT	Descrição	Prazo	SKU	Quantidade	Valor
1	350949	KASPERSKY NEXT EDR OPTIMUM 36 meses	36 meses	KL4066KASTJ	160	R$ 57.310,40

2) FUNDAMENTAÇÃO DA CONTRATAÇÃO

Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".
Considerando que esta casa de leis realiza a utilização da solução de segurança, sem ressalvas e visa proteger seu investimento, assegurar a padronização e compatibilidade com o ambiente computacional. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para, no mínimo, manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.
Com a iminente expiração da licença, torna-se necessária a renovação e aquisição para assegurar a proteção atualizada contra as ameaças virtuais mais recentes.
Sendo a demanda prevista no PAC, conforme documento de estudo técnico preliminar - ETP.

3) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução de segurança deve atender a necessidade de evolução e adequação desta casa em relação a suas ferramentas de proteção, esta casa de leis possui dois contratos ativos de licença da ferramenta KESB Select da desenvolvedora Kaspersky Global, em um deles possui o quantitativo de 130 licenças a expirar em 22/09/2024 e o outro de 20 licenças a expirar em 01/10/2024. Sendo assim, a solução apresentada deve fornecer 10 novas licenças e 150 em formato de renovação, adequada à nova linha de produtos das soluções de segurança com incremento de, no mínimo, EDR, bem como sua ativação. Referente a possibilidade de parcelamento, deve seguir de acordo com o ETP, por se tratar de uma solução integrada.

Custo Inicial Reduzido: Ao optar pela renovação, a empresa evita os altos custos iniciais de compra e instalação de novas soluções, permitindo a alocação de recursos para outras áreas críticas do negócio.

- **Suporte e atualizações:** Fornecimento dos serviços de suporte técnico, bem como atualizações, asseguram o perfeito funcionamento da solução.
- **Gestão Simplificada:** Por se tratar de uma solução integrada a gestão centralizada, permite aos profissionais maior autonomia e melhor condição de adaptação, visto que a equipe é reduzida.

Os itens da presente solução devem ser contratados em conjunto tendo em vista a necessidade de completa compatibilidade para o correto funcionamento.

a) Proteção antivírus de Arquivos;

b) Proteção antivírus da Web;

c) Firewall local de cada máquina;

d) Bloqueador de Ataques da Rede;

e) Inspeção do Sistema;

f) Inspeção avançada de dispositivos portáteis (pen drive, cartão de memória, etc);

g) Monitoramento de Vulnerabilidades.

4) REQUISITOS DA CONTRATAÇÃO

4.1. Do módulo de proteção de endpoint

a. A solução proposta deverá proteger os sistemas operacionais abaixo:

i. Windows 7
ii. Windows 8
iii. Windows 8.1
iv. Windows 10
v. Windows 11

b. Servidores

i. Windows Small Business Server 2011
ii. Windows MultiPoint Server 2011
iii. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

c. Servidores de terminal Microsoft

i. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

d. Sistemas operacionais Linux de 32 bits:

i. CentOS 6.7 e posterior
ii. Debian GNU/Linux 11.0 e posterior
iii. Debian GNU/Linux 12.0 e posterior
iv. Red Hat Enterprise Linux 6.7 e posterior

e. Sistemas operacionais Linux de 64 bits:

i. Amazon Linux 2.
ii. CentOS 6.7 e mais tarde
iii. CentOS 7.2 e posterior.
iv. CentOS Stream 8.
v. CentOS Stream 9.
vi. Debian GNU/Linux 11.0 e posterior.
vii. Debian GNU/Linux 12.0 e posterior.
viii. Linux Mint 20.3 e superior.
ix. Linux Mint 21.1 e posterior.
x. openSUSE Leap 15.0 e posterior.
xi. Oracle Linux 7.3 e posterior.
xii. Oracle Linux 8.0 e posterior.
xiii. Oracle Linux 9.0 e posterior.
xiv. Red Hat Enterprise Linux 6.7 e posterior
xv. Red Hat Enterprise Linux 7.2 e posterior.

xvi. Red Hat Enterprise Linux 8.0 e posterior.
xvii. Red Hat Enterprise Linux 9.0 e posterior.
xviii. Rocky Linux 8.5 e posterior.
xix. Rocky Linux 9.1.
xx. SUSE Linux Enterprise Server 12.5 ou posterior.
xxi. SUSE Linux Enterprise Server 15 ou posterior.
xxii. Ubuntu 20.04 LTS.
xxiii. Ubuntu 22.04 LTS.
xxiv. Sistemas operacionais Arm de 64 bits:
xxv. CentOS Stream 9.
xxvi. SUSE Linux Enterprise Server 15.
xxvii. Ubuntu 22.04 LTS.

f. Sistemas operacionais MAC OS:
i. macOS 12 – 14

g. Ferramentas de virtualização MAC OS:
i. Parallels Desktop 16 para Mac Business Edition
ii. VMware Fusion 11.5 Profissional
iii. VMware Fusion 12 Profissional

h. A solução proposta deverá suportar as seguintes plataformas virtuais:
i. VMware Workstation 17.0.2 Pro
ii. VMware ESXi 8.0 Update 2
iii. Microsoft Hyper-V Server 2019
iv. Citrix Virtual Apps e Desktop 7 2308
v. Citrix Provisioning 2308
vi. Citrix Hypervisor 8.2 Update 1

4.2. Do módulo de gerenciamento avançado

a. A solução proposta deve suportar arquitetura cloud-native e on-premisse;
b. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
i. Amazon Web Services
ii. Microsoft Azure
c. A solução proposta deve incluir as seguintes opções de integração SIEM:
i. HP (Microfoco) ArcSight
ii. IBM QRadar
iii. Splunk
iv. Kaspersky KUMA
d. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.
e. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;
f. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.
g. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.
h. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

i. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

j. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

k. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

l. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.

m. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

n. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:

i. Status do dispositivo
ii. Tag
iii. Diretório ativo
iv. Proprietários de dispositivos
v. Hardware

o. A solução proposta deve suportar os seguintes canais de entrega de notificação:

i. E-mail
ii. Registro de sistema
iii. SMS

p. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:

i. Atributos de rede
ii. Nome
iii. Domínio e/ou Sufixo de Domínio
iv. Endereço de IP
v. Endereço IP para servidor de gerenciamento
vi. Localização no Active Directory
vii. Unidade organizacional
viii. Grupo
ix. Sistema operacional
x. Número do pacote de serviço
xi. Arquitetura Virtual
xii. Registro de aplicativos
xiii. Nome da Aplicação
xiv. Versão do aplicativo
xv. Fabricante
xvi. Tipo e versão
xvii. Arquitetura

q. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

r. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

s. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

i. Dispositivos Desktop/Servidores
ii. Dispositivos móveis
iii. Dispositivos de rede
iv. Dispositivos virtuais
v. Componentes OEM
vi. Periféricos de computador
vii. Dispositivos IoT conectados
viii. Telefones VoIP
ix. Repositórios de rede

t. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

i. Nome da Aplicação
ii. Caminho do aplicativo
iii. Metadados do aplicativo
iv. Aplicativo Certificado digital
v. Categorias de aplicativos predefinidas pelo fornecedor
vi. SHA256 e MD5

u. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

i. Bluetooth
ii. Dispositivos móveis
iii. Modems externos
iv. CD/DVD
v. Câmeras e scanners
vi. MTPs
vii. E a transferência de dados para dispositivos móveis

v. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

w. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

x. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

i. Estruturas de domínios e grupos de trabalho do Windows
ii. Estruturas de grupos do Active Directory
iii. Conteúdo de um arquivo de texto criado manualmente pelo administrador

y. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

z. A solução proposta deve permitir realizar as seguintes ações para endpoints:

i. Verificação manual;
ii. Verificação no acesso;
iii. Verificação por demanda;
iv. Verificação de arquivos compactados
v. Verificação de arquivos individuais, pastas e unidades;
vi. Bloqueio e verificação de scripts

vii. Proteção contra alteração de registros;
viii. Proteção contra estouro de buffer;
ix. Verificação em segundo plano/inativa

1.1. Verificação de unidade removível na conexão com o sistema;
1.2. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.
1.3. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.
1.4. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.
1.5. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.
1.6. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.
1.7. A solução proposta deve suportar Windows Failover Cluster.
1.8. A solução proposta deve ter um recurso de clustering integrado.
1.9. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.
1.10. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.
1.11. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.
1.12. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.
1.13. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.
1.14. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.
1.15. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.
1.16. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.
1.17. A solução proposta deverá possuir controles para download de DLL e drivers.
1.18. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão.
1.19. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.
1.20. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).
1.21. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.
1.22. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir

as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.
1.23. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.
1.24. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.
1.25. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.
1.26. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.
1.27. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.
1.28. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.
1.29. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.
1.30. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.
1.31. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. .
1.32. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.
1.33. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.
1.34. A solução proposta deve permitir ao administrador personalizar relatórios.
1.35. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.
1.36. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.
1.37. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.
1.38. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.
1.39. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.

1.40. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.
1.41. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;
1.42. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.
1.43. A solução proposta deve suportar integração com solução APT.
1.44. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.
1.45. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:
1.45.1. Windows
1.45.2. Linux
1.46. A solução proposta deverá suportar os seguintes servidores de banco de dados:
1.46.1.1. Windows:
1.46.1.2. Microsoft SQL Server
1.46.1.3. Microsoft Banco de dados SQL do Azure
1.46.1.4. MySQL Standard e Enterprise
1.46.1.5. MariaDB
1.46.1.6. PostgreSQL
1.46.2. Linux:
1.46.2.1. MySQL
1.46.2.2. MariaDB
1.46.2.3. PostgreSQL
1.47. A solução proposta deverá suportar as seguintes plataformas virtuais:
1.47.1.1. Windows:
1.47.1.2. VMware vSphere 6.7 e 7.0
1.47.1.3. Estação de trabalho VMware 16 Pro
1.47.1.4. Servidor Microsoft Hyper-V 2012 de 64 bits
1.47.1.5. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
1.47.1.6. Microsoft Servidor Hyper -V 2016 de 64 bits
1.47.1.7. Servidor Microsoft Hyper-V 2019 de 64 bits
1.47.1.8. Servidor Microsoft Hyper-V 2022 de 64 bits
1.47.1.9. Citrix XenServer 7.1 LTSR
1.47.1.10. Citrix XenServer 8.x
1.47.1.11. Oracle VM VirtualBox 6.x
1.47.2. Linux:
1.47.2.1. VMware vSphere 6.7, 7.0 e 8.0
1.47.2.2. VMware Desktop 16 Pro e 17 Pro
1.47.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits
1.47.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
1.47.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits
1.47.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits
1.47.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits
1.47.2.8. Citrix XenServer 7.1 e 8.x

1.47.2.9. Oracle VM VirtualBox 6.x e7.x
1.48. A solução proposta deve suportar criptografia em vários níveis:
1.48.1. Criptografia completa do disco – incluindo disco do sistema
1.48.2. Criptografia de arquivos e pastas
1.48.3. Criptografia de mídia removível
1.48.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2
1.49. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:
1.49.1. A criptografia de arquivos em unidades de computador locais.
1.49.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.
1.49.3. A criação de listas criptografadas de pastas em unidades de computador locais.
1.50. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:
1.50.1. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.
1.50.2. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.
1.51. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:
1.51.1. A criptografia de todos os arquivos armazenados em unidades removíveis.
1.51.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.
1.52. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia
1.53. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.
1.54. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.
1.55. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.
1.56. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.
1.57. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.
1.58. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.

1.59. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.
1.60. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.
1.61. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.
1.62. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.
1.63. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.
1.64. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.
1.65. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário.
1.66. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.
1.67. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.
1.68. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:
1.68.1. Uso do Trusted Platform Module e configurações de senha.
1.68.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.
1.69. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).
1.70. A solução proposta deve suportar criptografia em Microsoft Surface Tablets.
1.71. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
1.71.1. Instalação remota de software de terceiros
1.71.2. Relatórios sobre software e hardware existentes
1.71.3. Monitoramento para instalação de software não autorizado
1.71.4. Remoção de software não autorizado
1.72. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.
1.73. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.
1.74. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.
1.75. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.
1.76. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.

1.77. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.
1.78. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.
1.79. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança
1.80. A solução proposta deve permitir ao administrador aprovar atualizações.
1.81. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.
1.82. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.
1.83. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.
1.84. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.
1.85. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.
1.86. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).
1.87. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.
1.88. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.
1.89. A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’.
1.90. A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”.
1.91. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.
1.92. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.
1.93. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.
1.94. A solução proposta deve apoiar a implantação do sistema operacional.
1.95. A solução proposta deve suportar Wake-on LAN e UEFI.
1.96. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.
1.97. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.
1.98. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.
1.99. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.
1.100. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.

1.101. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.
1.102. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.
1.103. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.
1.104. A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.
1.105. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:
1.105.1. Inicie a instalação ao reiniciar ou desligar o computador.
1.105.2. Instale o gerador necessário todos os pré-requisitos do sistema.
1.105.3. Permitir a instalação de novas versões de aplicativos durante as atualizações.
1.105.4. Baixe atualizações para o dispositivo sem instalá-las.
1.106. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.
1.107. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.
1.108. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:
1.108.1. CEF;
1.108.2. LEEF;
1.109. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.
1.110. O relatório da solução proposta deve conter informações CVE.
1.111. A solução proposta deve suportar instalação de aplicações e software de terceiros;

4.3. Do módulo de gerenciamento simplificado

1.112. A solução proposta deve suportar arquitetura cloud;
1.113. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.
1.114. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.
1.115. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.
1.116. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.
1.117. A solução proposta deve atender as condições apontadas no item e subintes 6.
1.118. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.
1.119. A solução proposta deve incluir informações do endpoint:
1.119.1. IP público de internet;
1.119.2. IP interno do dispositivo;
1.119.3. Versão do agente de proteção;

1.119.4. Ultima comunicação com a console, contendo data e hora;
1.119.5. Informações do sistema operacional;
1.120. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.
1.121. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.
1.122. A solução proposta deve incluir treinamento em segurança cibernética.

4.4. Requisitos gerais

1.123. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
1.123.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.
1.124. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
1.125. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).
1.126. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.
1.127. A solução proposta deve suportar o subsistema Linux no Windows.
1.128. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
1.128.1. Proteção contra ameaças sem arquivos (Fileless);
1.128.2. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;
1.129. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;
1.130. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.
1.131. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.
1.132. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.
1.133. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.
1.134. A solução proposta deve fornecer análise comportamental baseada em machine learning.
1.135. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.
1.136. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
1.136.1. Controles de aplicativos,
1.136.2. Controle web e dispositivos
1.136.3. HIPS e Firewall
1.136.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;

1.136.5. Gerenciamento de criptografia de arquivos e discos;
1.136.6. Controle adaptativo para detecção de anomalias;
1.137. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.
1.138. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.
1.139. A solução proposta deve ter bancos de dados de reputação locais e globais.
1.140. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.
1.141. A solução proposta deve incluir um módulo capaz, no mínimo, de:
1.141.1. Bloqueio de aplicativos com base em sua categorização.
1.141.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.
1.141.3. A adição de sub-redes e a modificação de permissões de atividade.
1.142. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.
1.143. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.
1.144. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.
1.145. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
1.145.1. Modo silencioso;
1.145.2. Discos rígidos e dispositivos removíveis;
1.145.3. De todos as contas de usuários do dispositivo.
1.146. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:
1.146.1. Exclusão imediata de dados;
1.146.2. Exclusão de dados adiada.
1.147. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:
1.147.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
1.147.2. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.
1.148. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.
1.149. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.
1.150. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.
1.151. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

1.152. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.
1.153. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.
1.154. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.
1.155. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;
1.156. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;
1.157. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.
1.158. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.
1.159. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.
1.160. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.
1.161. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.
1.162. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.
1.163. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.
1.164. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.
1.165. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.
1.166. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.
1.167. A solução proposta deve ter categoria de detecção para bloquear banners de sites.
1.168. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;
1.169. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.
1.170. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.
1.171. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.
1.172. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

1.173. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.
1.174. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.
1.175. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.
1.176. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.
1.177. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.
1.178. A solução proposta deve suportar o controle de scripts executados em PowerShell.
1.179. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.
1.180. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.
1.181. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.
1.182. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.
1.183. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.
1.184. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.
1.185. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
1.185.1. Filtro de anexos.
1.185.2. Verificação de mensagens de email ao receber, ler e enviar.
1.186. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.
1.187. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;
1.188. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);
1.189. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.
1.190. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.
1.191. A solução proposta deve incluir suporte ao protocolo IPv6.
1.192. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.
1.193. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
1.194. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.

1.195. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.
1.196. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.
1.197. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.
1.198. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.
1.199. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.
1.200. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.
1.201. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.
1.202. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.
1.203. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.
1.204. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.
1.205. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.
1.206. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.
1.207. A solução proposta deve suportar endereços IPv6.
1.208. A solução proposta deve suportar verificação em duas etapas (autenticação).
1.209. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.
1.210. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.
1.211. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.
1.212. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.
1.213. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.
1.214. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.
1.215. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.
1.216. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.

1.217. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.
1.218. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.
1.219. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.
1.220. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.
1.221. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.
1.222. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.
1.223. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.
1.224. A solução proposta deve ter a capacidade de excluir atualizações baixadas.
1.225. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.
1.226. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.
1.227. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.
1.228. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.
1.229. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.
1.230. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.
1.231. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.
1.232. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.
1.233. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
1.233.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.
1.233.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.
1.234. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.
1.235. A solução proposta deve gerar relatoiros de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

4.5. Do modulo de gerenciamento de dispositivos móveis

1.236. O modulo deve ser integrado a console de gerenciamento;
1.237. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
1.237.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)

1.238. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
1.238.1. iOS 10–17 ou iPadOS 13–17
1.239. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.
1.240. A solução proposta deve suportar dispositivos iOS supervisionados.
1.241. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.
1.242. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.
1.243. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.
1.244. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).
1.245. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.
1.246. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.
1.247. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.
1.248. A solução proposta deve ter recursos de conteinerização para dispositivos Android.
1.249. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:
1.249.1. Dados em contêineres
1.249.2. Contas de e-mail corporativo
1.249.3. Configurações para conexão à rede Wi-Fi corporativa e VPN
1.249.4. Nome do ponto de acesso (APN)
1.249.5. Perfil do Android for Work
1.249.6. Recipiente KNOX
1.249.7. Chave do gerenciador de licença KNOX
1.250. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
1.250.1. Todos os perfis de configuração instalados
1.250.2. Todos os perfis de provisionamento
1.250.3. O perfil iOS MDM
1.251. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas
1.252. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo .
1.253. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:
1.253.1. Critérios de verificação do dispositivo;

1.253.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;
1.254. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.
1.255. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:
1.255.1. Cartões de memória e outras unidades removíveis
1.255.2. Câmera do dispositivo
1.255.3. Conexões Wi-Fi
1.255.4. Conexões Bluetooth
1.255.5. Porta de conexão infravermelha
1.255.6. Ativação do ponto de acesso Wi-Fi
1.255.7. Conexão de área de trabalho remota
1.255.8. Sincronização de área de trabalho
1.255.9. Definir configurações da caixa de correio do Exchange
1.255.10. Configurar caixa de e-mail em dispositivos iOS MDM
1.255.11. Configure contêineres Samsung KNOX.
1.255.12. Definir as configurações do perfil do Android for Work
1.255.13. Configurar e-mail/calendário/contatos
1.255.14. Defina as configurações de restrição de conteúdo de mídia.
1.255.15. Definir configurações de proxy no dispositivo móvel
1.255.16. Configurar certificados e SCEP
1.256. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay .
1.257. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:
1.257.1. Google Play, Huawei App Gallery e Apple App Store
1.257.2. Portal de inscrição móvel KNOX
1.257.3. Pacotes de instalação pré-configurados independentes
1.258. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.
1.259. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.
1.260. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
1.260.1. VMware AirWatch 9.3 ou posterior
1.260.2. MobileIron 10.0 ou posterior
1.260.3. IBM MaaS360 10.68 ou posterior
1.260.4. Microsoft Intune 1908 ou posterior
1.260.5. SOTI MobiControl 14.1.4 (1693) ou posterior
1.261. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.
1.262. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:
1.262.1. Google Play
1.262.2. Galeria de aplicativos Huawei

1.262.3. Loja de aplicativos da Apple
1.263. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.
1.264. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.
1.265. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.
1.266. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.
1.267. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.
1.268. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.
1.269. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.
1.270. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.
1.271. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.
1.272. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.
1.273. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.
1.274. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.
1.275. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
1.276. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

4.6. Do módulo de EDR

4.6.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
4.6.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
4.6.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
4.6.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
4.6.5. Deve apresentar informações detalhadas contendo:
4.6.5.1.Usuário que executou a ação;
4.6.5.2.Informações acesso privilegiado;
4.6.6. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.
4.6.7. A solução proposta deve suportar integração com serviço de reputação em nuvem.
4.6.8. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)

4.6.9. O agente EDR deve ter integração com o aplicativo de proteção de endpoint(agente único).
4.6.10. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;
4.6.11. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.
4.6.12. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.
4.6.13. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.
4.6.14. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.
4.6.15. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.
4.6.16. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.
4.6.17. A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.
4.6.18. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.
4.6.19. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.
4.6.20. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:
4.6.21. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).
4.6.22. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.
4.6.23. Informações gerais sobre a detecção, incluindo modo de detecção.
4.6.24. Alterações no registro associadas à detecção.
4.6.25. Histórico da presença de arquivos no dispositivo.
4.6.26. Ações de resposta executadas pela aplicação.
4.6.27. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.
4.6.28. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:
4.6.29. Processo
4.6.30. Conexões de rede
4.6.31. Alterações no registro
4.6.32. Detalhes do download de objeto
4.6.33. A solução proposta deve fornecer orientação de resposta (resposta guiada).
4.6.34. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente

4.6.35. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
4.6.36. Impedir a execução de objetos
4.6.37. Isolamento de host
4.6.38. Excluir objeto do host ou grupo de hosts
4.6.39. Encerrar um processo no dispositivo
4.6.40. Colocar um objeto em quarentena
4.6.41. Execute a verificação do sistema
4.6.42. Execução remota de programa/processo/comando
4.6.43. Iniciar a varredura IoC para um grupo de hosts.

4.1. Requisitos para documentação da solução.
4.1.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:
4.1.2. Ajuda on-line para administradores
4.1.3. Ajuda on-line para melhores práticas de implementação
4.1.4. Ajuda on-line para proteção de servidores de administração
4.1.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.
4.2. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

5. PRAZO DE GARANTIA

5.1. As empresas licitantes deverão indicar o prazo da garantia do Software ou licença, que deverá ser de 36 meses oferecido diretamente ou com a autorização e responsabilidade do fabricante, sendo este o período em que se obrigam a prestar a manutenção e assistência técnica gratuita, nos termos regulados na minuta do contrato.

5.2. Serão desclassificadas as propostas que não ofereçam prazo de garantia ou abaixo do mínimo estipulado. As empresas licitantes indicarão, SOB PENA DE DESCLASSIFICAÇÃO, informações relacionadas à PADRONIZAÇÃO e COMPATIBILIDADE da solução, conforme detalhamento no ETP.

6. OBRIGAÇÕES DA CONTRATANTE

6.1. Comunicar à Contratada quaisquer irregularidades nos equipamentos, para adoção das providências cabíveis;

6.2. Designar funcionário para acompanhar/fiscalizar a entrega;

6.3. Efetuar os pagamentos relativos ao presente contrato em moeda corrente quando da apresentação da fatura de serviços executados respeitando os prazos de vencimentos;

6.4. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;

6.5. Qualquer alteração deste, somente deverá ser com o aval dos gestores do contrato;

6.6. Aplicar a contratada as sanções administrativas regulamentares e contratuais cabíveis;

7. OBRIGAÇÕES DA CONTRATADA

7.1. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

7.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do contrato, inerentes à execução do objeto contratual;

7.3. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

7.4. É de responsabilidade da CONTRATADA, manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

8. DA SUBCONTRATAÇÃO

8.1. Não será admitida a subcontratação do objeto.

9. MODELO DE EXECUÇÃO DO OBJETO

Em até, 30 dias, a contar da assinatura do contrato, as novas licenças deverão ser fornecidas e registradas em nome de CÂMARA MUNICIPAL DE FOZ DO IGUAÇU, nome fantasia PODER LEGISLATIVO, CNPJ 75.914.051/0001-28, atreladas a conta suporte@fozdoiguacu.pr.leg.br , dentro da plataforma da desenvolvedora Kaspersky Global.
Quando que realizada a disponibilização da licença, notificar via e-mail os responsáveis técnicos, sanches@fozdoiguacu.pr.leg.br e rodrigo@fozdoiguacu.pr.leg.br com detalhes do acesso.

10. MODELO DE GESTÃO DO CONTRATO E CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

A execução do objeto seguirá a seguinte dinâmica:

6.1 A contratante indicará Fiscal de contratos que irá acompanhar a execução do contrato em conformidade com este termo de referência.

6.2 O Contrato terá o prazo de 3 (três) anos, podendo ser prorrogado.

6.3 A Contratada formalizará a designação do preposto da empresa, especificando os poderes e responsabilidades relacionados à execução do objeto contratado.

6.4 Toda comunicação entre a Contratante e a Contratada deverá ser formalizada por escrito especialmente quando exigido por lei, podendo ser realizada por meio de mensagem eletrônica quando aplicável.

6.5 A execução será realizada de forma parcelada formalizada pelo envio da ordem de compra.

6.6 Os prazos e critérios para recebimento e pagamento estão detalhados nos itens 7.3 a 7.4.

6.7 Considera-se ocorrido o recebimento da nota fiscal quando a Gestão de contratos atestar a execução do objeto do contrato através do termo de recebimento definitivo.

6.8 Não haverá exigência de garantia contratual da execução, devido às características da

contratação.

6.9 A apresentação da Nota Fiscal/fatura é indispensável a cada fornecimento de bem ou serviço, para fins de liquidação e pagamento da despesa, emitida ao destinatário: Razão social: CÂMARA MUNICIPAL DE FOZ DO IGUACU; CNPJ: 75.914.051/0001-28; Endereço: Travessa Oscar Muxfeldt, nº 81, Centro, na cidade de Foz do Iguaçu-Paraná, CEP 85.851-490. Telefone: (45) 3521-8100.

6.10 Antes de cada pagamento à Contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

6.11 Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se- á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

6.12 Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

6.13 Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

6.14 Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 20 (vinte) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da Contratante.

6.15 Persistindo a irregularidade, a Contratante deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa.

6.16 Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso a Contratada não regularize sua situação junto ao SICAF.

6.17 O prazo desta contratação será de 36 meses, contados da assinatura do contrato.

6.18 Pagamento:

6.18.1 Os pagamentos serão efetuados até o 10° (décimo) dia após o recebimento definitivo dos bens, condicionado a apresentação da Nota Fiscal/Fatura, bem como os documentos de regularidade

fiscal, social e trabalhista exigidos pelo art. 68 da Lei n° 14.133/2021

6.18.2 Na eventualidade de ocorrer atraso no pagamento, o valor será atualizado pela variação acumulada do IPCA/IBGE, ocorrida entre a data de seu adimplemento e a do efetivo pagamento, calculada pro rata tempore.

7 Sanções:

7.1 Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei n° 14.133, de 2021, quais sejam:

7.2 Dar causa à inexecução parcial do contrato;

7.3 Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

7.4 Dar causa à inexecução total do contrato;

7.5 Deixar de entregar a documentação exigida para o certame;

7.6 Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

7.7 Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

7.8 Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

7.9 Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

7.10 Fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

7.11 Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

7.12 Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

7.13 Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;

7.14 O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Multa de até 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor,

b) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver

c) aplicado a sanção, pelo prazo máximo de 3 (três) anos.

d) Direta, quando não se justificar a imposição de penalidade mais grave;

e) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 8.9 a bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

8 A fiscalização do contrato será realizada pelo servidor(a) designado:

9 A gestão do contrato será realizada pelo servidor (a) designado:

11. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço.

Tratamento diferenciado e favorecido a ser dispensado às microempresas, às empresas de pequeno porte e aos microempreendedores individuais conforme definido pelo documento de estudo técnico preliminar (ETP).

12. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

As quantidades previstas a serem adquiridas, conforme os itens descritos, são:

Item	Descrição	SKU	Quantidade	Valor Unit.	Valor
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160	R$ 358,19	R$ 57.310,40

A pesquisa de preço foi realizada considerando os parâmetros dispostos da Lei 14.133 no art. 23 § inciso IV – *"pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital"*. Do qual optou-se pelo menor preço ofertado.

Quanto à não utilização dos parâmetros dos § Incisos I e II do Art. 23, consultas no portal PNCP (Inciso I) e contratações similares feitas pela Administração Pública (II), conforme descrito no parágrafo anterior, torna-se ineficaz e escassa a busca por contratações similares em outros órgãos. Regendo-se pela economicidade, melhor tecnologia e melhores resultados pretendidos pelo órgão, a consulta aos fornecedores torna-se mais eficaz.

13. ADEQUAÇÃO ORÇAMENTÁRIA

ITEM	DOTAÇÃO
1	01.01.01.031.0001.2002.3.3.90.40.99.05 - AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: ABC5-0F02-498C-9F1A

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

RODRIGO NISHIMORI (CPF 007.XXX.XXX-01) em 07/08/2024 11:21:12 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://fozdoiguacu.1doc.com.br/verificacao/ABC5-0F02-498C-9F1A

ESTUDO TÉCNICO PRELIMINAR

1) DESCRIÇÃO DA NECESSIDADE

1.1. Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

1.2. A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

1.3. Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

1.4. Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

1.5. Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

1.6. Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

1.7. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.

2) REQUISITOS DA CONTRATAÇÃO

Item	Descriçao	SKU	Quantidade
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160

3) LEVANTAMENTO DE MERCADO

Considerando que a Câmara Municipal de Foz do Iguaçu já dispõe de um sistema de antivírus, foram avaliadas duas alternativas sendo uma delas a renovação e upgrade de versão do sistema e a outra a aquisição de um sistema integrado com o nosso sistema de Firewall.

Mantendo os investimentos ocorridos no ano de 2018 (R$ 11.635) e 2021 (R$ 31.217,00 (Preço médio)) e já realizados, tendo em vista de que além da aquisição do sistema, foi também realizada no ano de 2023 (R$ 6.980,00) a contratação de uma empresa especializada para nos auxiliar na configuração recomendadas pelo fabricante, e com base nas pesquisa de preços e estudo entre outras soluções, por medida de economicidade optou-se pela renovação com upgrade da versão já utilizada do licenciamento da solução Kaspersky e aquisição de novas licenças de acordo com a

necessidade da CMFI , levando em consideração a ampliação do parque computacional que ocorreu nesses últimos anos e demandas futuras.

Notou-se ainda que a linha de produtos do desenvolvedor da solução passou por atualizações entregando novas versões de sua solução bem como mais recursos, a título de exemplo temos, portais de capacitação na solução, canais de suporte e a adoção da inteligência artificial para detecção e mitigação de vulnerabilidades.

4) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

As especificações do objeto desta licitação deverão estar detalhadas no termo de referência elaborado com base neste estudo técnico preliminar e de acordo com a solicitação elaborada pelo setor demandante.

5) ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

Item	Descrição	SKU	Quantidade	Valor
1	KASPERSKY NEXT EDR OPTIMUM 36 meses	KL4066KASTJ	160	R$ 57.310,40

Descrição Item 1

A solução deve incluir treinamento em segurança cibernética

Do módulo de proteção de endpoint

Compatibilidade com diferentes sistemas operacionais, MAC OS, Linux de 32 e 64 bits (CentOS, Red Hat Enterprise, Debian, Ubuntu, Oracle Linux), Windows 7, 8, 8.1, 10,11 para desktops, para servidores S.O Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022, Windows Small Business Server 2011, Servidores de terminal Microsoft (Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022).

Módulo de gerenciamento avançado

A solução deve suportar arquitetura cloud-native e on-premisse, a solução deve incluir suporte para implantação baseada em nuvem (Amazon Web Services e/ou Microsoft Azure. Integração nativa com as seguintes opções de SIEM (HP (Microfoco) ArcSight, IBM QRadar, Splunk, Kaspersky KUMA). 2.4.

A solução deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

A solução deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

A solução deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.
A solução deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.
O servidor de gerenciamento primário da solução deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.
A solução deve suportar os seguintes canais de entrega de notificação, E-mail, registro de sistema e SMS ou equivalente.
A solução deve ter a capacidade de etiquetar/marcar computadores com base em Atributos de rede, Nome, Domínio e/ou Sufixo de Domínio, Endereço de IP, Endereço IP para servidor de gerenciamento, Localização no Active Directory, Unidade organizacional, Grupo, Sistema operacional, Número do pacote de serviço, Arquitetura Virtual, Registro de aplicativos, Nome da Aplicação, Versão do aplicativo, Fabricante, Tipo e versão, Arquitetura.
A solução deverá permitir especificamente o bloqueio dos seguintes dispositivos, Bluetooth, Dispositivos móveis, Modems externos, CD/DVD, Câmeras e scanners.
A solução deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.
A solução deve permitir realizar as seguintes ações para endpoints, verificação manual, verificação no acesso, verificação por demanda, verificação de arquivos compactados, verificação de arquivos individuais, pastas e unidades, bloqueio e verificação de scripts, proteção contra alteração de registros, proteção contra estouro de buffer, verificação em segundo plano/inativa.

A solução deverá suportar os seguintes servidores de banco de dados:
Windows,

- Microsoft SQL Server
- Microsoft Banco de dados SQL do Azure
- MySQL Standard e Enterprise
- MariaDB
- PostgreSQL

Linux:

- MySQL
- MariaDB

- PostgreSQL

A solução deverá suportar as seguintes plataformas virtuais:

Windows:

- VMware vSphere 6.7 e 7.0
- Estação de trabalho VMware 16 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Oracle VM VirtualBox 6.x

2.74.2. Linux:

- VMware vSphere 6.7, 7.0 e 8.0
- VMware Desktop 16 Pro e 17 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 e 8.x

Do módulo de gerenciamento simplificado

A solução deve suportar arquitetura cloud;

A solução deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

A solução deve permitir ao administrador gerar relatórios pré-definidos.

A solução deve incluir informações do endpoint, IP público de internet, IP interno do dispositivo, Versão do agente de proteção, ultima comunicação com a console, contendo data e hora, informações do sistema operacional;

Requisitos gerais

A solução deve ser capaz de detectar os seguintes tipos de ameaças:
Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.
A solução deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
A solução deve ter capacidade de integração com a central de segurança do Windows Defender.
A solução deve suportar o subsistema Linux no Windows.
A solução deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

- Proteção contra ameaças sem arquivos (Fileless);
- Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

Do modulo de gerenciamento de dispositivos móveis

O modulo deve ser integrado a console de gerenciamento;
A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

- Android 5.0 ou posterior (incluindo Android 12L)

A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

- iOS 10–17 ou iPadOS 13–17

A solução deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

Do módulo de EDR

Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
A solução deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;

Deve apresentar informações detalhadas contendo:

- Usuário que executou a ação;
- Informações acesso privilegiado;

A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.

O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único).

6) IMPACTOS AMBIENTAIS

Não foram identificados impactos ambientes nesta contratação

7) JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Não se aplica, trata-se de um único item.

8) CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

Não se identificou contratações interdependentes e/ou correlatas, sendo que a prestação dos serviços depende exclusivamente do presente procedimento.

9) ALINHAMENTO COM PAC – PLANO ANUAL DE CONTRATAÇÕES

A demanda em questão encontra-se prevista no plano anual de contratações. Considerando que o mapa de gerenciamento de riscos tem natureza opcional, conforme previsto na NLL 14.133 e ato da presidência 133/2023.

10) RESULTADOS PRETENDIDOS

- Garantir um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;
- Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo estações de trabalho e notebooks comprometidos;
- Evitar, mitigar e conter a propagação de pragas digitais (vírus/malwares/spywares, spam, entre outros) com a administração centralizada da solução de proteção;

- Permitir o controle de acesso à rede por dispositivos computacionais, permitindo gerenciamento destes dispositivos;
- Possibilitar análise pormenorizada de arquivos, discos rígidos, unidades móveis, mensagens de e-mail e anexos, viabilizando detecção de ameaças, com intento de salvaguardar a estrutura tecnológica de ataques com teor e objetivo malicioso;
- Possibilitar o controle de acesso e tráfego de informações aos dispositivos e serviços operacionais na rede, através de gerenciamento centralizado, o que vem a complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;
- Aprimorar a segurança de TIC da CMFI frente a ameaças sofisticadas.

11) PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Tendo em vista que nosso ambiente de tecnologia já possui uma solução de firewall, não será necessária nenhuma providência prévia.

12) VIABILIDADE DA CONTRATAÇÃO

Esta equipe de TI declara viável esta contratação

13) TRATAMENTO DIFERENCIADO E FAVORECIDO A SER DISPENSADO ÀS MICROEMPRESAS, ÀS EMPRESAS DE PEQUENO PORTE E AOS MICROEMPREENDEDORES INDIVIDUAIS

Após diversas tentativas de localização e contato com empresas qualificadas como microempresas (ME) e empresas de pequeno porte (EPP) na região de Foz do Iguaçu para fornecimento das licenças, constatou-se a inexistência, inclusive pelo embasamento da pesquisa na base de de empresas credenciadas junto ao portal do desenvolvedor, acessado na data de 10/06/2024 às 09:38. Durante o processo de prospecção, entramos em contato direto com diversas empresas locais, incluindo aquelas registradas como ME e EPP, para verificar a capacidade técnica e a disponibilidade para fornecimento do serviço requerido. Nenhuma das ME/EPP contactadas demonstrou capacidade técnica ou interesse em participar do certame.

Diante dessas circunstâncias, a manutenção da exclusividade do certame para ME e EPP pode inviabilizar a contratação, comprometendo a eficiência e a continuidade dos serviços públicos dependentes de uma conexão estável e de alta velocidade, eis que

há sério risco da licitação ser deserta. Ressalta-se, porém, que as ME/EPP ainda poderão participar do certame com vantagens sobre os demais concorrentes conforme versa a legislação pátria.

Portanto, justifica-se o afastamento da exclusividade de participação de microempresas e empresas de pequeno porte neste certame específico, com base na inexistência de fornecedores locais qualificados e na necessidade imperiosa de garantir a prestação adequada e contínua dos serviços públicos.

14) RESPONSÁVEIS PELA ELABORAÇÃO DO ETP

Jeverson Siqueira
Cargo: Tecnico de Informatica
Matrícula: 202.045
Setor: Diretoria de Tecnologia

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: AD30-E329-B4EC-1FF9

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

JEVERSON SIQUEIRA (CPF 080.XXX.XXX-74) em 03/10/2024 08:41:08 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://fozdoiguacu.1doc.com.br/verificacao/AD30-E329-B4EC-1FF9

M I N U T A

CONTRATO Nº 19/2024

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS, QUE FAZEM ENTRE SI A CÂMARA MUNICIPAL DE FOZ DO IGUAÇU E A EMPRESA XXXXXXXXXXXXXXXXXX.

A **Câmara Municipal de Foz do Iguaçu**, pessoa jurídica de direito público, com sede em Foz do Iguaçu, Estado do Paraná, situada na Travessa Oscar Muxfeldt, 81, Centro, inscrita no CNPJ/MF sob o nº 75.914.051/0001-28, neste ato representada por seu Presidente, João José Arce Rodrigues, consoante competência originária prevista no art. 17 do Regimento Interno da Câmara Municipal de Foz do Iguaçu, daqui para frente denominada simplesmente de **CONTRATANTE,** e, de outro lado, a empresa XXXXXXXXXXXXXXXXXXXXXX, inscrita no CNPJ/MF sob o nº XXXXXXXXX/XXXX-XX, situado na XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, cidade de XXXXXXXXXX, Estado XXXXXXXXX, CEP: XX.XXX-XXX, representada por seu representante legal XXXXXXXXXXXXXXXXXXXXX, inscrito junto ao CPF/MF sob n. XXXXXXXXXX, a seguir denominada simplesmente **CONTRATADA**, firmam o presente contrato, sujeitando-se às cláusulas a seguir expostas e às normas da Lei n. 14.133/2021, têm entre si justo e contratado o que segue:

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O objeto do presente contratação de empresa especializada e tecnicamente qualificada para o fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 meses, de acordo com as características e especificações técnicas e, quantitativos descritos em termo de referência, bem como em seus anexos, conforme descrição a seguir:

ITEM	CAT/MAT	DESCRIÇÃO	QUANT.	UNIDADE	VALOR UNIT.	VALOR TOTAL
1	350949	KASPERSKY NEXT EDR OPTIMUM	160	Uni	R$ XXXXX,XX	R$ XXXXXX,XX
TOTAL						R$ XXXXXX,XX

2. CLÁUSULA SEGUNDA – DA VINCULAÇÃO

2.1. Os Contraentes reconhecem a vinculação desta contratação aos termos do Pregão Eletrônico n. XX/XXXX, emitido pela CONTRATANTE e à respectiva proposta que for vencedora, sendo que as

especificações técnicas mínimas do objeto, a fundamentação da contratação, a descrição da solução como um todo, as condições da garantia, os requisitos de habilitação, qualificação, técnica e capacidade operacional e de fornecimento, os requisitos da contratação, dentre outras informações, estão constantes em Termo de Referência, que é parte integrante deste Contrato independentemente de sua transcrição, ao qual também se declaram vinculados os contraentes.

3. CLÁUSULA TERCEIRA – DA LEGISLAÇÃO APLICÁVEL E DOS CASOS OMISSOS

3.1. Aplica-se a Lei n. 14.133/2021 à execução deste Contrato, sendo esta também a legislação a ser aplicadas aos casos omissos.

4. CLÁUSULA QUARTA – DO REGIME DE EXECUÇÃO

4.1. Os serviços serão executados sob o regime de execução indireta.

4.2. A execução dos serviços especificados neste Contrato e em Termo de Referência deverá ter início em até 30 dias, contados da assinatura do contrato, mediante fornecimento das licenças registradas em nome da CÂMARA MUNICIPAL DE FOZ DO IGUAÇU, nome fantasia PODER LEGISLATIVO, CNPJ n. 75.914.051/0001-28, atreladas a conta suporte@fozdoiguacu.pr.leg.br, dentro da plataforma da desenvolvedora Karpersky Global.

4.2. Quando realizada a disponibilização da licença, notificar via e-mail os responsáveis técnicos, sanches@fozdoiguacu.pr.leg.br e rodrigo@fozdoiguacu.pr.leg.br com detalhes do acesso.

4.3. Os serviços de instalação e manutenção deverão ser realizados na sede administrativa da CONTRATANTE, no endereço Travessa Oscar Muxfeldt, 81 - Centro, Foz do Iguaçu - PR, 85851-490

4.4. Os serviços a serem contratados constituem-se em atividades materiais acessórias, instrumentais ou complementares à área de competência legal da CONTRATANTE, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

4.5. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e a Administração, vedando-se qualquer relação entre elas que caracterize pessoalidade e subordinação direta.

4.6. Os serviços contratados são enquadrados como continuados, tendo em vista a sua necessidade permanente para a CONTRATANTE.

5. CLÁUSULA QUINTA – PREÇO

5.1. Em contra partida aos serviços prestados a CONTRATANTE pagará à CONTRATADA o valor mensal de até R$ XXXXX, totalizando estimativa de pagamento anual de até R$ XXXXX, conforme descrito na proposta apresentada pela empresa e constante no processo administrativo.

5.2. No valor indicado estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, seguro e outros necessários ao cumprimento integral do objeto da contratação.

6. CLÁUSULA SEXTA – DO REAJUSTE

6.1. Mediante expresso pedido da CONTRATADA, os valores contratados poderão ser reajustados a cada 12 (doze) meses, contados a partir da data da proposta apresentada pela CONTRATADA, com aplicação do índice de variação do ICTI – Índice de Custo da Tecnologia da Informação, calculado pelo IPEA, para o mesmo período ou outro índice que o substitua.
6.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de 12 (doze) meses para a próxima reajustamento, será contado a partir dos efeitos financeiros do último reajuste.
6.3. O reajuste previsto nesta cláusula poderá ser formalizado por Termo de Apostilamento.

7. CLÁUSULA SÉTIMA – DOS CRITÉRIOS DE MEDIÇÃO
7.1. Os Materiais entreguem dever estar em conformidade com as quantidades solicitadas dos itens já descritos neste documento;
7.2. A qualidade exigida dos equipamentos e materiais utilizados tem que estar de acordo com a qualidade de cada item, sendo vedada a utilização de materiais de qualidade inferior ou de não garantia.
7.3. Todos os pontos instalados devem ser certificados para assim constatar a qualidade do serviço e garantia de transmissão do mesmo.
7.4. Dos demais todos os itens devem ser novos seguidos rigidamente as especificações mínimas descritas na seção Requisitos da Contratação e amparados em seu prazo de garantia estabelecidos.

8. CLÁUSULA OITAVA – DO RECEBIMENTO
8.1. Os serviços serão recebidos provisoriamente no prazo de 05 (cinco) dias, para efeito de posterior verificação de sua conformidade com as especificações constantes na proposta;
8.2. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes na proposta, devendo ser substituídos no prazo de 10 (dez) dias, a contar da notificação da CONTRATANTE, às suas custas, sem prejuízo da aplicação das penalidades;
8.3. Na impossibilidade de realização dos serviços, a empresa vencedora deverá substituir o serviço por outro com especificações iguais ou superiores;
8.4. Os serviços serão recebidos definitivamente no prazo de 10 (dez) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação;
8.5. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo;
8.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

9. CLÁUSULA NONA – DO PAGAMENTO
9.1. Os pagamentos serão efetuados até o 10º (décimo) dia após o recebimento definitivo dos produtos/serviços, condicionado a apresentação da Nota Fiscal/Fatura, bem como os documentos de regularidade fiscal, social e trabalhista exigidos pelo art. 68 da Lei nº 14.133/2021.
9.2. Na eventualidade de ocorrer atraso no pagamento, o valor será atualizado pela variação acumulada do IPCA, ocorrida entre a data de seu adimplemento e a do efetivo pagamento, calculada pro rata tempore.

9.3. A apresentação da nota fiscal/fatura é indispensável a cada entrega de produtos ou prestação de serviços, para fins de liquidação e pagamento da despesa, a ser emitida ao destinatário: Razão social: CÂMARA MUNICIPAL DE FOZ DO IGUACU; CNPJ: 75.914.051/0001-28; Endereço: Travessa Oscar Muxfeldt, nº 81, Centro, na cidade de Foz do Iguaçu-Paraná, CEP 85.851-490. Telefone: (45) 3521-8100.
9.4. Antes de cada pagamento à CONTRATADA, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.
9.5. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se- á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.
9.6. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
9.7. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.
9.8. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua notificação, por escrito, para que, no prazo de 15 (quinze) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.
9.9. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.
9.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso a CONTRATADA não regularize sua situação junto ao SICAF.
9.11. O prazo desta contratação será de 36 meses, contados da assinatura do contrato.

10. CLÁUSULA DÉCIMA – DO PRAZO PARA RESPOSTA AOS PEDIDOS DE REPACTUAÇÃO DE PREÇOS E RESTABELECIMENTO DO EQUILÍBRIO ECONÔMICO

10.1. Quando for o caso de repactuação de preços e/ou de restabelecimento do equilíbrio econômico deste Contrato, será de 30 dias úteis o prazo resposta da CONTRATANTE, a contar da data de formalização do pedido por parte da CONTRATADA.

11. CLÁUSULA DÉCIMA PRIMEIRA - DA INEXIGÊNCIA DE GARANTIAS À EXECUÇÃO DO CONTRATO

11.1. Dadas as características da contratação, não haverá exigência de garantia à execução do contrato.

12. CLÁUSULA DÉCIMA SEGUNDA – DA GARANTIA DOS PRODUTOS E SERVIÇOS

12.1. As empresas licitantes deverão indicar o prazo da garantia do Software ou licença, que deverá ser de 36 meses oferecido diretamente ou com a autorização e responsabilidade do fabricante, sendo este o período em que se obrigam a prestar a manutenção e assistência técnica gratuita, nos termos regulados em termo de referência.

12.2. Serão desclassificadas as propostas que não ofereçam prazo de garantia ou abaixo do mínimo estipulado. As empresas licitantes indicarão, SOB PENA DE DESCLASSIFICAÇÃO, informações relacionadas à PADRONIZAÇÃO e COMPATIBILIDADE da solução, conforme detalhamento no ETP.

13. CLÁUSULA DÉCIMA TERCEIRA – DOTAÇÃO ORÇAMENTÁRIA

13.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da Câmara Municipal, para o exercício de 2024 nas classificações: item 1 – 01.01.01.031.0001.2002.3.3.90.40.99.05 – AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE.

13.2. Nos exercícios seguintes, correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

14. CLÁUSULA DÉCIMA QUARTA – DAS OBRIGAÇÕES DA CONTRATANTE

14.1. A CONTRATANTE obriga-se a:

14.1.1. Comunicar à Contratada quaisquer irregularidades nos equipamentos, para adoção das providências cabíveis;

14.1.2. Designar funcionário para acompanhar/fiscalizar a entrega;

14.1.3. Efetuar os pagamentos relativos ao presente contrato em moeda corrente quando da apresentação da fatura de serviços executados respeitando os prazos de vencimentos;

14.1.4. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;

14.1.5. Qualquer alteração deste, somente deverá ser com o aval dos gestores do contrato;

14.1.6. Aplicar a contratada as sanções administrativas regulamentares e contratuais cabíveis.

15. CLÁUSULA DÉCIMA QUINTA – DAS OBRIGAÇÕES DA CONTRATADA

15.1. A CONTRATADA obriga-se a:

15.1.1. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

15.1.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do contrato, inerentes à execução do objeto contratual;

15.1.3. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

15.1.4. É de responsabilidade da CONTRATADA, manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob

qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

16. CLÁUSULA DÉCIMA SEXTA – DAS SANÇÕES ADMINISTRATIVAS

16.1. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei n° 14.133, de 2021, quais sejam:

16.1.1. Dar causa à inexecução parcial do contrato;

16.1.2. Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

16.1.3. Dar causa à inexecução total do contrato;

16.1.4. Deixar de entregar a documentação exigida para o certame;

16.1.5. Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

16.1.6. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

16.1.7. Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

16.1.8. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

16.1.9. Fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

16.1.10. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

16.1.11. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

16.1.12. Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;

16.1.13. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

16.1.13.1. Multa de até 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor;

16.1.15. Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, quando não se justificar a imposição de penalidade mais grave;

16.1.16. Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 16.1.8 e bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

16.2. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao fornecedor.

17. CLÁUSULA DÉCIMA SÉTIMA - DA OBRIGAÇÃO DE MANUTENÇÃO DAS CONDIÇÕES DE QUALIFICAÇÃO

17.1. A CONTRATADA obriga-se a manter, durante toda a execução do Contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições para a qualificação na contratação direta que precedeu a este instrumento;

18. CLÁUSULA DÉCIMA OITAVA - DA OBRIGAÇÃO DE RESERVA DE CARGOS PREVISTA EM LEI

18.1. A CONTRATADA, durante toda a execução do Contrato, obriga-se a cumprir as exigências de reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz.

19. CLÁUSULA DÉCIMA NONA – MODELO DE GESTÃO DO CONTRATO

19.1. A execução do objeto seguirá a seguinte dinâmica:

19.1.1. A contratante indicará Fiscal de contratos que irá acompanhar a execução do contrato em conformidade com este termo de referência.

19.1.2. O Contrato terá o prazo de 3 (três) anos, podendo ser prorrogado.

19.1.3. A Contratada formalizará a designação do preposto da empresa, especificando os poderes e responsabilidades relacionados à execução do objeto contratado.

19.1.4. Toda comunicação entre a Contratante e a Contratada deverá ser formalizada por escrito, especialmente quando exigido por lei, podendo ser realizada por meio de mensagem eletrônica, quando aplicável.

19.1.5. A execução será realizada de forma parcelada formalizada pelo envio da ordem de compra.

19.1.6. Os prazos e critérios para recebimento e pagamento estão detalhados nas cláusulas 7 a 9 retro.

19.1.7. Considera-se ocorrido o recebimento da nota fiscal quando a Gestão de contratos atestar a execução do objeto do contrato através do termo de recebimento definitivo.

19.1.8. Não haverá exigência de garantia contratual da execução, devido às características da contratação.

20. CLÁUSULA VIGÉSIMA – DA INEXECUÇÃO E DA EXTINÇÃO DO CONTRATO

20.1. A inexecução total ou parcial do contrato ensejará a sua extinção com as consequências contratuais e as previstas em lei, com fulcro no Título III, Capítulo VIII da Lei n. 14.133/2021, nos seguintes modos:

20.1.1. determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta;

20.1.2. consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração;

20.1.3. determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

20.2. Constituirão motivos para extinção do contrato, a qual deverá ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa, as seguintes situações:

20.2.1. não cumprimento ou cumprimento irregular de normas editalícias ou de cláusulas contratuais, de especificações, de projetos ou de prazos;

20.2.2. desatendimento das determinações regulares emitidas pela autoridade designada para acompanhar e fiscalizar sua execução ou por autoridade superior;
20.2.3. alteração social ou modificação da finalidade ou da estrutura da empresa que restrinja sua capacidade de concluir o contrato;
20.2.4. decretação de falência ou de insolvência civil, dissolução da sociedade ou falecimento do contratado;
20.2.5. caso fortuito ou força maior, regularmente comprovados, impeditivos da execução do contrato;
20.2.6. atraso na obtenção da licença ambiental, ou impossibilidade de obtê-la, ou alteração substancial do anteprojeto que dela resultar, ainda que obtida no prazo previsto;
20.2.7. atraso na liberação das áreas sujeitas a desapropriação, a desocupação ou a servidão administrativa, ou impossibilidade de liberação dessas áreas;
20.2.8. razões de interesse público, justificadas pela autoridade máxima do órgão ou da entidade CONTRATANTE.
20.3. O descumprimento, por parte da CONTRATADA, de suas obrigações legais e/ou contratuais assegurará ao CONTRATANTE o direito de extinguir o contrato a qualquer tempo, independentemente de aviso, interpelação judicial e/ou extrajudicial.
20.4. A extinção por ato unilateral do CONTRATANTE sujeitará a CONTRATADA à multa rescisória de até 10% (dez por cento) sobre o valor do saldo do contrato existente na data da extinção, independentemente de outras penalidades.
20.5. Caso o valor do prejuízo do CONTRATANTE advindo da extinção contratual por culpa da CONTRATADA exceder o valor da Cláusula Penal prevista no parágrafo anterior, esta valerá como mínimo de indenização, na forma do disposto no art. 416, parágrafo único, do Código Civil.
20.6. A extinção determinada por ato unilateral da Administração e a extinção consensual deverão ser precedidas de autorização escrita e fundamentada da autoridade competente e reduzidas a termo no respectivo processo.
20.7. A CONTRATANTE poderá rescindir o presente instrumento contratual, sem qualquer ônus à Administração, quando da conclusão de eventual novo procedimento de contratação de interesse público para objeto afim.

21. CLÁUSULA VIGÉSIMA PRIMEIRA – DA VIGÊNCIA

21.1. O presente Contrato terá validade de 36 (trinta e seis) meses, contados da data da assinatura, podendo ser prorrogado, a critério da Administração, conforme o disposto no art. 107, da Lei n. 14.133/2021 e suas alterações posteriores.
21.2. A prorrogação deste contrato deverá ser promovida mediante celebração de termo aditivo.

22. CLÁUSULA VIGÉSIMA SEGUNDA – DA FISCALIZAÇÃO

22.1. O acompanhamento e a fiscalização da execução das obrigações oriundas deste contrato ficarão a cargo do Gestor José Marceo Nicoletti Teixeira, e do Fiscal de Contratos, Jeverson Siqueira, e consiste na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais

representantes da CONTRATANTE, especialmente designados, na forma do art. 117 da Lei nº 14.133/2021.
22.2. O fiscal do contrato deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 117 da Lei nº 14.133/2021.
22.3. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela CONTRATADA ensejará a aplicação de sanções administrativas, previstas neste Termo de Contrato e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 156 e 137 da Lei nº 14.133/2021.
22.4. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da CONTRATANTE ou de seus agentes e prepostos, de conformidade com art. 120 da Lei nº 14.133/2021.

23. CLÁUSULA VIGÉSIMA TERCEIRA – DA SUBCONTRATAÇÃO
23.1. É vedada a subcontratação total ou parcial do objeto deste Termo de Contrato.

24. CLÁUSULA VIGÉSIMA QUARTA – DAS VEDAÇÕES
24.1. É vedado à CONTRATADA:
24.1.1. Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;
24.1.2. Interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

25. CLÁUSULA VIGÉSIMA QUINTA – DAS ALTERAÇÕES
25.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos art. 124 a 136 da Lei n. 14.133/2021.

26. CLÁUSULA VIGÉSIMA SEXTA – DA PUBLICAÇÃO
26.1. A CONTRATANTE providenciará a publicação deste contrato no Diário Oficial do Município de Foz do Iguaçu, na página da Câmara Municipal de Foz do Iguaçu nos termos do art. 174 da Lei n. 14.133/2021 e no Portal Nacional de Contratações Públicas (PNCP), para fins de garantia a ampla publicidade.

27. CLÁUSULA VIGÉSIMA SÉTIMA – DO FORO
27.1. Fica eleito o foro desta cidade de Foz do Iguaçu, Estado do Paraná, para dirimir toda e qualquer questão que derivar deste contrato.

E por estarem justas e acordadas, assinam as partes o presente instrumento, na presença de duas testemunhas, que também o subscrevem, para que surtam todos os efeitos jurídicos e legais.

Foz do Iguaçu, xx de xxxxx de 2024.

CÂMARA MUNICIPAL DE FOZ DO IGUAÇU
João José Arce Morales

XXXXXXXXXXX
xxxxxxxxxxx

Testemunhas:

_____
Nome: XXXXXX
RG: XXXXXX
CPF: XXXXXXX

_____
Nome: XXXXXXXXX
RG: XXXXXXX
CPF XXXXXX

ANEXO IV - MODELO DE PROPOSTA DE PREÇOS
PREGÃO, NA FORMA ELETRÔNICA, Nº 0x/2024

REF: PREGÃO, NA FORMA ELETRÔNICA, Nº 0x/2024-TIPO MENOR PREÇO

A empresa _____, estabelecida na _____, no bairro _____, no Município de _____, no Estado de _____, no n.º _____, na Prefeitura sob o n.º_____ e no Estado sob o nº_____, CNPJ n.º_____, telefone n.º (____) _____ e e-mail _____, pela presente e consoante as especificações técnicas contidas no Edital, vem propor os valores abaixo para fornecimento de licenças antivírus do Pregão, na forma Eletrônica, n° **0x/2024**, conforme segue:

ITEM	DESCRIÇÃO	SKU	QNT	VALOR UNITÁRIO	VALOR TOTAL
1	Licença Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal license	KL4066KASTJ	160		

O **PREÇO TOTAL** apresentado na presente proposta é de R$ _____ (valor por extenso).

Nesta proposta de percentual de desconto e preço estão considerados obrigatoriamente:

a) **O atendimento às especificações detalhadas do objeto, consoante Anexo I deste Edital;**
b) **A inclusão de todas as despesas que influenciam nos custos, tais como despesas com custo, transporte e frete, tributos (impostos, taxas, emolumentos, contribuições fiscais e parafiscais), obrigações sociais, trabalhistas, fiscais, encargos comerciais ou de qualquer natureza e todos os ônus diretos e indiretos,**
c) **O prazo de validade da proposta é de 90 (noventa) dias, a contar da data da sessão do pregão, na forma eletrônica.**

Esta empresa declara que está ciente e cumprirá, integralmente, todas as cláusulas do EDITAL retro citado.

Foz do Iguaçu, _____ de _____ de _____.

_____

Assinatura do representante legal da empresa proponente
NOME:
RG:
CARGO:

Proc. Administrativo 30- 279/2024

De: CARLOS K. - AGCONT

Para: Envolvidos internos acompanhando

Data: 15/10/2024 às 08:41:20

Felipe Gomes Cabral - CMFI-PRESID-DG-ATDG-DIRJUR-EADJpara análise.

–

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras

Proc. Administrativo 31- 279/2024

De: Felipe C. - CMFI-PRESID-DG-ATDG-DIRJUR-EADJ

Para: AGCONT - Agente de contratação

Data: 17/10/2024 às 13:12:44

_

Felipe Gomes Cabral – Consultor Jurídico, OAB/PR86944, mat. 202.053.

Documento assinado, datado e validado eletronicamente pelo sistema 1Doc, Sistema Eletrônico oficial da Câmara dos Vereadores de Foz do Iguaçu.

Anexos:

Parecer_299_2024_1_doc_pregao_inicial_servicos_antivirus_kaspersky.pdf

---

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Felipe Gomes Cabral	17/10/2024 13:12:58	1Doc	FELIPE GOMES CABRAL CPF 067.XXX.XXX-40

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **45F0-435D-5552-24F4**

PARECER Nº 299/2024 de 17/10/2024

PROCESSO ADMINISTRATIVO nº 180/2024 – Pregão Eletrônico (a numerar) – CRITÉRIO DE JULGAMENTO: MENOR PREÇO POR ITEM

ORIGEM: DIRETORIA DE SEGURANÇA FÍSICA E DIGITAL

OBJETO: Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

Valor estimado: R$ 57.310,40 (cinquenta e sete mil, trezentos e dez reais e quarenta centavos).

Ementa: DIREITO ADMINISTRATIVO. LICITAÇÕES E CONTRATOS. PREGÃO ELETRÔNICO. CONTRATAÇÃO DE SERVIÇOS COMUNS. MINUTA DE EDITAL. ANÁLISE JURÍDICA PRÉVIA. ART. 53, *CAPUT* E §1º DA LEI Nº 14.133/2021. ANÁLISE JURÍDICA DO PROCEDIMENTO E DAS MINUTAS. PROCEDIMENTO SUFICIENTEMENTE INSTRUÍDO. RESSALVAS E RECOMENDAÇÕES. POSSIBILIDADE DE PROSSEGUIMENTO DO FEITO APÓS OBSERVAÇÕES DOS APONTAMENTOS.
1. o pregão é modalidade de licitação obrigatória para aquisição de bens e serviços comuns, cujo critério de julgamento poderá ser o de menor preço ou o de maior desconto, conforme prescreve o art. 6º, XLI da Lei nº 14133/2021;
2. o ETP e TR devem sempre verificar o atendimento do conteúdo mínimo obrigatório previsto na normatização regente (arts. 6º, XX; 18, I; § 1º, § 2º, da Lei nº 14.133/2021 e IN nº 58/2022-ME/SEGES; e arts. 6º, XXIII; 18, II, 40, §1º, da Lei nº 14.133/2021 e IN nº 81/2022-SEGES-ME);
3. pesquisa de preço em procedimento de contratação que segue o rito do art. 23, *caput* e §1º, da Lei nº 14.133/2021 e AP136/2023, bem como subsidiariamente IN nº 65/2021-SEGES/ME que tratam sobre a pesquisa de preço em procedimentos licitatórios;
4. procedimento suficientemente instruído que, no entanto, comporta ressalvas e recomendações para sua regularidade;
5. possibilidade de prosseguimento do feito após observação e prévio cumprimento dos apontamentos.

Travessa Oscar Muxfeldt, nº 81, Centro / Foz do Iguaçu, PR - CEP: 85851-490 / Fone/FAX: (45) 3521-8100

1. RELATÓRIO

A Comissão de Pregão desta Câmara Municipal solicita parecer sobre a fase interna de processo licitatório, na modalidade pregão eletrônico do tipo menor preço por item, para aquisição do objeto epigrafado.

A análise da Minuta do Edital se faz necessária em cumprimento ao disposto no art. 53, *caput* e §1º, bem como arts. 11 ao 18, arts. 40 e 44, todos da Lei nº 14.133/2021, que dispõem sobre **fase interna de contratação**. Aplicável ainda os arts. 6º, XLI, art. 7º, §5º, 28, I, 29 e seu respectivo parágrafo único, todos da Lei nº 14.133/2021, que tratam da modalidade de licitação do **pregão eletrônico**.

Consta do expediente, em síntese: autorização de abertura de processo licitatório, memorando de encaminhamento da demanda, DFD, ETP, TR, relatório de pesquisa de preços, cotações, declaração de adequação orçamentária, portarias de nomeação do pregoeiro/agente de contratação; minuta do Edital e minuta de contrato e outros documentos complementares, bem como manifestações e despachos de trâmite processual pelo sistema eletrônico utilizado para trâmite da contratação (Plataforma 1Doc).

O processo tramita desde 6 de agosto de 2024 e foi submetido para análise na data de 15 de outubro de 2024.

Os documentos pertinentes encontram-se devidamente assinados e o procedimento demonstra ter sido elaborado com suficiente segregação de funções.

Elaborados os documentos, o feito é encaminhado para análise da Consultoria Jurídica em sede de parecer opinativo prévio sobre o procedimento licitatório.

É o relatório, passo à fundamentação.

2. FUNDAMENTAÇÃO

A presente manifestação jurídica tem o escopo de assistir a autoridade assessorada no controle prévio de legalidade, conforme estabelece o artigo 53, § 1º, I e II, da Lei nº 14.133/2021.

> Art. 53. Ao final da fase preparatória, o processo licitatório seguirá para o órgão de **assessoramento jurídico da Administração**, que realizará **controle prévio de legalidade mediante análise jurídica da contratação**.
> § 1º Na elaboração do parecer jurídico, o órgão de assessoramento jurídico da Administração deverá:

Travessa Oscar Muxfeldt, nº 81, Centro / Foz do Iguaçu, PR - CEP: 85851-490 / Fone/FAX: (45) 3521-8100

I - apreciar o processo licitatório conforme critérios objetivos prévios de atribuição de prioridade;
II - redigir sua manifestação em linguagem simples e compreensível e de forma clara e objetiva, com apreciação de todos os elementos indispensáveis à contratação e com exposição dos pressupostos de fato e de direito levados em consideração na análise jurídica;

A finalidade deste parecer jurídico é orientar o Gestor Público quanto às exigências legais para a prática de determinado ato administrativo sob o aspecto jurídico-formal. Ressalte-se que o presente arrazoado tem caráter meramente opinativo, não vinculando o administrador em sua decisão, conforme entendimento exarado pelo Supremo Tribunal Federal no Mandado de Segurança nº 24.073/DF, da relatoria do Ministro Carlos Velloso, e ainda, ressalta-se que a presente manifestação cinge-se a análise estritamente jurídica, de acordo com os documentos fornecidos pelo consultante, não adentrando em critérios técnicos (orçamentário, contábil, detalhamento) outros ou de oportunidade e conveniência da Administração, salvo teratologia.

No que respeita aos limites do presente opinativo, necessário esclarecer que não compete a esta assessoria jurídica investigar todo o procedimento, o que é de competência dos órgãos de controle. A decisão pela contratação é da Administração Superior, que deve ter como norte o atendimento do interesse público, bem como obedecer aos princípios elencados pela Lei de Licitações. No mesmo sentido é da Gestão e da origem a obrigação pela aferição dos preços praticados no mercado, bem como da capacidade técnica, regularidade jurídica e fiscal da eventual contratada.

A decisão final pela contratação é da Administração desta Câmara Municipal, que deve ter como norte principal o atendimento do interesse público, aliado aos princípios elencados nos art. 37 da CF/88 e art. 5º da Lei nº 14.133/2021.

Quanto à composição do processo, em linhas gerais, é possível atestar razoabilidade em sua instrução, com a documentação e informações essenciais e pertinentes, consoante normatização regente, ressaltando-se a autorização superior, planejamento e previsão orçamentária para custeio da contratação, cujo objeto, devidamente definido, enquadra-se em hipótese licitável via pregão eletrônico do tipo menor preço para a contratação dos serviços comuns do objeto de informática.

O agente responsável pela contratação foi devidamente indicado por portaria de designação, atendendo o §5º do art. 8º da Lei nº 14.133/2021. Pode ser ressaltada ainda constatação de planejamento e previsão orçamentária para custeio da contratação.

Em atendimento ao Ato da Presidência nº 133/2023, e no mesmo sentido do que dispõe subsidiariamente as IN58/2022-SEGES e IN81/2023-SEGES quanto à necessidade de

Travessa Oscar Muxfeldt, nº 81, Centro / Foz do Iguaçu, PR - CEP: 85851-490 / Fone/FAX: (45) 3521-8100

utilização de documentos eletrônicos, a origem apresenta documentos com assinatura em plataforma própria da Câmara Municipal, sendo utilizado o 1Doc para a assinatura e validação de documentos, bem como o trâmite processual que se dá também por plataforma eletrônica oficialmente adotada, o que entendo adequado.

Entendo pertinente a escolha da modalidade para o procedimento licitatório, em vista de que o pregão é modalidade de licitação obrigatória para aquisição de bens e serviços comuns, cujo critério de julgamento poderá ser o de menor preço ou o de maior desconto, conforme prescreve o art. 6º, XLI da Lei nº 14133/2021.

DOS ESTUDOS TÉCNICOS PRELIMINARES (ETP)

Em relação aos documentos elaborados pela origem demandante, entendo que o ETP, fundamentadamente, apresenta a demanda e indica a solução mais adequada, porém, resta **parcialmente adequado**. O ETP apresentado está suficientemente adequado às formalidades arts. 6º, XX; 18, I; § 1º, § 2º; Ato da Presidência nº 133/2023 e subsidiariamente à IN nº 58/2022 que regram a hipótese, no entanto, ressalvo pela necessidade de revisão material de algumas de suas disposições.

Na página 2 a 3 dos Estudos Técnicos Preliminares que constam do despacho 28 do presente processo, assim foi a manifestação da origem em relação à pesquisa de mercado:

> 3) LEVANTAMENTO DE MERCADO Considerando que a Câmara Municipal de Foz do Iguaçu já dispõe de um sistema de antivírus, foram avaliadas duas alternativas sendo uma delas a renovação e upgrade de versão do sistema e a outra a aquisição de um sistema integrado com o nosso sistema de Firewall. Mantendo os investimentos ocorridos no ano de 2018 (R$ 11.635) e 2021 (R$ 31.217,00 (Preço médio)) e já realizados, tendo em vista de que além da aquisição do sistema, foi também realizada no ano de 2023 (R$ 6.980,00) a contratação de uma empresa especializada para nos auxiliar na configuração recomendadas pelo fabricante, e com base nas pesquisa de preços e estudo entre outras soluções, por medida de economicidade optou-se pela renovação com upgrade da versão já utilizada do licenciamento da solução Kaspersky e aquisição de novas licenças de acordo com a necessidade da CMFI , levando em consideração a ampliação do parque computacional que ocorreu nesses últimos anos e demandas futuras. Notou-se ainda que a linha de produtos do desenvolvedor da solução passou por atualizações entregando novas versões de sua solução bem como mais recursos, a título de exemplo temos, portais de capacitação na solução, canais de suporte e a adoção da inteligência artificial para detecção e mitigação de vulnerabilidades.

Travessa Oscar Muxfeldt, nº 81, Centro / Foz do Iguaçu, PR - CEP: 85851-490 / Fone/FAX: (45) 3521-8100

Em relação à pesquisa de mercado, **ressalvo** que embora tenha sido justificado por vantagem econômica e razoabilidade na adoção da mesma solução hoje já utilizada, não houve levantamento específico de demais soluções que possam dar alternativas ao gestor em relação à contratação.

Nesse sentido, entende-se que os autos do processo administrativo devem ser instruídos com Estudo Técnico Preliminar completo, assim como, a justificativa técnica da vantajosidade da solução proposta, bem como indicativo das demais soluções alternativas existentes no mercado, conforme art. 18, §1°, L14.133/2021.

Assim sendo, alertando-se ao gestor pela parcial instrução do ETP quanto ao levantamento de mercado, orienta-se que cabendo a ele a decisão final pela contratação, deve manifestar fundamentadamente pelo acolhimento das razões apresentadas para a escolha da atuação indicada pela equipe técnica, ou se necessário, determinar estudos complementares e apresentação de demais soluções para indicação definitiva do objeto a ser contratado.

DO PLANO DE CONTRATAÇÕES ANUAL

Em relação ao demonstrativo da previsão da contratação no plano de contratações anual, de modo a indicar o seu alinhamento com o instrumentos de planejamento do órgão ou entidade, foi apresentado o Plano Anual de Contratações da Câmara Municipal, bem como foi expressamente indicado nos Despachos 1 e 2 do processo em análise pela regularidade do planejamento e previsão no plano, o que, sob responsabilidade o setor que indicou a previsão, entendo regular.

DO TERMO DE REFERÊNCIA (TR)

Não sendo adequada manifestação jurídica sobre o descritivo técnico de item de informática descrito sob responsabilidade da origem, entendo que o termo de referência reúne suficientes requisitos necessários à qualificação e atendimento da necessidade pública em voga, conforme motivação da origem, estando razoavelmente adequado ao disposto nos arts. 6°, XXIII; 18, II, 40, §1°, Ato da Presidência n° 133/2023 e subsidiariamente IN n° 81/2022 que regram a hipótese.

Recomendo pela revisão, em reiteração à recomendação que já consta do despacho 16 do presente processo da numeração de itens que constam da página 20 em diante do edital e da página 4 em diante do Termo de Referência, que por sua quebra de sequência pode causar confusão aos licitantes em sede de estudo do edital e eventual impugnação/questionamento que depende de indicação numérica do item, o que pode ser objeto de apontamento.

Travessa Oscar Muxfeldt, nº 81, Centro / Foz do Iguaçu, PR - CEP: 85851-490 / Fone/FAX: (45) 3521-8100

DA PESQUISA DE PREÇOS

Noto que para composição da cesta de preços foi utilizada e justificada a metodologia de menor dos valores (despacho 27). A origem forneceu documento específico de cotação (relatório de pesquisa de preços e tabelamento de valores), tendo como parâmetros pesquisas com fornecedores, justificando tecnicamente pela falta de consultas a fontes de contratações públicas ou consultas ao PNCP.

Pelas razões do RPP e pelos documentos apresentados, entendo que o feito resta razoavelmente adequado ao art. 23, *caput* e §1°, da Lei nº 14.133/2021 e AP136/2023, bem como subsidiariamente IN nº 65/2021-SEGES/ME que tratam sobre a pesquisa de preço em procedimentos licitatórios. Ademais de razoável a justificativa da escolha do método de aferição (menor preço), não cabe a esta Consultoria, contudo, atestar pela veracidade dos relatórios e seus anexos, sendo de incumbência exclusiva da origem.

Entretanto, noto das cotações referenciais constantes do **despacho 8** do presente processo que a proposta da empresa Avant Services e da empresa Solo Network não têm assinatura, o que **deve ser suprido ou convalidado** para que tenha serventia legal.

DA MINUTA DO EDITAL

Noto que a minuta do edital (arts. 18, V da Lei nº 14.133/2021, AP134/2023 e subsidiariamente IN nº 73/2022 que trata de licitação eletrônica com julgamento por menor preço) segue o modelo padronizado pela Comissão de Pregão desta Câmara, contendo as adequações cabíveis ao caso concreto, ademais dos elementos essenciais e pertinentes ao regular processamento do feito e final contratação: preâmbulo, condições de participação, condições de participação, modo de disputa, vistoria, cadastramento da proposta, sessão pública, fase de disputa/verificação das propostas, formulação de lances, benefícios ME e EPP, julgamento, negociação, aceitabilidade da proposta, habilitação, verificação e solicitação da habilitação, declaração do vencedor, recurso, adjudicação/homologação, assinatura do contrato, penalidades, impugnação ao edital, disposições gerais.

O edital aponta, com base em critérios legais e discricionários, pelo afastamento das cotas pertinentes para licitação exclusiva de itens para ME/EPP e equiparados. Com esteio na LC nº 123/2006, bem como por toda a fundamentação apresentada pela origem, entendo possível o prosseguimento da contratação nos moldes apresentados quanto aos itens.

Não constando expressamente prevista a data de abertura na minuta apresentada, ressalto necessária adequação ao mínimo de 10 (dez) dias úteis para a apresentação de proposta, contados a partir do 1º dia útil subsequente à data de

Travessa Oscar Muxfeldt, nº 81, Centro / Foz do Iguaçu, PR - CEP: 85851-490 / Fone/FAX: (45) 3521-8100

divulgação do edital, com esteio nos arts. 55, II, "a" da nº Lei 14.133/2021, art. 16 do AP134/2023 e art. 17, I da INº 73/2022.

Ainda, não consta do edital previsão de aplicação ou afastamento quanto aos preceitos que da Lei Complementar Municipal nº 369/2022 em relação ao tratamento diferenciado especificamente previsto nas normas do Município. Em vista da norma municipal em vigor, **ressalvo** deve ser apresentada manifestação pela aplicação ou afastamento da margem aplicada por lei municipal.

DA MINUTA DO CONTRATO

Foi apresentada minuta de contrato, tratando-se de documento adequado ao caso concreto, podendo ser o instrumento considerado razoavelmente adequado ao que prescrevem os 89 e 92. As multas foram parametrizadas conforme prevê o edital e tabela padrão aplicada costumeiramente pela Câmara Municipal.

Por fim, é possível verificar que a fase de planejamento concluída atendeu, no cabível, as considerações previstas no art. 18 da Lei nº 14.133/2021. Em especial quanto ao ETP e TR, é possível verificar o atendimento do conteúdo mínimo obrigatório previsto na normatização regente (arts. 6º, XX; 18, I; § 1º, § 2º, da Lei nº 14.133/2021 e IN nº 58/2022-ME/SEGES; e arts. 6º, XXIII; 18, II, 40, §1º, da Lei nº 14.133/2021 e IN nº 81/2022-SEGES-ME).

Não obstante, devem ser previamente observadas as ressalvas e recomendações que constam do presente.

III. CONCLUSÃO

Logo, desde que previamente observadas as ressalvas e recomendações supra**, OPINO** pela possibilidade de prosseguimento do feito, com a deflagração da fase externa, observadas as demais disposições da Lei nº 14.133/2021, Ato da Presidência nº 134/2023 e Lei Complementar nº 123/2006.

Com prosseguimento do feito, a publicidade do edital de licitação será realizada mediante divulgação e manutenção do inteiro teor do ato convocatório e de seus anexos no **Portal Nacional de Contratações Públicas (PNCP)** no prazo de 20 (vinte) dias (art. 54 e parágrafos c/c art. 94, I da Lei nº 14.133/2021).

É o parecer.

Foz do Iguaçu, data e assinatura por certificação do sistema digital (sistema 1Doc).

Travessa Oscar Muxfeldt, nº 81, Centro / Foz do Iguaçu, PR - CEP: 85851-490 / Fone/FAX: (45) 3521-8100

Proc. Administrativo 32- 279/2024

De: CARLOS K. - CMFI-PRESID-DG-DIRFIN-COM

Para: CMFI-PRESID - Presidência

Data: 17/10/2024 às 13:41:02

Considerando a indicação de fl. 5 do Parecer retro, para ciência e decisão da presidência.

–

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras

Proc. Administrativo 33- 279/2024

De: Presidente I. - CMFI-PRESID

Para: CMFI-DG-DIRTEC - Diretoria de Tecnologia

Data: 18/10/2024 às 18:31:33

Ciente. Vem para análise expediente para decisão, diante do **Despacho 32- 279/2024,** no que tange a recomendação de revisão material de algumas disposições do ETP, especialmente quanto a eventual ausência de levantamento específico de demais soluções que possam dar alternativas ao gestor em relação a contratação.

No ETP anexado no **Despacho 28- 279/2024** consta que: "*foram avaliadas duas alternativas sendo uma delas a renovação e upgrade de versão do sistema e a outra a aquisição de um sistema integrado com o nosso sistema de Firewall*." Ou seja, a equipe técnica avaliou a atual ferramenta e as demais existentes no mercado, entendendo que a melhor alternativa para a CMFI é a renovação com a atual ferramenta e, ainda, realizando um *upgrade* na mesma. Evidente que a área demandante quem detém o conhecimento adequado para realizar tal avaliação, sendo que não foram apontados ilegalidades ou irregularidades no procedimento, mas sim eventual ausência de comprovações de pesquisa de outras alternativas, o que a área certifica que realizou. Trata-se de demanda que visa melhorar a segurança do ambiente virtual da CMFI, logo, de suma importância que se busque uma ferramenta mais eficaz e que atenda amplamente a necessidade.

Além disso, foram indicados valores já gastos na atual ferramenta, devendo ser considerado ainda que os Servidores já utilizam a ferramenta e, consequentemente detém o conhecimento de manejo da mesma, habituados com situações de criticidade, suporte, entre outras facilidades. Ainda, maior confiabilidade de utilização correta, com a imediata e ampla proteção, evitando maiores gastos com tempo em treinamento, suporte ou até mesmo ajuste para eventuais compatibilidades de sistemas.

Vale ressaltar o ponto em questão também, conforme mencionado no **Despacho 22- 279/2024** da lavra da Direção Geral da CMFI, que assim disserta: *"a Diretoria de Tecnologia, área especializada, é detentora de capacidade técnica para dimensionar a demanda e as necessidades atuais e futuras e, diante disso, a melhor alternativa para a solução e atendimento, o que deve ser considerado. Ainda, amplamente dissertado e debatido é que a melhor contratação para os órgãos públicos não são aquelas com o menor preço, mas sim, aquelas que efetivamente atendam a necessidade da demanda que se pretende suprir com a compra/contratação."*

Diante do exposto, com a fundamentação e motivação acima entendo suprida a ressalva e a recomendação do Parecer nº 299/2024, da Diretoria Jurídica desta Casa de Leis, determinando o prosseguimento do expediente com a deflagração da fase externa do procedimento.

No que tange as demais recomendações, referente a numeração dos itens do TR e do Edital, em que pese pertinente, entendo desnecessária correção, eis que não há duplicidade dos itens ou numerações, considerando ainda a urgência da demanda.

Entretanto, encaminho à Diretoria de Tecnologia para atender a ressalva referente as *"cotações referenciais constantes do despacho 8 do presente processo que a proposta da empresa Avant Services e da empresa Solo Network não têm assinatura,* ***o que deve ser suprido ou convalidado*** *para que tenha serventia legal"*.

Com a referida providência, encaminhe-se ao Agente de Contratações para prosseguimento.

Att,

_

João Morales

Presidente da Câmara Municipal de Foz do Iguaçu

Proc. Administrativo 34- 279/2024

De: Rafael A. - CMFI-DG-DIRTEC

Para: Envolvidos internos acompanhando

Data: 18/10/2024 às 20:32:12

Em atendimento ao despacho de numero 33 constante no processo eletronico de numero 279/2024, anexamos os fluxos de e-mails trocados com as empresas citadas no referido despacho.

–

Rafael Sanches
Diretoria de Tecnologia

Anexos:

E_mail_de_CAMARA_MUNICIPAL_DE_FOZ_DO_IGUACU_Solicitacao_de_orcamento_para_renovacao_Kaspersky_Avant.pdf
E_mail_de_CAMARA_MUNICIPAL_DE_FOZ_DO_IGUACU_Solo_Network___Proposta_Comercial_P24_570597A___Kaspersky.pdf

Câmara de Foz

Rafael Sanches <sanches@fozdoiguacu.pr.leg.br>

Solicitação de orçamento para renovação [Kaspersky]

6 mensagens

Rafael Sanches <sanches@fozdoiguacu.pr.leg.br> 8 de julho de 2024 às 09:54
Para: bianca.bombonato@avantservices.com.br

Bom dia Bianca, em nome da Câmara Municipal de Foz do Iguaçu (75.914.051/0001-28), gostaríamos de solicitar orçamento de renovação e upgrade de versão, para o seguinte produto:

Item	Descrição	SKU	Quantidade
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160

--

Rafael Sanches <sanches@fozdoiguacu.pr.leg.br> 12 de julho de 2024 às 15:13

Para: bianca.bombonato@avantservices.com.br, Rodrigo Nishimori <rodrigo@fozdoiguacu.pr.leg.br>

Boa tarde Binca, tudo bem?

Enviamos pedido de orçamento, você tem interesse em fornecer? Pergunto por que não recebi retorno.

[Texto das mensagens anteriores oculto]

--

Bianca Bombonato <bianca.bombonato@avantservices.com.br> 12 de julho de 2024 às 15:48

Para: Rafael Sanches <sanches@fozdoiguacu.pr.leg.br>, Rodrigo Nishimori <rodrigo@fozdoiguacu.pr.leg.br>

Olá Rafael, tudo bem?

Peço desculpas pela demora.

Farei o envio ainda hoje.

Atenciosamente,

Bianca Bombonato
Product Manager
(44) 4003-4912 / (11) 9 7723-2059
avantservices.com.br

AVANT

Fale comigo
no whatsapp

[Texto das mensagens anteriores oculto]

Bianca Bombonato <bianca.bombonato@avantservices.com.br> 12 de julho de 2024 às 16:13
Para: Rafael Sanches <sanches@fozdoiguacu.pr.leg.br>
Cc: Rodrigo Nishimori <rodrigo@fozdoiguacu.pr.leg.br>

Boa tarde Rafael, tudo bem?

Segue em anexo proposta comercial para sua análise.

Coloco-me à disposição

Atenciosamente,

Bianca Bombonato
Product Manager
(44) 4003-4912 / (11) 9 7723-2059
avantservices.com.br

AVANT

Fale comigo
no whatsapp

Proposta - CAMARA MUNICIPAL DE FOZ DO IGUACU.pdf
197K

Rafael Sanches <sanches@fozdoiguacu.pr.leg.br> 12 de julho de 2024 às 16:22
Para: Bianca Bombonato <bianca.bombonato@avantservices.com.br>
Cc: Rodrigo Nishimori <rodrigo@fozdoiguacu.pr.leg.br>

Boa tarde! recebido, muito obrigado.
[Texto das mensagens anteriores oculto]
--

Bianca Bombonato <bianca.bombonato@avantservices.com.br> 12 de julho de 2024 às 16:43
Para: Rafael Sanches <sanches@fozdoiguacu.pr.leg.br>
Cc: Rodrigo Nishimori <rodrigo@fozdoiguacu.pr.leg.br>

Rafael,

Imagina, obrigada você pela oportunidade de cotação!

Atenciosamente,

Bianca Bombonato
Product Manager
(44) 4003-4912 / (11) 9 7723-2059
avantservices.com.br

AVANT

Fale comigo
no whatsapp

De: Rafael Sanches <sanches@fozdoiguacu.pr.leg.br>
Enviada em: sexta-feira, 12 de julho de 2024 16:23
Para: Bianca Bombonato <bianca.bombonato@avantservices.com.br>
Cc: Rodrigo Nishimori <rodrigo@fozdoiguacu.pr.leg.br>
Assunto: Re: Solicitação de orçamento para renovação [Kaspersky]

Boa tarde! recebido, muito obrigado.

[Texto das mensagens anteriores oculto]

Rafael Sanches <sanches@fozdoiguacu.pr.leg.br>

Solo Network | Proposta Comercial P24-570597A | Kaspersky

Ana Beatriz Lopez Graciano <ana.graciano@solonetwork.com.br> 12 de julho de 2024 às 16:23
Para: "sanches@fozdoiguacu.pr.leg.br" <sanches@fozdoiguacu.pr.leg.br>, "rodrigo@fozdoiguacu.pr.leg.br" <rodrigo@fozdoiguacu.pr.leg.br>
Cc: Rafael Felix Hahn Lehmkuhl <rafael.lehmkuhl@solonetwork.com.br>

Solo Network | Proposta Comercial | P24-570597A

Olá , Rodrigo ,

Conforme solicitado segue proposta comercial (Kaspersky) **em anexo.**

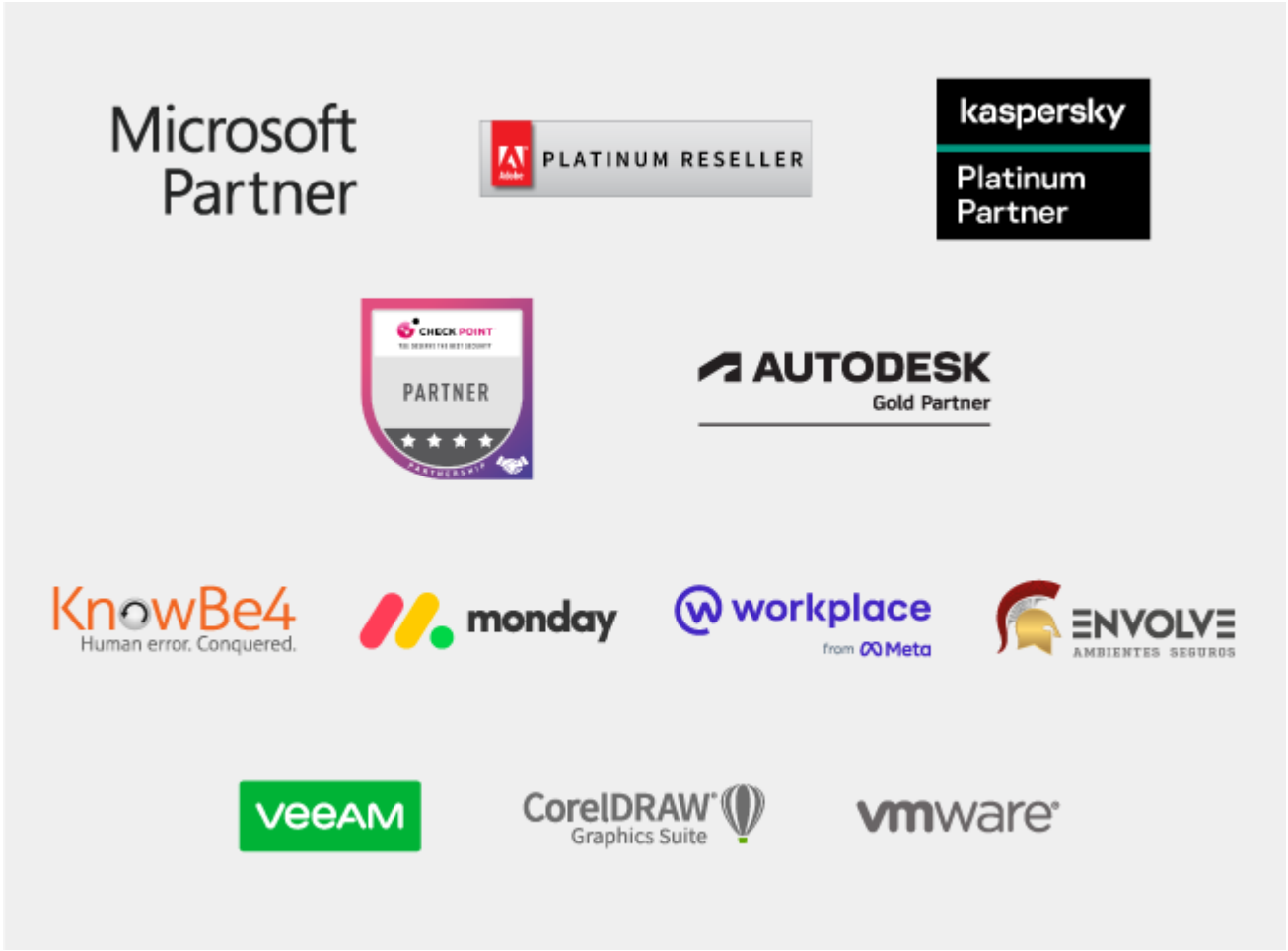
Esta proposta terá validade até **19/07/2024** ou enquanto durarem os estoques (no caso de produtos). Atente-se ao prazo para não perder esta oportunidade!

Desde 2002 no mercado brasileiro a **Solo Network** é uma empresa de tecnologia com grande foco em serviços e soluções de TI. A Solo Network dispõe dos mais altos níveis de certificações e é premiada nacional e internacionalmente pelas fabricantes que representa.

Em caso de dúvidas ou novas cotações, entre em contato conosco. Nossa equipe prontamente te auxiliará em consultas de produtos e serviços da linha corporativa, governamental e educacional.

Desde já agradecemos a escolha da Solo Network como seu fornecedor!

Alguns fabricantes representados pela Solo Network


Microsoft Partner
PLATINUM RESELLER
kaspersky
Platinum Partner
CHECK POINT
PARTNER
AUTODESK
Gold Partner
KnowBe4
Human error. Conquered.
monday
workplace
from Meta
ENVOLVE
AMBIENTES SEGUROS
VEEAM
CorelDRAW
Graphics Suite
vmware


Conheça nosso portfólio completo
Clique aqui e acesse nosso site

Tenha um ótimo dia!

Solo Network - Proposta P24-570597A - Kaspersky.pdf
304K

Proc. Administrativo 35- 279/2024

De: CARLOS K. - AGCONT

Para: CMFI-PRESID - Presidência

Data: 24/10/2024 às 08:47:22

Satisfeita a determinação constante no [DESPACHO 33], em cumprimento à determinação constante, encaminho edital para assinatura.

_

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras

Anexos:

EDITAL_PREGAO_06_24_COMPLETO.pdf

Assinado digitalmente (anexos) por:

Assinante	Data	Assinatura	
Presidente da Câmara Munic...	24/10/2024 10:44:16	1Doc	PRESIDENTE DA CÂMARA MUNICIPAL DE FOZ DO IGU...

Para verificar as assinaturas, acesse **https://fozdoiguacu.1doc.com.br/verificacao/** e informe o código: **E719-274A-F498-8605**

PREGÃO ELETRÔNICO

06/2024
(90006/2024 no sistema compras.gov.br)

CONTRATANTE (UASG)

Câmara Municipal de Foz do Iguaçu (926470)

OBJETO

Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

VALOR TOTAL DA CONTRATAÇÃO

R$ 57.310,40 (Cinquenta e sete mil, trezentos e dez reais e quarenta centavos).

DATA DA SESSÃO PÚBLICA

Dia **26/11/2024** às **10h (horário de Brasília)**

CRITÉRIO DE JULGAMENTO:

Menor preço por item.

MODO DE DISPUTA:

Aberto e fechado

PREFERÊNCIA ME/EPP/EQUIPARADAS

SIM

Baixe o APP Compras.gov.br
e apresente sua proposta!

Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

Sumário

Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

CÂMARA MUNICIPAL DE FOZ DO IGUAÇU

PREGÃO ELETRÔNICO Nº 05/2024.

(Processo Administrativo 1DOC n°279/2024)

Torna-se público que a Câmara Municipal de Foz do Iguaçu, por meio do Setor de Compras, sediada na Travessa Oscar Muxfeldt, nº 81, Centro, Foz do Iguaçu – PR, realizará licitação, para registro de preços, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da Lei nº 14.133, de 1º de abril de 2021, do Atos da Presidência nº 131/2023 e nº 134/2023 demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. O objeto da presente licitação é a Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

1.2. A licitação será realizada em item único.

ITEM	DESCRIÇÃO	BENEFÍCIO ME/EPP	QNT	VALOR UNITÁRIO	VALOR TOTAL
1	Licença KASPERSKY NEXT EDR OPTIMUM 36 meses	Tratamento favorecido	160	R$ 358,19	R$ 57.310,40

2. DA PARTICIPAÇÃO NA LICITAÇÃO

2.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).

2.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

2.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

2.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

2.5. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015, bem como para bens e serviços

produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010

2.6. Não poderão disputar esta licitação:

2.6.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

2.6.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;

2.6.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;

2.6.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

2.6.5. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

2.6.6. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

2.6.7. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;

2.6.8. agente público do órgão ou entidade licitante;

2.6.9. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

2.6.10. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.

2.7. O impedimento de que trata o item 2.6.4 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

2.8. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 2.6.2 e 2.6.3 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

2.9. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

2.10. O disposto nos itens 2.6.2 e 2.6.3 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

2.11. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da

contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133/2021.

2.12. A vedação de que trata o item 2.6.8 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

3. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

3.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

3.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.

3.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 7.1.1 e 7.11.1 deste Edital.

3.4. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:

3.4.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;

3.4.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

3.4.3. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

3.4.4. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

3.5. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

3.6. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

3.6.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;

3.6.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

3.7. A falsidade da declaração de que trata os itens 3.4 ou 3.6 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

3.8. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

3.9. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

3.10. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

3.11. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

3.11.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

3.11.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

3.12. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

3.12.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

3.12.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.

3.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 3.11 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

3.14. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

3.15. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

4. DO PREENCHIMENTO DA PROPOSTA

4.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

4.1.1. Valor unitário e total do item;

4.1.2. Marca;

4.1.3. Fabricante;

4.1.4. Quantidade cotada, devendo respeitar o mínimo para cada item.

4.2. Todas as especificações do objeto contidas na proposta aceita pela Administração vinculam o licitante.

4.2.1. O licitante NÃO poderá oferecer proposta em quantitativo inferior ao previsto para a contratação.

4.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.

4.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

4.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

4.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

4.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, quando devidamente aceita pela administração, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

4.7.1. O prazo de validade da proposta **não será inferior a 90 (noventa)** dias**,** a contar da data de sua apresentação, independentemente do prazo indicado no documento encaminhado.

4.7.2. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

4.8. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

5. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

5.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.

5.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.

5.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.

5.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

5.5. O lance deverá ser ofertado pelo valor unitário do item

5.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

5.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

5.8. O intervalo mínimo de diferença de valores, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 1,00 (Um real).

5.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

5.10. O procedimento seguirá de acordo com o modo de disputa aberto e fechado.

5.11. Para o envio de lances no pregão eletrônico o modo de disputa "aberto e fechado", os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

5.11.1. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

5.11.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.11.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

5.11.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

5.11.5. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.12. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

5.13. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

5.14. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

5.15. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

5.16. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

5.17. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

5.18. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

5.18.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

5.18.2. A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

5.18.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

5.18.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

5.19. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

5.19.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

5.19.1.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

5.19.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

5.19.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

5.19.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

5.19.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

5.19.2.1. empresas estabelecidas no território do Estado do Paraná;

5.19.2.2. empresas brasileiras;

5.19.2.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

5.19.2.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

5.19.3. Se, mesmo após a aplicação dos procedimentos previstos nos itens acima, ainda persistir o empate, será realizado sorteio público para fins de desempate;

5.19.3.1. Será informado no chat da sessão pública, a data, hora e local do sorteio, a ser realizado no site sorteio.com (ou outro compatível), com transmissão ao vivo no Youtube ou outra plataforma de streaming;

5.19.3.2. Haverá lavratura de ata de sorteio, com presença de testemunhas, que será incluída no processo administrativo.

5.20. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro deverá negociar condições mais vantajosas, após definido o resultado do julgamento.

5.20.1. Não será admitida a previsão de preços diferentes em razão de local de entrega ou de acondicionamento, tamanho de lote ou qualquer outro motivo.

5.20.2. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

5.20.3. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

5.20.4. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

5.20.5. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

5.20.6. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

5.21. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

6. DA FASE DE JULGAMENTO

6.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 2.5 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

6.1.1. SICAF;

6.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

6.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

6.1.4. Cadastro de restrições ao direito de contratar com a Administração Pública (https://crcap.tce.pr.gov.br/ConsultarImpedidos.aspx)

6.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

6.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

6.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

6.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação.

6.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

6.4. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

6.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com os itens 3.5.1 e 4.6 deste edital.

6.6. Verificadas as condições de participação, o pregoeiro examinará a proposta final ajustada, ofertada pela empresa classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 27 a 33 do Ato da Presidência nº 134/2023.

6.7. Será desclassificada a proposta vencedora que:

6.7.1. contiver vícios insanáveis;

6.7.2. não obedecer às especificações técnicas contidas no Termo de Referência;

6.7.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

6.7.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

6.7.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

6.8. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

6.8.1. A inexequibilidade, na hipótese de que trata o **caput**, só será considerada após diligência do pregoeiro, que comprove:

6.8.1.1. que o custo do licitante ultrapassa o valor da proposta; e

6.8.1.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

6.8.2. Será desclassificada a proposta que não tiver sua exequibilidade demonstrada, quando exigido pela Administração.

6.9. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

6.10. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante ou da área especializada no objeto.

7. DA FASE DE HABILITAÇÃO

7.1. Os documentos previstos neste item, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

7.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

7.2. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

7.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor

juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

7.4. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, por cópia ou original e cópia simples para autenticação pela Equipe de Pregão e posterior devolução.

7.5. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

7.6. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

7.7. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

7.8. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

7.9. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

7.9.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

7.10. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (IN nº 3/2018, art. 7º, *caput*).

7.10.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. (IN nº 3/2018, art. 7º, parágrafo único).

7.11. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

7.11.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de DUAS HORAS, prorrogável por igual período, contado da solicitação do pregoeiro.

7.12. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

7.12.1. Os documentos relativos à regularidade fiscal somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

7.13. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e Ato da Presidência nº 134/2023, art. 35, §4º):

7.13.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

7.13.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

7.14. Na análise dos documentos de habilitação, a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

7.15. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital.

7.16. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

7.17. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

7.18. Serão exigidos os seguintes documentos para a habilitação:

7.18.1. Habilitação jurídica nos termos do art. 66 da Lei nº 14.133/2021;

7.18.2. Prova da inexistência de fato impeditivo para licitar ou contratar com a Administração Pública, mediante a juntada de pesquisa realizada junto ao Tribunal de Contas da União e ao Tribunal de Contas do Estado do Paraná;

7.18.3. Habilitação fiscal, social e trabalhista, nos termos do Art. 68 da Lei nº 14-133/2021;

7.18.4. Habilitação econômico-financeira, mediante o fornecimento de Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante;

8. DOS RECURSOS

8.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

8.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

8.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

8.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

8.3.1.1. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

8.3.2. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

8.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

8.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

8.6. Os recursos interpostos fora do prazo não serão conhecidos.

8.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

8.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

8.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

8.10. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico https://www.fozdoiguacu.pr.leg.br/transparencia/licitacoes/2024/pregao-eletronico-006-2024/

9. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

9.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

9.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

9.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

9.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

9.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

9.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

9.1.2.4. deixar de apresentar amostra;

9.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

9.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

9.1.3.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

9.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação

9.1.5. fraudar a licitação

9.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

9.1.6.1. agir em conluio ou em desconformidade com a lei;

9.1.6.2. induzir deliberadamente a erro no julgamento;

9.1.6.3. apresentar amostra falsificada ou deteriorada;

9.1.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

9.1.8. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

9.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

9.2.1. advertência;

9.2.2. multa;

9.2.3. impedimento de licitar e contratar e

9.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

9.3. Na aplicação das sanções serão considerados:

9.3.1. a natureza e a gravidade da infração cometida.

9.3.2. as peculiaridades do caso concreto

9.3.3. as circunstâncias agravantes ou atenuantes

9.3.4. os danos que dela provierem para a Administração Pública

9.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

9.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor da proposta, recolhida no prazo máximo de **15 (quinze) dias** úteis, a contar da comunicação oficial.

9.4.1. Para as infrações previstas nos itens 9.1.1, 9.1.2 e 9.1.3, a multa será de 5% do valor total da proposta.

9.4.2. Para as infrações previstas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, a multa será de 30% do valor total da proposta.

9.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

9.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

9.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 9.1.1, 9.1.2 e 9.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

9.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 9.1.4, 9.1.5, 9.1.6, 9.1.7 e 9.1.8, bem como pelas infrações administrativas previstas nos itens 9.1.1, 9.1.2 e 9.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

9.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 9.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

9.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.

9.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida,

que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

9.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

9.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

9.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

10. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

10.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

10.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

10.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, pelos *seguintes meios*: protocolo digital através do sistema 1doc através do link https://fozdoiguacu.1doc.com.br/b.php?pg=wp/wp&itd=12 ou envio através do email licitacao@fozdoiguacu.pr.leg.br.

10.4. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

10.4.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.

10.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

11. DAS DISPOSIÇÕES GERAIS

11.1. Será divulgada ata da sessão pública no sistema eletrônico.

11.2. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

11.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

11.4. A homologação do resultado desta licitação não implicará direito à contratação.

11.5. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

11.6. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.

11.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

11.8. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

11.9. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

11.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico https://www.fozdoiguacu.pr.leg.br/transparencia/licitacoes/2024/pregao-eletronico-006-2024.

11.11. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

11.11.1. ANEXO I - Termo de Referência

11.11.2. ANEXO II – Estudo Técnico Preliminar

11.11.3. ANEXO III - Minuta de Termo de Contrato

11.11.4. ANEXO IV – Modelo da Proposta de Preços

JOÃO MORALES

PRESIDENTE DA CÂMARA MUNICIPAL DO IGUAÇU

TERMO DE REFERÊNCIA

1) DEFINIÇÃO DO OBJETO

Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 (trinta e seis) meses, de acordo com as condições e especificações constantes neste documento e estudo técnico preliminar (ETP).

Item	CAT/ MAT	Descrição	SKU	Quantidade total	Valor Unit.	Valor Total
1	350949	Licença de uso individual da solução Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160	R$ 358,19	R$ 57.310,40

2) FUNDAMENTAÇÃO DA CONTRATAÇÃO

Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da

qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.
Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".
Considerando que esta casa de leis realiza a utilização da solução de segurança, sem ressalvas e visa proteger seu investimento, assegurar a padronização e compatibilidade com o ambiente computacional. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para, no mínimo, manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.
Com a iminente expiração da licença, torna-se necessária a renovação e aquisição para assegurar a proteção atualizada contra as ameaças virtuais mais recentes.
Sendo a demanda prevista no PAC, conforme documento de estudo técnico preliminar - ETP.

3) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução de segurança deve atender a necessidade de evolução e adequação desta casa em relação a suas ferramentas de proteção, esta casa de leis possui dois contratos ativos de licença da ferramenta KESB Select da desenvolvedora Kaspersky Global, em um deles possui o quantitativo de 130 licenças a expirar em 22/09/2024 e o outro de 20 licenças a expirar em 01/10/2024. Sendo assim, a solução apresentada deve fornecer 10 novas licenças e 150 em formato de renovação, adequada à nova linha de produtos das soluções de segurança com incremento de, no mínimo, EDR, bem como sua ativação. Referente a possibilidade de parcelamento, deve seguir de acordo com o ETP, por se tratar de uma solução integrada.

Custo Inicial Reduzido: Ao optar pela renovação, a empresa evita os altos custos iniciais de compra e instalação de novas soluções, permitindo a alocação de recursos para outras áreas críticas do negócio.

- **Suporte e atualizações:** Fornecimento dos serviços de suporte técnico, bem como atualizações, asseguram o perfeito funcionamento da solução.
- **Gestão Simplificada:** Por se tratar de uma solução integrada a gestão centralizada, permite aos profissionais maior autonomia e melhor condição de adaptação, visto que a equipe é reduzida.

Os itens da presente solução devem ser contratados em conjunto tendo em vista a necessidade de completa compatibilidade para o correto funcionamento.

a) Proteção antivírus de Arquivos;

b) Proteção antivírus da Web;

c) Firewall local de cada máquina;

d) Bloqueador de Ataques da Rede;

e) Inspeção do Sistema;

f) Inspeção avançada de dispositivos portáteis (pen drive, cartão de memória, etc);

g) Monitoramento de Vulnerabilidades.

4) REQUISITOS DA CONTRATAÇÃO

4.1. Do módulo de proteção de endpoint

a. A solução proposta deverá proteger os sistemas operacionais abaixo:
   i. Windows 7
   ii. Windows 8
   iii. Windows 8.1
   iv. Windows 10
   v. Windows 11
b. Servidores
   i. Windows Small Business Server 2011
   ii. Windows MultiPoint Server 2011
   iii. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022
c. Servidores de terminal Microsoft
   i. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022
d. Sistemas operacionais Linux de 32 bits:
   i. CentOS 6.7 e posterior
   ii. Debian GNU/Linux 11.0 e posterior
   iii. Debian GNU/Linux 12.0 e posterior
   iv. Red Hat Enterprise Linux 6.7 e posterior
e. Sistemas operacionais Linux de 64 bits:
   i. Amazon Linux 2.
   ii. CentOS 6.7 e mais tarde
   iii. CentOS 7.2 e posterior.
   iv. CentOS Stream 8.
   v. CentOS Stream 9.
   vi. Debian GNU/Linux 11.0 e posterior.
   vii. Debian GNU/Linux 12.0 e posterior.
   viii. Linux Mint 20.3 e superior.
   ix. Linux Mint 21.1 e posterior.
   x. openSUSE Leap 15.0 e posterior.
   xi. Oracle Linux 7.3 e posterior.

xii. Oracle Linux 8.0 e posterior.
xiii. Oracle Linux 9.0 e posterior.
xiv. Red Hat Enterprise Linux 6.7 e posterior
xv. Red Hat Enterprise Linux 7.2 e posterior.
xvi. Red Hat Enterprise Linux 8.0 e posterior.
xvii. Red Hat Enterprise Linux 9.0 e posterior.
xviii. Rocky Linux 8.5 e posterior.
xix. Rocky Linux 9.1.
xx. SUSE Linux Enterprise Server 12.5 ou posterior.
xxi. SUSE Linux Enterprise Server 15 ou posterior.
xxii. Ubuntu 20.04 LTS.
xxiii. Ubuntu 22.04 LTS.
xxiv. Sistemas operacionais Arm de 64 bits:
xxv. CentOS Stream 9.
xxvi. SUSE Linux Enterprise Server 15.
xxvii. Ubuntu 22.04 LTS.

f. Sistemas operacionais MAC OS:
    i. macOS 12 – 14
g. Ferramentas de virtualização MAC OS:
    i. Parallels Desktop 16 para Mac Business Edition
    ii. VMware Fusion 11.5 Profissional
    iii. VMware Fusion 12 Profissional
h. A solução proposta deverá suportar as seguintes plataformas virtuais:
    i. VMware Workstation 17.0.2 Pro
    ii. VMware ESXi 8.0 Update 2
    iii. Microsoft Hyper-V Server 2019
    iv. Citrix Virtual Apps e Desktop 7 2308
    v. Citrix Provisioning 2308
    vi. Citrix Hypervisor 8.2 Update 1

4.2. Do módulo de gerenciamento avançado

a. A solução proposta deve suportar arquitetura cloud-native e on-premisse;
b. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
    i. Amazon Web Services
    ii. Microsoft Azure
c. A solução proposta deve incluir as seguintes opções de integração SIEM:
    i. HP (Microfoco) ArcSight
    ii. IBM QRadar
    iii. Splunk
    iv. Kaspersky KUMA
d. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.
e. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

f. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.
g. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.
h. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.
i. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.
j. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.
k. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.
l. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.
m. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.
n. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:
    i. Status do dispositivo
    ii. Tag
    iii. Diretório ativo
    iv. Proprietários de dispositivos
    v. Hardware
o. A solução proposta deve suportar os seguintes canais de entrega de notificação:
    i. E-mail
    ii. Registro de sistema
    iii. SMS
p. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:
    i. Atributos de rede
    ii. Nome
    iii. Domínio e/ou Sufixo de Domínio
    iv. Endereço de IP
    v. Endereço IP para servidor de gerenciamento
    vi. Localização no Active Directory
    vii. Unidade organizacional
    viii. Grupo
    ix. Sistema operacional
    x. Número do pacote de serviço
    xi. Arquitetura Virtual
    xii. Registro de aplicativos
    xiii. Nome da Aplicação
    xiv. Versão do aplicativo
    xv. Fabricante

xvi. Tipo e versão
xvii. Arquitetura

q. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.
r. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.
s. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:
    i. Dispositivos Desktop/Servidores
    ii. Dispositivos móveis
    iii. Dispositivos de rede
    iv. Dispositivos virtuais
    v. Componentes OEM
    vi. Periféricos de computador
    vii. Dispositivos IoT conectados
    viii. Telefones VoIP
    ix. Repositórios de rede
t. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:
    i. Nome da Aplicação
    ii. Caminho do aplicativo
    iii. Metadados do aplicativo
    iv. Aplicativo Certificado digital
    v. Categorias de aplicativos predefinidas pelo fornecedor
    vi. SHA256 e MD5
u. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:
    i. Bluetooth
    ii. Dispositivos móveis
    iii. Modems externos
    iv. CD/DVD
    v. Câmeras e scanners
    vi. MTPs
    vii. E a transferência de dados para dispositivos móveis
v. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.
w. A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.
x. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:
    i. Estruturas de domínios e grupos de trabalho do Windows
    ii. Estruturas de grupos do Active Directory
    iii. Conteúdo de um arquivo de texto criado manualmente pelo administrador

y. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.
z. A solução proposta deve permitir realizar as seguintes ações para endpoints:
   i. Verificação manual;
   ii. Verificação no acesso;
   iii. Verificação por demanda;
   iv. Verificação de arquivos compactados
   v. Verificação de arquivos individuais, pastas e unidades;
   vi. Bloqueio e verificação de scripts
   vii. Proteção contra alteração de registros;
   viii. Proteção contra estouro de buffer;
   ix. Verificação em segundo plano/inativa

1.1. Verificação de unidade removível na conexão com o sistema;
1.2. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.
1.3. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.
1.4. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.
1.5. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.
1.6. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.
1.7. A solução proposta deve suportar Windows Failover Cluster.
1.8. A solução proposta deve ter um recurso de clustering integrado.
1.9. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.
1.10. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.
1.11. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.
1.12. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.
1.13. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.
1.14. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.
1.15. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.
1.16. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.
1.17. A solução proposta deverá possuir controles para download de DLL e drivers.

1.18. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão.
1.19. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.
1.20. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).
1.21. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.
1.22. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.
1.23. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.
1.24. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.
1.25. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.
1.26. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.
1.27. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.
1.28. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.
1.29. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.
1.30. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.
1.31. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. .
1.32. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.
1.33. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante

um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.

1.34. A solução proposta deve permitir ao administrador personalizar relatórios.

1.35. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.

1.36. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.

1.37. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.

1.38. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.

1.39. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.

1.40. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.

1.41. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;

1.42. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.

1.43. A solução proposta deve suportar integração com solução APT.

1.44. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.

1.45. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:

1.45.1. Windows

1.45.2. Linux

1.46. A solução proposta deverá suportar os seguintes servidores de banco de dados:

1.46.1.1. Windows:

1.46.1.2. Microsoft SQL Server

1.46.1.3. Microsoft Banco de dados SQL do Azure

1.46.1.4. MySQL Standard e Enterprise

1.46.1.5. MariaDB

1.46.1.6. PostgreSQL

1.46.2. Linux:

1.46.2.1. MySQL

1.46.2.2. MariaDB

1.46.2.3. PostgreSQL

1.47. A solução proposta deverá suportar as seguintes plataformas virtuais:

1.47.1.1. Windows:

1.47.1.2. VMware vSphere 6.7 e 7.0

1.47.1.3. Estação de trabalho VMware 16 Pro

1.47.1.4. Servidor Microsoft Hyper-V 2012 de 64 bits

1.47.1.5. Servidor Microsoft Hyper-V 2012 R2 de 64 bits

1.47.1.6. Microsoft Servidor Hyper -V 2016 de 64 bits
1.47.1.7. Servidor Microsoft Hyper-V 2019 de 64 bits
1.47.1.8. Servidor Microsoft Hyper-V 2022 de 64 bits
1.47.1.9. Citrix XenServer 7.1 LTSR
1.47.1.10. Citrix XenServer 8.x
1.47.1.11. Oracle VM VirtualBox 6.x

1.47.2. Linux:

1.47.2.1. VMware vSphere 6.7, 7.0 e 8.0
1.47.2.2. VMware Desktop 16 Pro e 17 Pro
1.47.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits
1.47.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
1.47.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits
1.47.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits
1.47.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits
1.47.2.8. Citrix XenServer 7.1 e 8.x
1.47.2.9. Oracle VM VirtualBox 6.x e7.x

1.48. A solução proposta deve suportar criptografia em vários níveis:
1.48.1. Criptografia completa do disco – incluindo disco do sistema
1.48.2. Criptografia de arquivos e pastas
1.48.3. Criptografia de mídia removível
1.48.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2

1.49. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:
1.49.1. A criptografia de arquivos em unidades de computador locais.
1.49.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.
1.49.3. A criação de listas criptografadas de pastas em unidades de computador locais.

1.50. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:
1.50.1. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.
1.50.2. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.

1.51. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:
1.51.1. A criptografia de todos os arquivos armazenados em unidades removíveis.
1.51.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.

1.52. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia

1.53. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.

1.54. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.

1.55. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.

1.56. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.

1.57. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.

1.58. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.

1.59. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.

1.60. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.

1.61. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.

1.62. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.

1.63. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.

1.64. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.

1.65. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário.

1.66. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.

1.67. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.

1.68. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:

1.68.1. Uso do Trusted Platform Module e configurações de senha.

1.68.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.

1.69. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).
1.70. A solução proposta deve suportar criptografia em Microsoft Surface Tablets.
1.71. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
1.71.1. Instalação remota de software de terceiros
1.71.2. Relatórios sobre software e hardware existentes
1.71.3. Monitoramento para instalação de software não autorizado
1.71.4. Remoção de software não autorizado
1.72. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.
1.73. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.
1.74. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.
1.75. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.
1.76. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.
1.77. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.
1.78. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.
1.79. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança
1.80. A solução proposta deve permitir ao administrador aprovar atualizações.
1.81. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.
1.82. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.
1.83. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.
1.84. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.
1.85. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.
1.86. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).
1.87. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.
1.88. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.
1.89. A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’.

1.90. A solução proposta deve incluir campos dedicados que contenham informações sobre "Ameaça encontrada para a vulnerabilidade".
1.91. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.
1.92. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.
1.93. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.
1.94. A solução proposta deve apoiar a implantação do sistema operacional.
1.95. A solução proposta deve suportar Wake-on LAN e UEFI.
1.96. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.
1.97. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.
1.98. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.
1.99. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.
1.100. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.
1.101. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.
1.102. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.
1.103. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.
1.104. A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.
1.105. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:
1.105.1. Inicie a instalação ao reiniciar ou desligar o computador.
1.105.2. Instale o gerador necessário todos os pré-requisitos do sistema.
1.105.3. Permitir a instalação de novas versões de aplicativos durante as atualizações.
1.105.4. Baixe atualizações para o dispositivo sem instalá-las.
1.106. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.
1.107. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.
1.108. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:
1.108.1. CEF;

1.108.2. LEEF;

1.109. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.

1.110. O relatório da solução proposta deve conter informações CVE.

1.111. A solução proposta deve suportar instalação de aplicações e software de terceiros;

4.3. Do módulo de gerenciamento simplificado

1.112. A solução proposta deve suportar arquitetura cloud;

1.113. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

1.114. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

1.115. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.

1.116. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.

1.117. A solução proposta deve atender as condições apontadas no item e subintes 6.

1.118. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.

1.119. A solução proposta deve incluir informações do endpoint:

1.119.1. IP público de internet;

1.119.2. IP interno do dispositivo;

1.119.3. Versão do agente de proteção;

1.119.4. Ultima comunicação com a console, contendo data e hora;

1.119.5. Informações do sistema operacional;

1.120. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.

1.121. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.

1.122. A solução proposta deve incluir treinamento em segurança cibernética.

4.4. Requisitos gerais

1.123. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:

1.123.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

1.124. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.

1.125. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).

1.126. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.

1.127. A solução proposta deve suportar o subsistema Linux no Windows.

1.128. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

1.128.1. Proteção contra ameaças sem arquivos (Fileless);

1.128.2. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

1.129. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;
1.130. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.
1.131. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.
1.132. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.
1.133. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.
1.134. A solução proposta deve fornecer análise comportamental baseada em machine learning.
1.135. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.
1.136. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
1.136.1. Controles de aplicativos,
1.136.2. Controle web e dispositivos
1.136.3. HIPS e Firewall
1.136.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;
1.136.5. Gerenciamento de criptografia de arquivos e discos;
1.136.6. Controle adaptativo para detecção de anomalias;
1.137. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.
1.138. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.
1.139. A solução proposta deve ter bancos de dados de reputação locais e globais.
1.140. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.
1.141. A solução proposta deve incluir um módulo capaz, no mínimo, de:
1.141.1. Bloqueio de aplicativos com base em sua categorização.
1.141.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.
1.141.3. A adição de sub-redes e a modificação de permissões de atividade.
1.142. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.
1.143. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.
1.144. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem

ser armazenados em um formato específico que garanta que não representem qualquer ameaça.

1.145. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:

1.145.1. Modo silencioso;

1.145.2. Discos rígidos e dispositivos removíveis;

1.145.3. De todos as contas de usuários do dispositivo.

1.146. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:

1.146.1. Exclusão imediata de dados;

1.146.2. Exclusão de dados adiada.

1.147. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:

1.147.1. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;

1.147.2. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.

1.148. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.

1.149. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.

1.150. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.

1.151. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

1.152. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.

1.153. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.

1.154. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.

1.155. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;

1.156. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;

1.157. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.

1.158. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.

1.159. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.

1.160. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.
1.161. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.
1.162. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.
1.163. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.
1.164. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.
1.165. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.
1.166. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.
1.167. A solução proposta deve ter categoria de detecção para bloquear banners de sites.
1.168. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;
1.169. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.
1.170. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.
1.171. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.
1.172. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;
1.173. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.
1.174. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.
1.175. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.
1.176. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.
1.177. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.
1.178. A solução proposta deve suportar o controle de scripts executados em PowerShell.
1.179. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.
1.180. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.
1.181. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.

1.182. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.
1.183. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.
1.184. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.
1.185. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
1.185.1. Filtro de anexos.
1.185.2. Verificação de mensagens de email ao receber, ler e enviar.
1.186. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.
1.187. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;
1.188. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);
1.189. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.
1.190. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.
1.191. A solução proposta deve incluir suporte ao protocolo IPv6.
1.192. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.
1.193. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
1.194. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.
1.195. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.
1.196. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.
1.197. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.
1.198. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.
1.199. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.
1.200. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.
1.201. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.

1.202. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.
1.203. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.
1.204. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.
1.205. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.
1.206. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.
1.207. A solução proposta deve suportar endereços IPv6.
1.208. A solução proposta deve suportar verificação em duas etapas (autenticação).
1.209. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.
1.210. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.
1.211. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.
1.212. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.
1.213. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.
1.214. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.
1.215. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.
1.216. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.
1.217. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.
1.218. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.
1.219. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.
1.220. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.
1.221. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.
1.222. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.

1.223. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.
1.224. A solução proposta deve ter a capacidade de excluir atualizações baixadas.
1.225. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.
1.226. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.
1.227. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.
1.228. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.
1.229. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.
1.230. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.
1.231. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.
1.232. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.
1.233. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
1.233.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.
1.233.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.
1.234. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.
1.235. A solução proposta deve gerar relatoiros de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

4.5. Do modulo de gerenciamento de dispositivos móveis

1.236. O modulo deve ser integrado a console de gerenciamento;
1.237. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
1.237.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)
1.238. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
1.238.1. iOS 10–17 ou iPadOS 13–17
1.239. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.
1.240. A solução proposta deve suportar dispositivos iOS supervisionados.
1.241. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.

1.242. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.

1.243. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.

1.244. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).

1.245. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.

1.246. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

1.247. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.

1.248. A solução proposta deve ter recursos de conteinerização para dispositivos Android.

1.249. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:

1.249.1. Dados em contêineres

1.249.2. Contas de e-mail corporativo

1.249.3. Configurações para conexão à rede Wi-Fi corporativa e VPN

1.249.4. Nome do ponto de acesso (APN)

1.249.5. Perfil do Android for Work

1.249.6. Recipiente KNOX

1.249.7. Chave do gerenciador de licença KNOX

1.250. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:

1.250.1. Todos os perfis de configuração instalados

1.250.2. Todos os perfis de provisionamento

1.250.3. O perfil iOS MDM

1.251. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas

1.252. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo .

1.253. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:

1.253.1. Critérios de verificação do dispositivo;

1.253.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;

1.254. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.

1.255. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:

1.255.1. Cartões de memória e outras unidades removíveis
1.255.2. Câmera do dispositivo
1.255.3. Conexões Wi-Fi
1.255.4. Conexões Bluetooth
1.255.5. Porta de conexão infravermelha
1.255.6. Ativação do ponto de acesso Wi-Fi
1.255.7. Conexão de área de trabalho remota
1.255.8. Sincronização de área de trabalho
1.255.9. Definir configurações da caixa de correio do Exchange
1.255.10. Configurar caixa de e-mail em dispositivos iOS MDM
1.255.11. Configure contêineres Samsung KNOX.
1.255.12. Definir as configurações do perfil do Android for Work
1.255.13. Configurar e-mail/calendário/contatos
1.255.14. Defina as configurações de restrição de conteúdo de mídia.
1.255.15. Definir configurações de proxy no dispositivo móvel
1.255.16. Configurar certificados e SCEP

1.256. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay .

1.257. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:
1.257.1. Google Play, Huawei App Gallery e Apple App Store
1.257.2. Portal de inscrição móvel KNOX
1.257.3. Pacotes de instalação pré-configurados independentes

1.258. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.

1.259. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.

1.260. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
1.260.1. VMware AirWatch 9.3 ou posterior
1.260.2. MobileIron 10.0 ou posterior
1.260.3. IBM MaaS360 10.68 ou posterior
1.260.4. Microsoft Intune 1908 ou posterior
1.260.5. SOTI MobiControl 14.1.4 (1693) ou posterior

1.261. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.

1.262. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:
1.262.1. Google Play
1.262.2. Galeria de aplicativos Huawei
1.262.3. Loja de aplicativos da Apple

1.263. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.

1.264. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.

1.265. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.
1.266. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.
1.267. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.
1.268. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.
1.269. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.
1.270. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.
1.271. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.
1.272. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.
1.273. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.
1.274. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.
1.275. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
1.276. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

4.6. Do módulo de EDR

4.6.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
4.6.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
4.6.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
4.6.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
4.6.5. Deve apresentar informações detalhadas contendo:
4.6.5.1. Usuário que executou a ação;
4.6.5.2. Informações acesso privilegiado;
4.6.6. A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.
4.6.7. A solução proposta deve suportar integração com serviço de reputação em nuvem.
4.6.8. A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado.

(Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)

4.6.9. O agente EDR deve ter integração com o aplicativo de proteção de endpoint(agente único).

4.6.10. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;

4.6.11. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.

4.6.12. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.

4.6.13. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.

4.6.14. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.

4.6.15. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.

4.6.16. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.

4.6.17. A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.

4.6.18. A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.

4.6.19. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.

4.6.20. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:

4.6.21. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).

4.6.22. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.

4.6.23. Informações gerais sobre a detecção, incluindo modo de detecção.

4.6.24. Alterações no registro associadas à detecção.

4.6.25. Histórico da presença de arquivos no dispositivo.

4.6.26. Ações de resposta executadas pela aplicação.

4.6.27. O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.

4.6.28. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:

4.6.29. Processo

4.6.30. Conexões de rede

4.6.31. Alterações no registro

4.6.32. Detalhes do download de objeto

4.6.33. A solução proposta deve fornecer orientação de resposta (resposta guiada).

4.6.34. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente
4.6.35. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
4.6.36. Impedir a execução de objetos
4.6.37. Isolamento de host
4.6.38. Excluir objeto do host ou grupo de hosts
4.6.39. Encerrar um processo no dispositivo
4.6.40. Colocar um objeto em quarentena
4.6.41. Execute a verificação do sistema
4.6.42. Execução remota de programa/processo/comando
4.6.43. Iniciar a varredura IoC para um grupo de hosts.

4.7. **Requisitos para documentação da solução.**

4.7.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:
4.7.2. Ajuda on-line para administradores
4.7.3. Ajuda on-line para melhores práticas de implementação
4.7.4. Ajuda on-line para proteção de servidores de administração
4.7.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.
4.7.6. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

04. PRAZO DE GARANTIA

a. As empresas licitantes deverão indicar o prazo da garantia do Software ou licença, que deverá ser de 36 meses oferecido diretamente ou com a autorização e responsabilidade do fabricante, sendo este o período em que se obrigam a prestar a manutenção e assistência técnica gratuita, nos termos regulados na minuta do contrato.

b. Serão desclassificadas as propostas que não ofereçam prazo de garantia ou abaixo do mínimo estipulado. As empresas licitantes indicarão, SOB PENA DE DESCLASSIFICAÇÃO, informações relacionadas à PADRONIZAÇÃO e COMPATIBILIDADE da solução, conforme detalhamento no ETP.

05. OBRIGAÇÕES DA CONTRATANTE

a. Comunicar à Contratada quaisquer irregularidades nos equipamentos, para adoção das providências cabíveis;

b. Designar funcionário para acompanhar/fiscalizar a entrega;

c. Efetuar os pagamentos relativos ao presente contrato em moeda corrente quando da apresentação da fatura de serviços executados respeitando os prazos de vencimentos;

d. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;

e. Qualquer alteração deste, somente deverá ser com o aval dos gestores do contrato;

f. Aplicar a contratada as sanções administrativas regulamentares e contratuais cabíveis;

06. OBRIGAÇÕES DA CONTRATADA

a. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

b. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do contrato, inerentes à execução do objeto contratual;

c. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

d. É de responsabilidade da CONTRATADA, manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

07. DA SUBCONTRATAÇÃO

a. Não será admitida a subcontratação do objeto.

08. MODELO DE EXECUÇÃO DO OBJETO

Em até, 30 dias, a contar da assinatura do contrato, as novas licenças deverão ser fornecidas e registradas em nome de CÂMARA MUNICIPAL DE FOZ DO IGUAÇU, nome fantasia PODER LEGISLATIVO, CNPJ 75.914.051/0001-28, atreladas a conta suporte@fozdoiguacu.pr.leg.br , dentro da plataforma da desenvolvedora Kaspersky Global.
Quando que realizada a disponibilização da licença, notificar via e-mail os responsáveis técnicos, sanches@fozdoiguacu.pr.leg.br e rodrigo@fozdoiguacu.pr.leg.br com detalhes do acesso.

09. MODELO DE GESTÃO DO CONTRATO E CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

A execução do objeto seguirá a seguinte dinâmica:

a. A contratante indicará Fiscal de contratos que irá acompanhar a execução do contrato em conformidade com este termo de referência.

b. O Contrato terá o prazo de 3 (três) anos, podendo ser prorrogado.

c. A Contratada formalizará a designação do preposto da empresa, especificando os poderes e responsabilidades relacionados à execução do objeto contratado.

d. Toda comunicação entre a Contratante e a Contratada deverá ser formalizada por escrito especialmente quando exigido por lei, podendo ser realizada por meio de mensagem eletrônica, quando aplicável.

e. A execução será realizada de forma parcelada formalizada pelo envio da ordem de compra.

f. Os prazos e critérios para recebimento e pagamento estão detalhados nos itens 7.3 a 7.4.

g. Considera-se ocorrido o recebimento da nota fiscal quando a Gestão de contratos atestar a

execução do objeto do contrato através do termo de recebimento definitivo.

h. Não haverá exigência de garantia contratual da execução, devido às características da contratação.

i. A apresentação da Nota Fiscal/fatura é indispensável a cada fornecimento de bem ou serviço, para fins de liquidação e pagamento da despesa, emitida ao destinatário: Razão social: CÂMARA MUNICIPAL DE FOZ DO IGUACU; CNPJ: 75.914.051/0001-28; Endereço: Travessa Oscar Muxfeldt, nº 81, Centro, na cidade de Foz do Iguaçu-Paraná, CEP 85.851-490. Telefone: (45) 3521-8100.

j. Antes de cada pagamento à Contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

k. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, como, por exemplo, obrigação financeira pendente, decorrente de penalidade imposta ou inadimplência, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se- á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante.

l. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

m. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. A Contratada regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

n. Constatando-se, junto ao SICAF, a situação de irregularidade da contratada, será providenciada sua notificação, por escrito, para que, no prazo de 20 (vinte) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da Contratante.

o. Persistindo a irregularidade, a Contratante deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa.

p. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso a Contratada não regularize sua situação junto ao SICAF.

q. O prazo desta contratação será de 36 meses, contados da assinatura do contrato.

r. Pagamento:

i. Os pagamentos serão efetuados até o 10° (décimo) dia após o recebimento definitivo dos bens, condicionado a apresentação da Nota Fiscal/Fatura, bem como os documentos de regularidade fiscal, social e trabalhista exigidos pelo art. 68 da Lei n° 14.133/2021

ii. Na eventualidade de ocorrer atraso no pagamento, o valor será atualizado pela variação acumulada do IPCA/IBGE, ocorrida entre a data de seu adimplemento e a do efetivo pagamento, calculada pro rata tempore.

Sanções:

s. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei n° 14.133, de 2021, quais sejam:

t. Dar causa à inexecução parcial do contrato;

u. Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

v. Dar causa à inexecução total do contrato;

w. Deixar de entregar a documentação exigida para o certame;

x. Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

y. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

z. Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

aa. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

bb. Fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

cc. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

dd. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

ee. Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;

ff. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Multa de até 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor,

b) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver

c) aplicado a sanção, pelo prazo máximo de 3 (três) anos.

d) Direta, quando não se justificar a imposição de penalidade mais grave;

e) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 8.9 a bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

07. A fiscalização do contrato será realizada pelo servidor(a) designado:

08. A gestão do contrato será realizada pelo servidor (a) designado:

10. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço.

Tratamento diferenciado e favorecido a ser dispensado às microempresas, às empresas de pequeno porte e aos microempreendedores individuais conforme definido pelo documento de estudo técnico preliminar (ETP).

11. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

As quantidades previstas a serem adquiridas, conforme os itens descritos, são:

Item	Descrição	SKU	Quantidade	Valor Unit.	Valor
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160	R$ 358,19	R$ 57.310,40

A pesquisa de preço foi realizada considerando os parâmetros dispostos da Lei 14.133 no art. 23 § inciso IV – *"pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital"*. Do qual optou-se pelo menor preço ofertado.

Quanto à não utilização dos parâmetros dos § Incisos I e II do Art. 23, consultas no portal PNCP (Inciso I) e contratações similares feitas pela Administração Pública (II), conforme descrito no parágrafo anterior, torna-se ineficaz e escassa a busca por contratações similares em outros órgãos. Regendo-se pela economicidade, melhor tecnologia e melhores resultados pretendidos pelo órgão, a consulta aos fornecedores torna-se mais eficaz.

12. ADEQUAÇÃO ORÇAMENTÁRIA

ITEM	DOTAÇÃO

1	01.01.01.031.0001.2002.3.3.90.40.99.05 - AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: 8D6E-2A15-90A9-AA4D

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

WALDSON DE ALMEIDA DIAS (CPF 425.XXX.XXX-20) em 13/09/2024 11:04:35 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://fozdoiguacu.1doc.com.br/verificacao/8D6E-2A15-90A9-AA4D

ESTUDO TÉCNICO PRELIMINAR

1) DESCRIÇÃO DA NECESSIDADE

1.1. Atualmente a CMFI disponibiliza diversos serviços e aplicações internas e externa para os seus servidores, estas operações são fundamentais para o funcionamento desta casa de leis e estão fortemente dependentes dos serviços disponíveis em sua rede de computadores, de maneira que se torna necessário o constante monitoramento e o aperfeiçoamento dos serviços existentes, bem como garantir a segurança das informações de forma a minimizar o risco de perdas e paradas causando um impacto negativo sobre o desempenho institucional.

1.2. A segurança deste ambiente torna-se cada vez mais crítica com o passar do tempo, o que requer ações conjuntas e complementares aos esforços já adotados pela área de tecnologia e é extremamente necessário que a CMFI mantenha as operações de segurança em níveis de risco admissíveis.

1.3. Os ataques cibernéticos estão cada vez mais diversificados, adotando várias formas para obter dados sigilosos das instituições, informações dos usuários, ou sobre a sua infraestrutura, o que combinado com outras técnicas de ataques conhecidas, permite ao crime organizado compor cenários de fraudes e ataques ainda mais complexos, sem que nunca se desconfie por onde houve o vazamento de informações, ou que se identifique a própria falha de segurança que levou a elas.

1.4. Mesmo diante a este cenário de ataques cibernéticos, a CMFI está sempre na busca pelo atendimento adequado aos anseios e necessidades da população, desenvolvendo projetos específicos, vislumbrando a diminuição no tempo de atendimento aos serviços prestados e efetividade nas informações repassadas. Estes projetos e melhorias, devem ter como lastro a integração tecnológica de forma adequada e segura.

1.5. Considerando o aumento no volume de acessos e de novas ameaças cibernéticas, tentativas de invasão aos sistemas e a iminente expiração das atuais licenças de proteção de endpoint, que podem impactar de modo negativo a eficiente gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, faz-se presente a obrigação de preservar a integridade, confidencialidade e disponibilidade das informações custodiadas nesta casa de leis, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

1.6. Cabe ressaltar o comprometimento por parte desta casa de leis a busca por conformidade com padrões e normas do mercado privado e público, incluindo a Lei nº 13.709 de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado e que menciona em seu Art. 46 a obrigação legal das entidades públicas ou privadas em "adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

1.7. Mediante ao exposto, é necessária a renovação da Solução de Proteção de Endpoints da fabricante Kaspersky para manter o padrão de proteção atualmente utilizado pela CMFI e reforçar a segurança digital do ambiente, com a prevenção contra ameaças complexas e outros como vírus de computador, spyware, ransomware e outras ameaças digitais, contratação de uma solução atendendo minimamente as mesmas especificações do sistema já utilizado permitindo que permitindo que o analista descubra, priorize, investigue e neutralize rapidamente ameaças complexas e ataques tipo APT, utilizando toda tecnologia em um único agente.

2) REQUISITOS DA CONTRATAÇÃO

Item	Descriçao	SKU	Quantidade
1	Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal License	KL4066KASTJ	160

3) LEVANTAMENTO DE MERCADO

Considerando que a Câmara Municipal de Foz do Iguaçu já dispõe de um sistema de antivírus, foram avaliadas duas alternativas sendo uma delas a renovação e upgrade de versão do sistema e a outra a aquisição de um sistema integrado com o nosso sistema de Firewall.

Mantendo os investimentos ocorridos no ano de 2018 (R$ 11.635) e 2021 (R$ 31.217,00 (Preço médio)) e já realizados, tendo em vista de que além da aquisição do sistema, foi também realizada no ano de 2023 (R$ 6.980,00) a contratação de uma empresa especializada para nos auxiliar na configuração recomendadas pelo fabricante, e com base nas pesquisa de preços e estudo entre outras soluções, por medida de economicidade optou-se pela renovação com upgrade da versão já utilizada do licenciamento da solução Kaspersky e aquisição de novas licenças de acordo com a

necessidade da CMFI , levando em consideração a ampliação do parque computacional que ocorreu nesses últimos anos e demandas futuras.

Notou-se ainda que a linha de produtos do desenvolvedor da solução passou por atualizações entregando novas versões de sua solução bem como mais recursos, a título de exemplo temos, portais de capacitação na solução, canais de suporte e a adoção da inteligência artificial para detecção e mitigação de vulnerabilidades.

4) DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

As especificações do objeto desta licitação deverão estar detalhadas no termo de referência elaborado com base neste estudo técnico preliminar e de acordo com a solicitação elaborada pelo setor demandante.

5) ESTIMATIVA DO PREÇO DA CONTRATAÇÃO

Item	Descrição	SKU	Quantidade	Valor
1	KASPERSKY NEXT EDR OPTIMUM 36 meses	KL4066KASTJ	160	R$ 57.310,40

Descrição Item 1

A solução deve incluir treinamento em segurança cibernética

Do módulo de proteção de endpoint

Compatibilidade com diferentes sistemas operacionais, MAC OS, Linux de 32 e 64 bits (CentOS, Red Hat Enterprise, Debian, Ubuntu, Oracle Linux), Windows 7, 8, 8.1, 10,11 para desktops, para servidores S.O Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022, Windows Small Business Server 2011, Servidores de terminal Microsoft (Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022).

Módulo de gerenciamento avançado

A solução deve suportar arquitetura cloud-native e on-premisse, a solução deve incluir suporte para implantação baseada em nuvem (Amazon Web Services e/ou Microsoft Azure. Integração nativa com as seguintes opções de SIEM (HP (Microfoco) ArcSight, IBM QRadar, Splunk, Kaspersky KUMA). 2.4.

A solução deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

A solução deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

A solução deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

A solução deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

O servidor de gerenciamento primário da solução deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

A solução deve suportar os seguintes canais de entrega de notificação, E-mail, registro de sistema e SMS ou equivalente.

A solução deve ter a capacidade de etiquetar/marcar computadores com base em Atributos de rede, Nome, Domínio e/ou Sufixo de Domínio, Endereço de IP, Endereço IP para servidor de gerenciamento, Localização no Active Directory, Unidade organizacional, Grupo, Sistema operacional, Número do pacote de serviço, Arquitetura Virtual, Registro de aplicativos, Nome da Aplicação, Versão do aplicativo, Fabricante, Tipo e versão, Arquitetura.

A solução deverá permitir especificamente o bloqueio dos seguintes dispositivos, Bluetooth, Dispositivos móveis, Modems externos, CD/DVD, Câmeras e scanners.

A solução deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

A solução deve permitir realizar as seguintes ações para endpoints, verificação manual, verificação no acesso, verificação por demanda, verificação de arquivos compactados, verificação de arquivos individuais, pastas e unidades, bloqueio e verificação de scripts, proteção contra alteração de registros, proteção contra estouro de buffer, verificação em segundo plano/inativa.

A solução deverá suportar os seguintes servidores de banco de dados:

Windows,

- Microsoft SQL Server
- Microsoft Banco de dados SQL do Azure
- MySQL Standard e Enterprise
- MariaDB
- PostgreSQL

Linux:

- MySQL
- MariaDB

- PostgreSQL

A solução deverá suportar as seguintes plataformas virtuais:

Windows:

- VMware vSphere 6.7 e 7.0
- Estação de trabalho VMware 16 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Oracle VM VirtualBox 6.x

2.74.2. Linux:

- VMware vSphere 6.7, 7.0 e 8.0
- VMware Desktop 16 Pro e 17 Pro
- Servidor Microsoft Hyper-V 2012 de 64 bits
- Servidor Microsoft Hyper-V 2012 R2 de 64 bits
- Microsoft Servidor Hyper -V 2016 de 64 bits
- Servidor Microsoft Hyper-V 2019 de 64 bits
- Servidor Microsoft Hyper-V 2022 de 64 bits
- Citrix XenServer 7.1 e 8.x

Do módulo de gerenciamento simplificado

A solução deve suportar arquitetura cloud;

A solução deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

A solução deve permitir ao administrador gerar relatórios pré-definidos.

A solução deve incluir informações do endpoint, IP público de internet, IP interno do dispositivo, Versão do agente de proteção, ultima comunicação com a console, contendo data e hora, informações do sistema operacional;

Requisitos gerais

A solução deve ser capaz de detectar os seguintes tipos de ameaças:
Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.
A solução deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
A solução deve ter capacidade de integração com a central de segurança do Windows Defender.
A solução deve suportar o subsistema Linux no Windows.
A solução deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

- Proteção contra ameaças sem arquivos (Fileless);
- Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

Do modulo de gerenciamento de dispositivos móveis

O modulo deve ser integrado a console de gerenciamento;
A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

- Android 5.0 ou posterior (incluindo Android 12L)

A solução deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

- iOS 10–17 ou iPadOS 13–17

A solução deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

Do módulo de EDR

Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
A solução deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;

Deve apresentar informações detalhadas contendo:

- Usuário que executou a ação;
- Informações acesso privilegiado;

A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.

O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único).

6) IMPACTOS AMBIENTAIS

Não foram identificados impactos ambientes nesta contratação

7) JUSTIFICATIVA PARA PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Não se aplica, trata-se de um único item.

8) CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

Não se identificou contratações interdependentes e/ou correlatas, sendo que a prestação dos serviços depende exclusivamente do presente procedimento.

9) ALINHAMENTO COM PAC – PLANO ANUAL DE CONTRATAÇÕES

A demanda em questão encontra-se prevista no plano anual de contratações. Considerando que o mapa de gerenciamento de riscos tem natureza opcional, conforme previsto na NLL 14.133 e ato da presidência 133/2023.

10) RESULTADOS PRETENDIDOS

- Garantir um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas em meios tecnológicos;
- Oferecer maior agilidade e eficácia no tratamento de incidentes envolvendo estações de trabalho e notebooks comprometidos;
- Evitar, mitigar e conter a propagação de pragas digitais (vírus/malwares/spywares, spam, entre outros) com a administração centralizada da solução de proteção;

- Permitir o controle de acesso à rede por dispositivos computacionais, permitindo gerenciamento destes dispositivos;
- Possibilitar análise pormenorizada de arquivos, discos rígidos, unidades móveis, mensagens de e-mail e anexos, viabilizando detecção de ameaças, com intento de salvaguardar a estrutura tecnológica de ataques com teor e objetivo malicioso;
- Possibilitar o controle de acesso e tráfego de informações aos dispositivos e serviços operacionais na rede, através de gerenciamento centralizado, o que vem a complementar o conjunto de procedimentos que contemplam a política de segurança, concebendo qualidade no serviço de proteção;
- Aprimorar a segurança de TIC da CMFI frente a ameaças sofisticadas.

11) PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Tendo em vista que nosso ambiente de tecnologia já possui uma solução de firewall, não será necessária nenhuma providência prévia.

12) VIABILIDADE DA CONTRATAÇÃO

Esta equipe de TI declara viável esta contratação

13) TRATAMENTO DIFERENCIADO E FAVORECIDO A SER DISPENSADO ÀS MICROEMPRESAS, ÀS EMPRESAS DE PEQUENO PORTE E AOS MICROEMPREENDEDORES INDIVIDUAIS

Após diversas tentativas de localização e contato com empresas qualificadas como microempresas (ME) e empresas de pequeno porte (EPP) na região de Foz do Iguaçu para fornecimento das licenças, constatou-se a inexistência, inclusive pelo embasamento da pesquisa na base de de empresas credenciadas junto ao portal do desenvolvedor, acessado na data de 10/06/2024 às 09:38. Durante o processo de prospecção, entramos em contato direto com diversas empresas locais, incluindo aquelas registradas como ME e EPP, para verificar a capacidade técnica e a disponibilidade para fornecimento do serviço requerido. Nenhuma das ME/EPP contactadas demonstrou capacidade técnica ou interesse em participar do certame.

Diante dessas circunstâncias, a manutenção da exclusividade do certame para ME e EPP pode inviabilizar a contratação, comprometendo a eficiência e a continuidade dos serviços públicos dependentes de uma conexão estável e de alta velocidade, eis que

há sério risco da licitação ser deserta. Ressalta-se, porém, que as ME/EPP ainda poderão participar do certame com vantagens sobre os demais concorrentes conforme versa a legislação pátria.

Portanto, justifica-se o afastamento da exclusividade de participação de microempresas e empresas de pequeno porte neste certame específico, com base na inexistência de fornecedores locais qualificados e na necessidade imperiosa de garantir a prestação adequada e contínua dos serviços públicos.

14) RESPONSÁVEIS PELA ELABORAÇÃO DO ETP

Jeverson Siqueira
Cargo: Tecnico de Informatica
Matrícula: 202.045
Setor: Diretoria de Tecnologia

VERIFICAÇÃO DAS ASSINATURAS

Código para verificação: AD30-E329-B4EC-1FF9

Este documento foi assinado digitalmente pelos seguintes signatários nas datas indicadas:

JEVERSON SIQUEIRA (CPF 080.XXX.XXX-74) em 03/10/2024 08:41:08 (GMT-03:00)
Papel: Parte
Emitido por: Sub-Autoridade Certificadora 1Doc (Assinatura 1Doc)

Para verificar a validade das assinaturas, acesse a Central de Verificação por meio do link:

https://fozdoiguacu.1doc.com.br/verificacao/AD30-E329-B4EC-1FF9

M I N U T A

CONTRATO Nº 19/2024

TERMO DE CONTRATO DE PRESTAÇÃO DE SERVIÇOS, QUE FAZEM ENTRE SI A CÂMARA MUNICIPAL DE FOZ DO IGUAÇU E A EMPRESA XXXXXXXXXXXXXXXXXX.

A **Câmara Municipal de Foz do Iguaçu**, pessoa jurídica de direito público, com sede em Foz do Iguaçu, Estado do Paraná, situada na Travessa Oscar Muxfeldt, 81, Centro, inscrita no CNPJ/MF sob o nº 75.914.051/0001-28, neste ato representada por seu Presidente, João José Arce Rodrigues, consoante competência originária prevista no art. 17 do Regimento Interno da Câmara Municipal de Foz do Iguaçu, daqui para frente denominada simplesmente de **CONTRATANTE,** e, de outro lado, a empresa XXXXXXXXXXXXXXXXXXXXXX, inscrita no CNPJ/MF sob o nº XXXXXXXXX/XXXX-XX, situado na XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, cidade de XXXXXXXXXX, Estado XXXXXXXXX, CEP: XX.XXX-XXX, representada por seu representante legal XXXXXXXXXXXXXXXXXXXX, inscrito junto ao CPF/MF sob n. XXXXXXXXXX, a seguir denominada simplesmente **CONTRATADA**, firmam o presente contrato, sujeitando-se às cláusulas a seguir expostas e às normas da Lei n. 14.133/2021, têm entre si justo e contratado o que segue:

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O objeto do presente contratação de empresa especializada e tecnicamente qualificada para o fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business (KESB SELECT), com upgrade para Kaspersky Next EDR Optimum, para um período de 36 meses, de acordo com as características e especificações técnicas e, quantitativos descritos em termo de referência, bem como em seus anexos, conforme descrição a seguir:

ITEM	CAT/MAT	DESCRIÇÃO	QUANT.	UNIDADE	VALOR UNIT.	VALOR TOTAL
1	350949	KASPERSKY NEXT EDR OPTIMUM	160	Uni	R$ XXXXX,XX	R$ XXXXXX,XX
TOTAL						R$ XXXXXX,XX

2. CLÁUSULA SEGUNDA – DA VINCULAÇÃO

2.1. Os Contraentes reconhecem a vinculação desta contratação aos termos do Pregão Eletrônico n. XX/XXXX, emitido pela CONTRATANTE e à respectiva proposta que for vencedora, sendo que as

especificações técnicas mínimas do objeto, a fundamentação da contratação, a descrição da solução como um todo, as condições da garantia, os requisitos de habilitação, qualificação, técnica e capacidade operacional e de fornecimento, os requisitos da contratação, dentre outras informações, estão constantes em Termo de Referência, que é parte integrante deste Contrato independentemente de sua transcrição, ao qual também se declaram vinculados os contraentes.

3. CLÁUSULA TERCEIRA – DA LEGISLAÇÃO APLICÁVEL E DOS CASOS OMISSOS

3.1. Aplica-se a Lei n. 14.133/2021 à execução deste Contrato, sendo esta também a legislação a ser aplicadas aos casos omissos.

4. CLÁUSULA QUARTA – DO REGIME DE EXECUÇÃO

4.1. Os serviços serão executados sob o regime de execução indireta.

4.2. A execução dos serviços especificados neste Contrato e em Termo de Referência deverá ter início em até 30 dias, contados da assinatura do contrato, mediante fornecimento das licenças registradas em nome da CÂMARA MUNICIPAL DE FOZ DO IGUAÇU, nome fantasia PODER LEGISLATIVO, CNPJ n. 75.914.051/0001-28, atreladas a conta suporte@fozdoiguacu.pr.leg.br, dentro da plataforma da desenvolvedora Karpersky Global.

4.2. Quando realizada a disponibilização da licença, notificar via e-mail os responsáveis técnicos, sanches@fozdoiguacu.pr.leg.br e rodrigo@fozdoiguacu.pr.leg.br com detalhes do acesso.

4.3. Os serviços de instalação e manutenção deverão ser realizados na sede administrativa da CONTRATANTE, no endereço Travessa Oscar Muxfeldt, 81 - Centro, Foz do Iguaçu - PR, 85851-490

4.4. Os serviços a serem contratados constituem-se em atividades materiais acessórias, instrumentais ou complementares à área de competência legal da CONTRATANTE, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

4.5. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e a Administração, vedando-se qualquer relação entre elas que caracterize pessoalidade e subordinação direta.

4.6. Os serviços contratados são enquadrados como continuados, tendo em vista a sua necessidade permanente para a CONTRATANTE.

5. CLÁUSULA QUINTA – PREÇO

5.1. Em contra partida aos serviços prestados a CONTRATANTE pagará à CONTRATADA o valor mensal de até R$ XXXXX, totalizando estimativa de pagamento anual de até R$ XXXXX, conforme descrito na proposta apresentada pela empresa e constante no processo administrativo.

5.2. No valor indicado estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, seguro e outros necessários ao cumprimento integral do objeto da contratação.

6. CLÁUSULA SEXTA – DO REAJUSTE

6.1. Mediante expresso pedido da CONTRATADA, os valores contratados poderão ser reajustados a cada 12 (doze) meses, contados a partir da data da proposta apresentada pela CONTRATADA, com aplicação do índice de variação do ICTI – Índice de Custo da Tecnologia da Informação, calculado pelo IPEA, para o mesmo período ou outro índice que o substitua.
6.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de 12 (doze) meses para a próxima reajustamento, será contado a partir dos efeitos financeiros do último reajuste.
6.3. O reajuste previsto nesta cláusula poderá ser formalizado por Termo de Apostilamento.

7. CLÁUSULA SÉTIMA – DOS CRITÉRIOS DE MEDIÇÃO
7.1. Os Materiais entreguem dever estar em conformidade com as quantidades solicitadas dos itens já descritos neste documento;
7.2. A qualidade exigida dos equipamentos e materiais utilizados tem que estar de acordo com a qualidade de cada item, sendo vedada a utilização de materiais de qualidade inferior ou de não garantia.
7.3. Todos os pontos instalados devem ser certificados para assim constatar a qualidade do serviço e garantia de transmissão do mesmo.
7.4. Dos demais todos os itens devem ser novos seguidos rigidamente as especificações mínimas descritas na seção Requisitos da Contratação e amparados em seu prazo de garantia estabelecidos.

8. CLÁUSULA OITAVA – DO RECEBIMENTO
8.1. Os serviços serão recebidos provisoriamente no prazo de 05 (cinco) dias, para efeito de posterior verificação de sua conformidade com as especificações constantes na proposta;
8.2. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes na proposta, devendo ser substituídos no prazo de 10 (dez) dias, a contar da notificação da CONTRATANTE, às suas custas, sem prejuízo da aplicação das penalidades;
8.3. Na impossibilidade de realização dos serviços, a empresa vencedora deverá substituir o serviço por outro com especificações iguais ou superiores;
8.4. Os serviços serão recebidos definitivamente no prazo de 10 (dez) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação;
8.5. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo;
8.6. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da CONTRATADA pelos prejuízos resultantes da incorreta execução do contrato.

9. CLÁUSULA NONA – DO PAGAMENTO
9.1. Os pagamentos serão efetuados até o 10º (décimo) dia após o recebimento definitivo dos produtos/serviços, condicionado a apresentação da Nota Fiscal/Fatura, bem como os documentos de regularidade fiscal, social e trabalhista exigidos pelo art. 68 da Lei nº 14.133/2021.
9.2. Na eventualidade de ocorrer atraso no pagamento, o valor será atualizado pela variação acumulada do IPCA, ocorrida entre a data de seu adimplemento e a do efetivo pagamento, calculada pro rata tempore.

9.3. A apresentação da nota fiscal/fatura é indispensável a cada entrega de produtos ou prestação de serviços, para fins de liquidação e pagamento da despesa, a ser emitida ao destinatário: Razão social: CÂMARA MUNICIPAL DE FOZ DO IGUACU; CNPJ: 75.914.051/0001-28; Endereço: Travessa Oscar Muxfeldt, nº 81, Centro, na cidade de Foz do Iguaçu-Paraná, CEP 85.851-490. Telefone: (45) 3521-8100.
9.4. Antes de cada pagamento à CONTRATADA, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.
9.5. Havendo erro na apresentação da Nota Fiscal ou dos documentos pertinentes à contratação, ou, ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a CONTRATADA providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se- á após a comprovação da regularização da situação, não acarretando qualquer ônus para a CONTRATANTE.
9.6. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
9.7. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável. A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.
9.8. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua notificação, por escrito, para que, no prazo de 15 (quinze) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.
9.9. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à extinção contratual nos autos do processo administrativo correspondente, assegurada à CONTRATADA a ampla defesa.
9.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela extinção do contrato, caso a CONTRATADA não regularize sua situação junto ao SICAF.
9.11. O prazo desta contratação será de 36 meses, contados da assinatura do contrato.

10. CLÁUSULA DÉCIMA – DO PRAZO PARA RESPOSTA AOS PEDIDOS DE REPACTUAÇÃO DE PREÇOS E RESTABELECIMENTO DO EQUILÍBRIO ECONÔMICO

10.1. Quando for o caso de repactuação de preços e/ou de restabelecimento do equilíbrio econômico deste Contrato, será de 30 dias úteis o prazo resposta da CONTRATANTE, a contar da data de formalização do pedido por parte da CONTRATADA.

11. CLÁUSULA DÉCIMA PRIMEIRA - DA INEXIGÊNCIA DE GARANTIAS À EXECUÇÃO DO CONTRATO

11.1. Dadas as características da contratação, não haverá exigência de garantia à execução do contrato.

12. CLÁUSULA DÉCIMA SEGUNDA – DA GARANTIA DOS PRODUTOS E SERVIÇOS

12.1. As empresas licitantes deverão indicar o prazo da garantia do Software ou licença, que deverá ser de 36 meses oferecido diretamente ou com a autorização e responsabilidade do fabricante, sendo este o período em que se obrigam a prestar a manutenção e assistência técnica gratuita, nos termos regulados em termo de referência.

12.2. Serão desclassificadas as propostas que não ofereçam prazo de garantia ou abaixo do mínimo estipulado. As empresas licitantes indicarão, SOB PENA DE DESCLASSIFICAÇÃO, informações relacionadas à PADRONIZAÇÃO e COMPATIBILIDADE da solução, conforme detalhamento no ETP.

13. CLÁUSULA DÉCIMA TERCEIRA – DOTAÇÃO ORÇAMENTÁRIA

13.1. As despesas decorrentes desta contratação estão programadas em dotação orçamentária própria, prevista no orçamento da Câmara Municipal, para o exercício de 2024 nas classificações: item 1 – 01.01.01.031.0001.2002.3.3.90.40.99.05 – AQUISIÇÃO DE LICENÇA TEMPORÁRIA DE SOFTWARE.

13.2. Nos exercícios seguintes, correrão à conta dos recursos próprios para atender às despesas da mesma natureza, cuja alocação será feita no início de cada exercício financeiro.

14. CLÁUSULA DÉCIMA QUARTA – DAS OBRIGAÇÕES DA CONTRATANTE

14.1. A CONTRATANTE obriga-se a:

14.1.1. Comunicar à Contratada quaisquer irregularidades nos equipamentos, para adoção das providências cabíveis;

14.1.2. Designar funcionário para acompanhar/fiscalizar a entrega;

14.1.3. Efetuar os pagamentos relativos ao presente contrato em moeda corrente quando da apresentação da fatura de serviços executados respeitando os prazos de vencimentos;

14.1.4. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta;

14.1.5. Qualquer alteração deste, somente deverá ser com o aval dos gestores do contrato;

14.1.6. Aplicar a contratada as sanções administrativas regulamentares e contratuais cabíveis.

15. CLÁUSULA DÉCIMA QUINTA – DAS OBRIGAÇÕES DA CONTRATADA

15.1. A CONTRATADA obriga-se a:

15.1.1. Cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto;

15.1.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do contrato, inerentes à execução do objeto contratual;

15.1.3. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

15.1.4. É de responsabilidade da CONTRATADA, manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob

qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

16. CLÁUSULA DÉCIMA SEXTA – DAS SANÇÕES ADMINISTRATIVAS

16.1. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei n° 14.133, de 2021, quais sejam:

16.1.1. Dar causa à inexecução parcial do contrato;

16.1.2. Dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

16.1.3. Dar causa à inexecução total do contrato;

16.1.4. Deixar de entregar a documentação exigida para o certame;

16.1.5. Não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

16.1.6. Não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

16.1.7. Ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

16.1.8. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

16.1.9. Fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

16.1.10. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

16.1.11. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

16.1.12. Praticar atos ilícitos com vistas a frustrar os objetivos deste certame;

16.1.13. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

16.1.13.1. Multa de até 10 % (dez por cento) sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor;

16.1.15. Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, quando não se justificar a imposição de penalidade mais grave;

16.1.16. Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 16.1.8 e bem como nos demais casos que justifiquem a imposição da penalidade mais grave.

16.2. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao fornecedor.

17. CLÁUSULA DÉCIMA SÉTIMA - DA OBRIGAÇÃO DE MANUTENÇÃO DAS CONDIÇÕES DE QUALIFICAÇÃO

17.1. A CONTRATADA obriga-se a manter, durante toda a execução do Contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições para a qualificação na contratação direta que precedeu a este instrumento;

18. CLÁUSULA DÉCIMA OITAVA - DA OBRIGAÇÃO DE RESERVA DE CARGOS PREVISTA EM LEI

18.1. A CONTRATADA, durante toda a execução do Contrato, obriga-se a cumprir as exigências de reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz.

19. CLÁUSULA DÉCIMA NONA – MODELO DE GESTÃO DO CONTRATO

19.1. A execução do objeto seguirá a seguinte dinâmica:

19.1.1. A contratante indicará Fiscal de contratos que irá acompanhar a execução do contrato em conformidade com este termo de referência.

19.1.2. O Contrato terá o prazo de 3 (três) anos, podendo ser prorrogado.

19.1.3. A Contratada formalizará a designação do preposto da empresa, especificando os poderes e responsabilidades relacionados à execução do objeto contratado.

19.1.4. Toda comunicação entre a Contratante e a Contratada deverá ser formalizada por escrito, especialmente quando exigido por lei, podendo ser realizada por meio de mensagem eletrônica, quando aplicável.

19.1.5. A execução será realizada de forma parcelada formalizada pelo envio da ordem de compra.

19.1.6. Os prazos e critérios para recebimento e pagamento estão detalhados nas cláusulas 7 a 9 retro.

19.1.7. Considera-se ocorrido o recebimento da nota fiscal quando a Gestão de contratos atestar a execução do objeto do contrato através do termo de recebimento definitivo.

19.1.8. Não haverá exigência de garantia contratual da execução, devido às características da contratação.

20. CLÁUSULA VIGÉSIMA – DA INEXECUÇÃO E DA EXTINÇÃO DO CONTRATO

20.1. A inexecução total ou parcial do contrato ensejará a sua extinção com as consequências contratuais e as previstas em lei, com fulcro no Título III, Capítulo VIII da Lei n. 14.133/2021, nos seguintes modos:

20.1.1. determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta;

20.1.2. consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração;

20.1.3. determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

20.2. Constituirão motivos para extinção do contrato, a qual deverá ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa, as seguintes situações:

20.2.1. não cumprimento ou cumprimento irregular de normas editalícias ou de cláusulas contratuais, de especificações, de projetos ou de prazos;

20.2.2. desatendimento das determinações regulares emitidas pela autoridade designada para acompanhar e fiscalizar sua execução ou por autoridade superior;
20.2.3. alteração social ou modificação da finalidade ou da estrutura da empresa que restrinja sua capacidade de concluir o contrato;
20.2.4. decretação de falência ou de insolvência civil, dissolução da sociedade ou falecimento do contratado;
20.2.5. caso fortuito ou força maior, regularmente comprovados, impeditivos da execução do contrato;
20.2.6. atraso na obtenção da licença ambiental, ou impossibilidade de obtê-la, ou alteração substancial do anteprojeto que dela resultar, ainda que obtida no prazo previsto;
20.2.7. atraso na liberação das áreas sujeitas a desapropriação, a desocupação ou a servidão administrativa, ou impossibilidade de liberação dessas áreas;
20.2.8. razões de interesse público, justificadas pela autoridade máxima do órgão ou da entidade CONTRATANTE.
20.3. O descumprimento, por parte da CONTRATADA, de suas obrigações legais e/ou contratuais assegurará ao CONTRATANTE o direito de extinguir o contrato a qualquer tempo, independentemente de aviso, interpelação judicial e/ou extrajudicial.
20.4. A extinção por ato unilateral do CONTRATANTE sujeitará a CONTRATADA à multa rescisória de até 10% (dez por cento) sobre o valor do saldo do contrato existente na data da extinção, independentemente de outras penalidades.
20.5. Caso o valor do prejuízo do CONTRATANTE advindo da extinção contratual por culpa da CONTRATADA exceder o valor da Cláusula Penal prevista no parágrafo anterior, esta valerá como mínimo de indenização, na forma do disposto no art. 416, parágrafo único, do Código Civil.
20.6. A extinção determinada por ato unilateral da Administração e a extinção consensual deverão ser precedidas de autorização escrita e fundamentada da autoridade competente e reduzidas a termo no respectivo processo.
20.7. A CONTRATANTE poderá rescindir o presente instrumento contratual, sem qualquer ônus à Administração, quando da conclusão de eventual novo procedimento de contratação de interesse público para objeto afim.

21. CLÁUSULA VIGÉSIMA PRIMEIRA – DA VIGÊNCIA

21.1. O presente Contrato terá validade de 36 (trinta e seis) meses, contados da data da assinatura, podendo ser prorrogado, a critério da Administração, conforme o disposto no art. 107, da Lei n. 14.133/2021 e suas alterações posteriores.
21.2. A prorrogação deste contrato deverá ser promovida mediante celebração de termo aditivo.

22. CLÁUSULA VIGÉSIMA SEGUNDA – DA FISCALIZAÇÃO

22.1. O acompanhamento e a fiscalização da execução das obrigações oriundas deste contrato ficarão a cargo do Gestor José Marceo Nicoletti Teixeira, e do Fiscal de Contratos, Jeverson Siqueira, e consiste na verificação da conformidade da prestação dos serviços e da alocação dos recursos necessários, de forma a assegurar o perfeito cumprimento do ajuste, devendo ser exercidos por um ou mais

representantes da CONTRATANTE, especialmente designados, na forma do art. 117 da Lei nº 14.133/2021.
22.2. O fiscal do contrato deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto nos §§ 1º e 2º do art. 117 da Lei nº 14.133/2021.
22.3. O descumprimento total ou parcial das demais obrigações e responsabilidades assumidas pela CONTRATADA ensejará a aplicação de sanções administrativas, previstas neste Termo de Contrato e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto nos artigos 156 e 137 da Lei nº 14.133/2021.
22.4. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da CONTRATANTE ou de seus agentes e prepostos, de conformidade com art. 120 da Lei nº 14.133/2021.

23. CLÁUSULA VIGÉSIMA TERCEIRA – DA SUBCONTRATAÇÃO
23.1. É vedada a subcontratação total ou parcial do objeto deste Termo de Contrato.

24. CLÁUSULA VIGÉSIMA QUARTA – DAS VEDAÇÕES
24.1. É vedado à CONTRATADA:
24.1.1. Caucionar ou utilizar este Termo de Contrato para qualquer operação financeira;
24.1.2. Interromper a execução dos serviços sob alegação de inadimplemento por parte da CONTRATANTE, salvo nos casos previstos em lei.

25. CLÁUSULA VIGÉSIMA QUINTA – DAS ALTERAÇÕES
25.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos art. 124 a 136 da Lei n. 14.133/2021.

26. CLÁUSULA VIGÉSIMA SEXTA – DA PUBLICAÇÃO
26.1. A CONTRATANTE providenciará a publicação deste contrato no Diário Oficial do Município de Foz do Iguaçu, na página da Câmara Municipal de Foz do Iguaçu nos termos do art. 174 da Lei n. 14.133/2021 e no Portal Nacional de Contratações Públicas (PNCP), para fins de garantia a ampla publicidade.

27. CLÁUSULA VIGÉSIMA SÉTIMA – DO FORO
27.1. Fica eleito o foro desta cidade de Foz do Iguaçu, Estado do Paraná, para dirimir toda e qualquer questão que derivar deste contrato.

E por estarem justas e acordadas, assinam as partes o presente instrumento, na presença de duas testemunhas, que também o subscrevem, para que surtam todos os efeitos jurídicos e legais.

Foz do Iguaçu, xx de xxxxx de 2024.

CÂMARA MUNICIPAL DE FOZ DO IGUAÇU
João José Arce Morales

XXXXXXXXXXX
xxxxxxxxxxx

Testemunhas:

_____
Nome: XXXXXX
RG: XXXXXX
CPF: XXXXXXX

_____
Nome: XXXXXXXXX
RG: XXXXXXX
CPF XXXXXX

ANEXO IV - MODELO DE PROPOSTA DE PREÇOS
PREGÃO, NA FORMA ELETRÔNICA, Nº 06/2024

REF: PREGÃO, NA FORMA ELETRÔNICA, Nº 06/2024-TIPO MENOR PREÇO

A empresa _____, estabelecida na _____, no bairro _____, no Município de _____, no Estado de _____, no n.º _____, na Prefeitura sob o n.º_____ e no Estado sob o nº_____, CNPJ n.º_____, telefone n.º (____) _____ e e-mail _____, pela presente e consoante as especificações técnicas contidas no Edital, vem propor os valores abaixo para fornecimento de licenças antivírus do Pregão, na forma Eletrônica, n° **06/2024**, conforme segue:

ITEM	DESCRIÇÃO	SKU	QNT	VALOR UNITÁRIO	VALOR TOTAL
1	Licença Kaspersky Next EDR Optimum Brazilian Edition. 150-249 User 3 year Governmental Renewal license	KL4066KASTJ	160		

O **PREÇO TOTAL** apresentado na presente proposta é de R$ _____ (valor por extenso).

Nesta proposta de percentual de desconto e preço estão considerados obrigatoriamente:

a) **O atendimento às especificações detalhadas do objeto, consoante Anexo I deste Edital;**
b) **A inclusão de todas as despesas que influenciam nos custos, tais como despesas com custo, transporte e frete, tributos (impostos, taxas, emolumentos, contribuições fiscais e parafiscais), obrigações sociais, trabalhistas, fiscais, encargos comerciais ou de qualquer natureza e todos os ônus diretos e indiretos,**
c) **O prazo de validade da proposta é de 90 (noventa) dias, a contar da data da sessão do pregão, na forma eletrônica.**

Esta empresa declara que está ciente e cumprirá, integralmente, todas as cláusulas do EDITAL retro citado.

Foz do Iguaçu, _____ de _____ de _____.

_____

Assinatura do representante legal da empresa proponente
NOME:
RG:
CARGO:

Proc. Administrativo 36- 279/2024

De: CARLOS K. - AGCONT

Para: Envolvidos internos acompanhando

Data: 25/10/2024 às 09:18:18

Certifico que a Licitação foi devidamente cadastrada no sistema compras.gov.br, com sessão prevista para acontecer no dia **26 de novembro de 2024, às 10h00** .

–

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras

Memorando 5.967/2024

De: CARLOS K. - AGCONT

Para: CMFI-DG-DIRADM-SG - Secretaria Geral

Data: 25/10/2024 às 09:24:04

Solicito vossos préstimos visando nova publicação junto ao Diário Oficial do arquivo anexo

_

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras

Anexos:

Aviso_de_Licitacao_Diario_Oficial_do_Municipio_Pregao_006_2024.docx
Aviso_de_Licitacao___Site___PE_06_assinado.pdf

Câmara Municipal de Foz do Iguaçu

ESTADO DO PARANÁ

Aviso de Licitação

Pregão, na Forma Eletrônica, nº 006/2024 – UASG 926470

OBJETO: Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business.

DATA DE ABERTURA: 26 de Novembro de 2024, às 10h00, no endereço eletrônico: https://www.gov.br/compras/pt-br/.

RECEBIMENTO DAS PROPOSTAS: Até as 10h00 do dia 26 de Novembro de 2024, às 10h00, exclusivamente por meio eletrônico, no endereço eletrônico https://www.gov.br/compras/pt-br/.

CRITÉRIO DE JULGAMENTO: Menor Preço por Item.

PREÇO MÁXIMO GLOBAL: O preço máximo deste certame está fixado em R$ 57.310,40 (Cinquenta e sete mil, trezentos e dez reais e quarenta centavos).

INFORMAÇÕES: O Edital e seus anexos podem ser obtidos no Protocolo Geral da Câmara Municipal, localizado na Travessa Oscar Muxfeldt, nº 81, Centro - Foz do Iguaçu/PR, no horário das 08h00min às 14h00min, no site da Câmara Municipal de Foz do Iguaçu: www.fozdoiguacu.pr.leg.br e no site https://www.gov.br/compras/pt-br/. Esclarecimentos adicionais serão prestados através do telefone (45) 3521-8100 ou pelo e-mail licitacao@fozdoiguacu.pr.leg.br.

Foz do Iguaçu, 25 de Outubro de 2024.

gov.br Documento assinado digitalmente
CARLOS ALBERTO KASPER
Data: 25/10/2024 09:23:14-0300
Verifique em https://validar.iti.gov.br

Carlos Alberto Kasper

Agente de Contratação

Memorando 1- 5.967/2024

De: Kelly N. - CMFI-DG-DIRADM-SG

Para: AGCONT - Agente de contratação

Data: 30/10/2024 às 10:39:42

Aviso publicado no DOM 5079, de 29/10/2024.

Anexos:

DOM_5079_p_25_27.pdf

RESOLVE:

Art. 1°. Aprovar a Minuta de Acordo de Cooperação **sem** Compartilhamento de Recurso Patrimonial e a Minuta de Acordo de Cooperação **com** Compartilhamento de Recurso Patrimonial, para se estabelecer vínculo cooperativo que não envolva a transferência de recursos, entre o Município de Foz do Iguaçu, por intermédio da Secretaria Municipal de Saúde - SMSA, e Organizações da Sociedade Civil, visando a execução de ações de interesses e condições recíprocas ou equivalentes, de modo a realizar um propósito comum, voltado ao interesse público, fundamentados na consolidação da sociedade civil e com o intuito de fortalecer as políticas públicas de saúde.

Art. 2°. Esta resolução entra em vigor na data de sua publicação.

Publique-se. Anote-se.

Foz do Iguaçu, 29 de outubro de 2024.

Osli de Souza Machado
Procurador Geral do Município
OAB/PR 14.343 – Matrícula 18828.02

ATOS DO LEGISLATIVO

PORTARIA DA PRESIDÊNCIA Nº 253/2024

O Presidente da Câmara Municipal de Foz do Iguaçu, Estado do Paraná, no uso de suas atribuições legais, com fundamento no Capítulo VI, da Lei Complementar nº 414/2023, e na forma do disposto na Resolução Legislativa nº 37/2007, e suas alterações posteriores e, tendo em vista o Despacho nº 11 que encaminha o Relatório Final do Processo Administrativo 1DOC 381/2024, da Comissão de Avaliação de Desempenho Funcional,

RESOLVE

Conceder, a contar de 1º de outubro de 2024, **Promoção Funcional** aos servidores relacionados a seguir, ocupantes de Cargo de Provimento Efetivo na Câmara Municipal de Foz do Iguaçu, com as respectivas matrículas, nomenclaturas dos cargos e níveis, na forma e condições mencionadas abaixo:

Mat.	Servidor	Cargo Atual	Cargo Novo
201.500	Cláudia Cristina de Araújo	Agente Administrativo V NM X – Letra B	Agente Administrativo VI NM XI – Letra B
201.499	Fábio Sérgio da Silva	Agente Administrativo VI NM XI – Letra C	Agente Administrativo VII NM XII– Letra C

João Morales
Presidente

AVISO DE CANCELAMENTO DE AUDIÊNCIA PÚBLICA

A Comissão de Educação, Cultura, Assistência Social e Defesa do Cidadão da Câmara Municipal de Foz do Iguaçu, Estado do Paraná, comunica que está cancelada a Audiência Pública que seria realizada no dia 6 de novembro de 2024, com início às 9:00 hrs, no Plenário desta Casa, para discussão do Projeto de Lei nº 131/2023, que "Institui e inclui no Calendário de Eventos Oficiais do Município a "Semana Municipal de combate ao aborto e reafirmação do direito à vida".

Câmara Municipal de Foz do Iguaçu, 23 de outubro de 2024.

Yasmin Hachem
Presidente da CECASDC

AVISO DE CANCELAMENTO DE AUDIÊNCIA PÚBLICA

A Comissão de Educação, Cultura, Assistência Social e Defesa do Cidadão da Câmara Municipal de Foz do Iguaçu, Estado do Paraná, comunica que está cancelada a Audiência Pública que seria realizada no dia 13 de novembro de 2024, com início às 9:00 hrs, no Plenário desta Casa, para discussão do Projeto de Lei nº 40/2024, que "Dispõe sobre a proibição de acesso ao benefício do Auxílio Aluguel no município para pessoas condenadas por maus-tratos contra animais".

Câmara Municipal de Foz do Iguaçu, 23 de outubro de 2024.

Yasmin Hachem
Presidente da CECASDC

AVISO DE LICITAÇÃO
Pregão, na Forma Eletrônica, nº 004/2024
UASG 926470 [90004/2024 NO SISTEMA COMPRAS.GOV]
- REPUBLICAÇÃO -

OBJETO: Contratação de empresa especializada para fornecimento de equipamentos de informática.

DATA DE ABERTURA: 21 de novembro de 2024, às 10h00, no endereço eletrônico: https://www.gov.br/compras/pt-br/.

RECEBIMENTO DAS PROPOSTAS: Até as 10h00 do dia 21 de novembro de 2024, exclusivamente por meio eletrônico, no endereço eletrônico https://www.gov.br/compras/pt-br/.

CRITÉRIO DE JULGAMENTO: Menor Preço por Item.

PREÇO MÁXIMO GLOBAL: O preço máximo deste certame está fixado em R$ 998.867,58 (Novecentos e noventa e oito mil, oitocentos e sessenta e sete reais e cinquenta e oito centavos).

INFORMAÇÕES: O Edital e seus anexos podem ser obtidos no Protocolo Geral da Câmara Municipal, localizado na Travessa Oscar Muxfeldt, nº 81, Centro - Foz do Iguaçu/PR, no horário das 08h00min às 14h00min, no site da Câmara Municipal de Foz do Iguaçu: www.fozdoiguacu.pr.leg.br e no site https://www.gov.br/compras/pt-br/. Esclarecimentos adicionais serão prestados através do e-mail licitacao@fozdoiguacu.pr.leg.br.

Foz do Iguaçu, 24 de Outubro de 2024

Carlos Alberto Kasper
Agente de Contratação

AVISO DE LICITAÇÃO
Pregão, na Forma Eletrônica, nº 006/2024 – UASG 926470

OBJETO: Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business.

DATA DE ABERTURA: 26 de Novembro de 2024, às 10h00, no endereço eletrônico: https://www.gov.br/compras/pt-br/.

RECEBIMENTO DAS PROPOSTAS: Até as 10h00 do dia 26 de Novembro de 2024, às 10h00, exclusivamente por meio eletrônico, no endereço eletrônico https://www.gov.br/compras/pt-br/.

CRITÉRIO DE JULGAMENTO: Menor Preço por Item.

PREÇO MÁXIMO GLOBAL: O preço máximo deste certame está fixado em R$ 57.310,40 (Cinquenta e sete mil, trezentos e dez reais e quarenta centavos).

INFORMAÇÕES: O Edital e seus anexos podem ser obtidos no Protocolo Geral da Câmara Municipal, localizado na Travessa Oscar Muxfeldt, nº 81, Centro - Foz do Iguaçu/PR, no horário das 08h00min às 14h00min, no site da Câmara Municipal de Foz do Iguaçu: www.fozdoiguacu.pr.leg.br e no site https://www.gov.br/compras/pt-br/. Esclarecimentos adicionais serão prestados através do telefone (45) 3521-8100 ou pelo e-mail licitacao@fozdoiguacu.pr.leg.br.

Foz do Iguaçu, 25 de Outubro de 2024.

Carlos Alberto Kasper
Agente de Contratação

FOZPREV

PORTARIA Nº 9.929

A Diretora-Superintendente da Autarquia Previdenciária – Foz Previdência – do Município de Foz do Iguaçu, Estado do Paraná, no uso das atribuições que lhe são conferidas pelo inciso VII do art. 79 do Decreto nº 18.345, de 4 de julho de 2008, em cumprimento da determinação judicial constante nos Autos nº **0028002-97.2022.8.16.0030**, do 1º Juizado Especial da Fazenda Pública de Foz do Iguaçu, e, ainda, em atendimento ao Memorando Interno nº 1274/2024, emitido em 22 de outubro de 2024 pela Procuradoria Jurídica da Foz Previdência, com ratificação pelo Chefe do Poder Executivo Municipal,

R E S O L V E:

Art. 1º REVISAR o cálculo e o valor do provento constantes no inciso II do Art. 1º da Portaria nº 7.839/2022, publicada no DOM nº 4.464, de 1º de agosto de 2022, página 15, que trata da concessão de Aposentadoria Voluntária por Idade e Tempo de Contribuição ao segurado **ANTONIO DIAS DE SOUZA**, matrícula nº 9819.01, cujo dispositivo passa a vigorar com a seguinte redação:

II – provento mensal inicial: **R$ 4.275,69** (quatro mil, duzentos e setenta e cinco reais e sessenta e nove centavos) correspondente ao valor integral de seu último vencimento base no cargo efetivo, nível de referência de vencimento **63** (R$ 3.886,99), acrescido do valor de R$ 388,70 a título de adicional de permanência, na competência julho/2022.

Parágrafo único. O valor do provento de aposentadoria devidamente atualizado pelos reajustes concedidos ao funcionalismo público até a presente revisão resultou no valor de **R$ 4.863,35** (quatro mil, oitocentos e sessenta e três reais e trinta e cinco centavos), a ser implantado na Folha de Pagamento de Benefícios na competência novembro/2024.

Memorando 5.968/2024

De: CARLOS K. - AGCONT

Para: GEST-CONT-FISC-CONT - Fiscalização de Contratos Administrativos - A/C Waldecir S.

Data: 25/10/2024 às 09:25:03

Solicito vossos préstimos visando a publicação do arquivo anexo junto à diário de grande circulação

_

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras

Anexos:

Aviso_de_Licitacao_Diario_de_Circulacao_Regional_Pregao_006_2024.docx

Memorando 1- 5.968/2024

De: Lucas H. - GEST-CONT-FISC-CONT

Para: AGCONT - Agente de contratação - A/C CARLOS K.

Data: 29/10/2024 às 10:19:39

Prezado,

Segue anexada a publicação solicitada, para a devida conferência e utilização, caso esteja em conformidade com a requisição realizada.

_

Lucas Matheus Horst
Agente Adminitrativo

Anexos:

Publicacao_Camara_Foz_do_Iguacu_29_10_2024.pdf

MARECHAL CANDIDO RONDON – PR
CONSELHO MUNICIPAL DOS DIREITOS DA CRIANÇA E DO ADOLESCENTE - CMDCA
Resolução nº 53/2024

SÚMULA: APROVAÇÃO DA COMISSÃO DE AVALIAÇÃO E INSCRIÇÃO DE ENTIDADES DO CONSELHO MUNICIPAL DOS DIREITOS DA CRIANÇA E DO ADOLESCENTE

O Conselho Municipal dos Direitos da Criança e do Adolescente – CMDCA/ Marechal Cândido Rondon, em conformidade com o artigo 11º da Lei Municipal nº 5.023 de 16 de Março de 2018, reunido em assembleia no dia 14 de outubro de 2024;

RESOLVE:

Art. 1º. – Aprovar a comissão de avaliação e inscrição de entidades do Conselho Municipal dos direitos da criança e do adolescente.

a) Patricia Adams
b) Beatriz Petry
c) Cleudimar Robeson Wulff
d) Roseli de Fatima Castro

Art. 2º. Revoga-se a Resolução **18/2023;**

Art. 3º. - Esta resolução passa a vigorar a partir de sua publicação.

Marechal Cândido Rondon, 28 de outubro de 2024

Cleudimar Robeson Wulff
Presidente do C.M.D.C.A.

MARECHAL CÂNDIDO RONDON – PR
CONSELHO MUNICIPAL DOS DIREITOS DA CRIANÇA E DO ADOLESCENTE - CMDCA
Resolução nº 51/2024

SÚMULA: Aprova a comissão de processo disciplinar

O Conselho Municipal dos Direitos da Criança e do Adolescente de Marechal Cândido Rondon (CMDCA – Mal.Cdo.Rondon), em conformidade com a Lei Municipal nº 5.023 de 16 de Março de 2018, reunido em assembleia no dia 14 de outubro de 2024;

RESOLVE:

Art.1°- Aprovar a comissão de processo disciplinar.

a) Roselaine Feiden
b) Tania Cristina Steffen Schumann
c) Nair Boehs
d) Magna Marcia Merlini

Art.2°-Revoga-se a Resolução 01/2024;

Art.3º-Esta resolução passa a vigorar a partir da sua publicação.

Marechal Cândido Rondon, 28 de outubro de 2024.

Cleudimar Robeson Wulff
Presidente do C.M.D.C.A.

MARECHAL CANDIDO RONDON- PR
CONSELHO MUNICIPAL DOS DIREITOS DA CRIANÇA E DO ADOLESCENTE - CMDCA

Edital de Convocação Nº 016/2024

O Conselho Municipal dos Direitos da Criança e do Adolescente de Marechal Cândido Rondon CONVOCA seus membros conselheiros e convida os demais interessados a participarem da reunião extraordinária, que será realizada no dia 04 de novembro de 2024, às 09:00 horas, nas dependências do Auditório da Prefeitura, situado à Rua Espírito Santo, 777, nesta cidade, Centro. Convocação esta, tendo como pauta:

a) Análise e votação do relatório final da Comissão de Ética do processo: 01/2024.

Marechal Cândido Rondon, 28 de outubro de 2024.

Cleudimar Robeson Wulff
Presidente do C.M.D.C.A.

SERVIÇO AUTÔNOMO DE ÁGUA E ESGOTO – SAAE
MARECHAL CÂNDIDORODON – PARANÁ
CNPJ: 76.878.669/0001-42

CERTIDÃO DE TRÂNSITO EM JULGADO

Processo Administrativo Sancionador n.º 002/2024 Assunto: Inexecução Contratual - Processo Licitatório nº 70/2023 – Pregão nº 24/2023 - Contrato Administrativo n.º 64/2023 Empresa Sancionada: Backup Manutenção e Distribuição de Produtos de Informática Ltda. **CNPJ**: 40.224.243.0001/28**Sanção**: Suspensão de licitar e contratar com o Serviço Autônomo de Água e Esgoto de Marechal Cândido Rondon, pelo prazo de 02 (dois) ano. Certifico que na data de 22 de agosto de 2024 TRANSITOU EM JULGADO a decisão de fls. 84-88, estando a sanção apta a ser aplicada a partir de tal data. Marechal Cândido Rondon - PR, 22 de outubro de 2024. **Anderson Loffi Schmoeller** Diretor Executivo Portaria Municipal n 1.126/2023

* **OBS**: Documentos na íntegra no site da Prefeitura: https://marechalcandidorondon.atende.net/?pg=autoatendimento#!/tipo/servico/valor/8/padrao/1/load/0/ – Entidade: SAAE. Gabinete do Diretor Executivo do Serviço Autônomo de Água e Esgoto – SAAE, de Marechal Cândido Rondon-PR, em 28 de outubro de 2024. Anderson Loffi Schmoeller, Diretor Executivo. Publicidade suplementar, na forma da Lei n.º 4.838/2016, art. 3º, § 1°.

PODER JUDICIÁRIO DO ESTADO DO PARANÁ
COMARCA DE TOLEDO
3ª SECRETARIA DO CÍVEL DE TOLEDO - PROJUDI
Rua Almirante Barroso, 3202 - Fórum Juiz Vilson Balão - Centro - Toledo/PR - CEP: 85.900-020
Fone: 45 3327-9254 - E-mail: tol-3vj-s@tjpr.jus.b

EDITAL DE CITAÇÃO DA EXECUTADO GILBERT SOARES CAETANO
PRAZO DE 20 (VINTE) DIAS.

CITAÇÃO de: GILBERT SOARES CAETANO, brasileiro, em união estável, empresário, inscrito no CPF nº. 150.637.528-61.

PROCESSO: 0003737-33.2021.8.16.0170 de Execução de Título Extrajudicial, em que é exequente COOPERATIVA DE CREDITO DA REGIAO MERIDIONAL DO BRASIL - SICOOB UNICOOB MERIDIONAL, inscrita no CNPJ nº. 05.392.810/0001-54, em trâmite na 3ª Secretaria do Cível da Comarca de Toledo, Estado do Paraná.

OBJETIVO: Citar o executado para, em 03 (três) dias, pagar o débito exequendo, acrescido das custas processuais e honorários advocatícios, conforme dispõe o artigo 829 do CPC, cientificando-o(a) ainda, de que poderá interpor Embargos à Execução, no prazo de 15 (quinze) dias, contados do decurso do prazo do presente edital, independentemente de penhora ou caução, nos termos dos artigos 914, § 1º e 915 do CPC. Cientifico-o(a) ainda, que lhe é facultado, no prazo de embargos, reconhecendo o crédito da exequente e comprovando o depósito de 30% do valor da execução, custas processuais e honorários advocatícios, requerer o pagamento do restante do débito em 06 (seis) parcelas mensais, acrescidas de correção monetária e juros de mora de 1% ao mês, conforme autoriza o artigo 916, caput, § 3º e § 5º do CPC. Sendo deferido o pedido, ficará suspensa a execução, contudo, na hipótese de indeferimento a execução prosseguirá, mantendo-se o depósito. Fixado os honorários advocatícios no valor equivalente a 10% do valor do débito conforme dispõe o artigo 827, *caput* do CPC, os quais serão reduzidos pela metade, na hipótese do executado efetuar o pagamento do débito no prazo de 03 (três) dias, conforme preceitua o parágrafo 1º desse dispositivo legal.

ALEGAÇÕES DA EXEQUENTE: "Trata-se de ação de execução de título extrajudicial ajuizada pela Cooperativa de Crédito da Região Meridional do Brasil - Sicoob Unicoob Meridional em decorrência do inadimplemento da Cédula de Crédito Bancário n° 861100, fato que ocasionou o vencimento antecipado das prestações devidas, conforme cláusula décima quinta. Diante disso, requereu-se a citação da parte Executada para quitação do débito.".

VALOR DA CAUSA: R$ 239.965,78 (duzentos e trinta e nove mil, novecentos e sessenta e cinco reais e setenta e oito centavos), em 16/04/2021.

ADVERTÊNCIA – Artigo 829 do CPC: "O executado será citado para pagar a dívida no prazo de 3 (três) dias, contado da citação". § 1º "Do mandado de citação constarão, também, a ordem de penhora e a avaliação a serem cumpridas pelo oficial de justiça tão logo verificado o não pagamento no prazo assinalado, de tudo lavrando-se auto, com intimação do executado". Artigo 257, IV do CPC: "(...) será nomeado curador especial em caso de revelia". E para que chegue ao conhecimento de todos, mandou expedir o presente edital, que será afixado no local de costume, na sede deste juízo e publicado na forma da Lei.

OBSERVAÇÃO: Este processo tramita através do sistema computacional PROJUDI, cujo endereço na *web* é *https://projudi.tjpr.jus.br/projudi/*. Todos os pedidos formulados em Juízo tramitarão por meio eletrônico (artigo 180 do CN). O acesso ao sistema pelos advogados depende de prévio cadastramento, o qual é obrigatório, devendo comparecer à Sede da Unidade Jurisdicional que já utilize o sistema eletrônico (OAB). Documentos devem ser anexados em formato digital em arquivos com no máximo 4MB cada.

PRAZO DO EDITAL: 20 (vinte) dias.

Dado e passado nesta cidade e Comarca de Toledo, Estado do Paraná, aos vinte e dois dias do mês de outubro do ano de dois mil e vinte e qutro. Eu, Natalia Tedeski Pena, Estagiária, o digitei e subscrevi.

Eugênio Giongo
Juiz de Direito

CÂMARA MUNICIPAL DE FOZ DO IGUAÇU
ESTADO DO PARANÁ

Aviso de Licitação
Pregão, na Forma Eletrônica, nº 006/2024 – UASG 926470

OBJETO: Contratação de empresa especializada e tecnicamente qualificada para fornecimento de licença de solução de segurança, na modalidade de renovação de licenças Kaspersky Endpoint Secury for Business.
DATA DE ABERTURA: 26 de Novembro de 2024, às 10h00, no endereço eletrônico: https://www.gov.br/compras/pt-br/.
RECEBIMENTO DAS PROPOSTAS: Até as 10h00 do dia 26 de Novembro de 2024, às 10h00, exclusivamente por meio eletrônico, no endereço eletrônico https://www.gov.br/compras/pt-br/.
CRITÉRIO DE JULGAMENTO: Menor Preço por Item.
PREÇO MÁXIMO GLOBAL: O preço máximo deste certame está fixado em R$ 57.310,40 (Cinquenta e sete mil, trezentos e dez reais e quarenta centavos).
INFORMAÇÕES: O Edital e seus anexos podem ser obtidos no Protocolo Geral da Câmara Municipal, localizado na Travessa Oscar Muxfeldt, nº 81, Centro - Foz do Iguaçu/PR, no horário das 08h00min às 14h00min, no site da Câmara Municipal de Foz do Iguaçu: www.fozdoiguacu.pr.leg.br e no site https://www.gov.br/compras/pt-br/. Esclarecimentos adicionais serão prestados através do telefone (45) 3521-8100 ou pelo e-mail licitacao@fozdoiguacu.pr.leg.br.

Foz do Iguaçu, 25 de Outubro de 2024.
Carlos Alberto Kasper - Agente de Contratação

MARECHAL CÂNDIDO RONDON – PR
CONSELHO MUNICIPAL DOS DIREITOS DA CRIANÇA E DO ADOLESCENTE - CMDCA
Resolução nº 52/2024

SÚMULA: Aprova a comissão especial de ética

O Conselho Municipal dos Direitos da Criança e do Adolescente – CMDCA/ Marechal Cândido Rondon, em conformidade com o artigo 11º da Lei Municipal nº 5.023 de 16 de Março de 2018, reunido em assembleia no dia 14 de outubro de 2024;

RESOLVE:

Art. 1º. – Aprovar a comissão especial de ética.

a) Patricia Adams
b) Viviane Spier Warken
c) Beatriz Petry
d) Roseni Trindade

Art. 2º. Revoga-se a Resolução **12/2023;**

Art. 3º. - Esta resolução passa a vigorar a partir de sua publicação.

Marechal Cândido Rondon, 28 de outubro de 2024

Cleudimar Robeson Wulff
Presidente do C.M.D.C.A.

EDITAL DE LEILÃO:

Dia 26 de novembro de 2.024, às 10:00 horas	Será oferecido o bem pelo valor de avaliação, não havendo interessados, será oferecido pela melhor oferta.

NÃO HAVENDO EXPEDIENTE NAS DATAS ACIMA OS LEILÕES SERÃO EFETUADOS NO PRIMEIRO DIA ÚTIL SUBSEQÜENTE.

LOCAL:	**LOCAL exclusivamente on-line NA PLATAFORMA: https://www.rmmleiloes.com.br**

RAIMUNDO MAGALHÃES DE MORAES, Leiloeiro Judicial, registrado na JUCEPAR sob o número 678 devidamente autorizado e designado pela Exma. Sra. Dra. Gabriela Macedo Outeiro, Juíza Titular da 2ª Vara do Trabalho de Toledo-PR, para realizar os atos expropriatórios através de hasta pública, venderá em Público Leilão, conforme art. 888 da CLT, no dia, hora e site supracitado, os bens objeto de penhora das ações trabalhistas, no estado de conservação em que se encontram, os bens serão oferecidos pelo valor da avaliação, não havendo licitantes, os bens serão oferecidos pela melhor, exceto preço vil. Sendo os processos e os bens a seguir descritos: **ATOrd 0000211-94.2017.5.09.0121, EDERSON BATISTA DE OLIVA X POLETTO ESTRUTURAS METALICAS E PRE-MOLDADOS LTDA E OUTROS.:** Semi Reboque SR/Rodokinho PRO 3E, carroceria Prancha, 3 eixos, ano/modelo: 2012/2012, cor cinza, placa: MME9D12, RENAVAN nº 1180788971, chassi: 9A9SCPAE3CCEN4075, avaliado em R$52.000,00, **ATSum 0000256-93.2020.5.09.0121, PIERRE RICHARD BOIS X CONCRETEX OESTE EIRELI.:** Veículo SCANIA/P114CB8X4NZ 330, pacas AJQ-6J33, renavam 0075.022522-0, chassi 9BSP8X4B013521304, Ano de fabricação/modelo 2000/2001, DIESEL, cor branca, equipado com betoneira para concreto 10m³, veículo com motor em manutenção, avaliado em R$320.000,00, **CartPrecCiv 0000888-80.2024.5.09.0121, DIEGO LUIS DA SILVA X MANICA COMERCIO DE ELETROMOVEIS - EIRELI.:** A - Um Box conjugado 1,38x1,88x52, Itália Versani, preto/branco, avaliado em R$1.115,50; B – Um Box conjugado conjugado 88x1,88x52 Itália Versani, preto/branco, avaliado em R$933,70; C – Um Roupeiro quatro portas 2GV Treviso Doripel branco/azul/rosa, avaliado em R$936,60; D – Um Roupeiro quatro portas 2GV com espelho Dallas Tozzeto Carvalho, avaliado em R$2552,50; E – Um Roupeiro quatro portas 4GV Bilbao Demobile am~emdoa/off White, avaliado em R$2.290,31; F – Um Roupeiro quatro portas 3GV retro Vitória Canaã, branco/wenge, avaliado em R$1.802,70; G – Um Estofado Pluma 2.50M Ret/Rec, personalle azul luxor, avaliado em R$3.936,60; H – Um Estofado Pluma 2.90M ret/rec Personalle cinza, avaliado em R$5.525,39; I – Um Estofado Belize canto 2,65x2,05 Ret Personalle marrom, avaliado em R$3.397,10; J – Um Estofado Sevilha 2.50 Ret/Rec idealflex azul, avaliado em R$3.566,80; K – Um Estofado Madri canto 205x190cm Hellen marrom Brown, avaliado em R$3.605,79; L – Um Estofado Maisa 2 metros Ret/Rec, Idealflex Marrom, avaliado em R$2.552,39; M - Estofado Kin 2.20 mts Ret/Rec Personalle Marrom, avaliado em R$2.830,39, avaliação total R$35.045,77, **ATSum 0000839-15.2019.5.09.0121, NEIDE ALVES DE OLIVEIRA E OUTROS X AURORA TEXTIL LTDA E OUTROS , ATOrd 0000939-67.2019.5.09.0121, ELIETE DOS SANTOS CHAVES X DLGV-INDUSTRIA E COMERCIO DE CONFECCOES LTDA E OUTROS.:** Cota parte de 8,33%, equivalente a 12.100m² do imóvel: Lote Rural nº 54.A.1, com a área de 145.200,00m², do 36ª Perímetro da Fazenda Britânia, localizado no distrito de Vila Nova, neste município e Comarca de Toledo-PR. Matrícula 46.024 do 1º Ofício de Registro de Imóveis da Comarca de Toledo/PR. Imóvel mecanizado e preparado para o plantio, atualmente com lavoura de milho. Em pequena porção do imóvel ainda há mata nativa (reserva legal), sem benfeitorias no imóvel, avaliado em sua totalidade em R$2.178.000,00 perfazendo a cota parte do executado de 8,33%, equivalente a 12.100m² em, avaliado em R$181.500,00. Os interessados em participar do leilão on-line deverão efetivar o cadastro e a solicitação de habilitação previamente no respectivo site (www.rmmleiloes.com.br), e apresentar os documentos necessários, podendo dirimir eventuais dúvidas pelo telefone (41) 3027-5252 e/ou (41) 98415-6982, diretamente com o Senhor Leiloeiro, Raimundo Magalhães de Moraes, matriculado na JUCEPAR sob n° 678. Os leilões serão regidos de acordo a Lei 21.981/32, pela CLT e subsidiariamente pelo CPC. Os bens móveis estarão na semana que antecede ao leilão, a disposição para a vistoria dos senhores interessados no endereço do leiloeiro e ou no endereço dos seus atuais depositários, sendo que os endereços estão nos escritórios do leiloeiro a disposição dos interessados. Já os bens imóveis estarão a disposição dos interessados para vistoria, desde que anteriormente agendados o dia e a hora junto ao leiloeiro. Os créditos tributários provenientes de impostos incidentes sobre o bem arrematado, até a data da realização da hasta pública, não serão de responsabilidade do arrematante, conforme dispõe o parágrafo único do art. 130, do Código Tributário Nacional. Demais despesas e ônus, inclusive as despesas de publicação de edital, serão por conta dos arrematantes. Ficam cientes os arrematantes que receberão os bens no estado em que se encontram e arcarão com os impostos, encargos e taxas para os devidos registros. Eventuais ônus e despesas que não puderam ser constatados antes da publicação deste edital serão informados quando da realização das hastas públicas. Alguns bens poderão ter a sua venda parcelada, conforme o Provimento 01/2005 e Provimento Geral da Corregedoria Regional do TRT 9ª Região. Ficam através deste edital intimadas as partes, os cônjuges, os credores hipotecários (artigo 1501 do Código Civil Brasileiro), os arrematantes e terceiros interessados. Cientes, também, que no ato da adjudicação, ou remição ou acordo entre as partes, serão cobrados os serviços do Leiloeiro, de armazenagem, do depositário judicial e as remunerações conforme Ordem de Serviços emitida pela Justiça do Trabalho TRT 9ª Região, das despesas informadas na Comunicação de Leilão e o Decreto Federal nº 21.981/1932, no Art. 22, alínea f. A comissão de Leilão, cujo resultado for positivo, sempre será devida ao Leiloeiro Oficial, pelo ATO PRATICADO (Decreto Federal N° 21.981/32), assumindo, conforme o caso, o arrematante, o adjudicante ou o remitente, o ônus desta despesa. No caso de indeferimento da arrematação pelo Juízo, a comissão será sempre devolvida ao arrematante. Caso os Exeqüentes, Executados, Credores hipotecários, cônjuges e terceiros interessados não sejam encontrados, notificados ou certificados por qualquer razão, da data de Praça e Leilão, quando da expedição das notificações respectivas, valerá o presente Edital de INTIMAÇÃO DE PRAÇA E LEILÃO. Fulcrado com o Artigo 238 da Lei 11.382 de 06 de dezembro de 2.006, Presumem-se válidas as comunicações e intimações dirigidas ao endereço residencial ou profissional declinado na inicial. O prazo para a apresentação de quaisquer medidas processuais contra os atos de expropriação, como embargos ou recursos, começará a contar da data do deferimento da arrematação e/ou adjudicação, independentemente de intimação. Toledo-PR, 16 de agosto de 2023 – Raimundo Magalhães de Moraes - Leiloeiro Judicial.

MUNICÍPIO DE MARECHAL CÂNDIDO RONDON

AUTORIZAÇÃO

PROCESSO LICITATÓRIO Nº 233/2024
DISPENSA DE LICITAÇÃO Nº 66/2024

O Prefeito do Município de Marechal Cândido Rondon, Estado do Paraná, bem como o Secretário Municipal de Agricultura, Pecuária e Desenvolvimento Sustentável, em cumprimento ao disposto no Artigo 75, da Lei nº 14.133/21, tendo em vista o parecer jurídico exarado no procedimento de **Dispensa nº 66/2024**, torna público o presente na forma seguinte:

OBJETO: **Contratação de serviço de coleta, transporte, triagem, processamento, beneficiamento e destinação final de resíduos sólidos recicláveis e reutilizáveis.** Este objeto será executado pela empresa **ASSOCIAÇÃO DE CATADORES AMIGOS DA NATUREZA (ACAN),** inscrita no CNPJ sob nº 32.393.906/0001-00, estabelecida na Est Linha Esquina Guaira, s/n, Horto Florestal – Zona Rural, na cidade de Marechal Cândido Rondon, Estado do Paraná, através de Dispensa de Licitação, pelo valor máximo de **R$1.028.286,96 (Um milhão, vinte e oito mil, duzentos e oitenta e seis reais e noventa e seis centavos)**.

FUNDAMENTO LEGAL: Contratação respaldada no Art. 75, inciso IV, alínea "j", da Lei de Licitações e Contratos nº 14.133, de 01/04/2021, conforme devidamente justificado no processo licitatório. Marechal Cândido Rondon, Paraná, em 25 de outubro de 2024. (a.a.) Marcio Andrei Rauber – Prefeito e Adriano Luiz Freitag – Secretário Municipal de Agricultura, Pecuária e Desenvolvimento Sustentável.

MUNICÍPIO DE MARECHAL CÂNDIDO RONDON

AVISO DE LICITAÇÃO - REPUBLICAÇÃO

MODALIDADE: CONCORRÊNCIA ELETRÔNICA Nº 26/2024. **(Localizar por 90.026/2024 – COMPRAS.GOV.BR)**
Critério de julgamento: Menor preço / Empreitada por preço global.
Objeto: Contratação de obra de reforma e ampliação da cobertura da Escola Municipal São João Batista, no Distrito de Novo Três Passos.
Valor Máximo: R$289.366,18
Recebimento de propostas: Das 08:00 horas do dia 29 de outubro de 2024, até às 08:29 horas do dia 21 de novembro de 2024.
Realização da sessão pública: A sessão pública iniciará às **08:30 horas no dia 21 de novembro de 2024**, na plataforma COMPRAS.GOV.BR - Portal de Compras do Governo Federal – https://www.gov.br/compras/pt-br/.
Local de Abertura/realização da sessão pública: COMPRAS.GOV.BR - Portal de Compras do Governo Federal – https://www.gov.br/compras/pt-br/.
Edital: O Edital, bem como demais arquivos relacionados, estará disponível aos interessados na Prefeitura Municipal de Marechal Cândido Rondon, situada à Rua Espírito Santo, nº 777, centro, em Marechal Cândido Rondon, Estado do Paraná, durante o horário normal de expediente, das 08h00min. às 11h45min. e das 13h15min. às 17h00min., através do site: www.mcr.pr.gov.br link: Licitações, consulta de licitações, escolher o edital e download, no COMPRAS.GOV.BR - Portal de Compras do Governo Federal e no Portal Nacional de Contratações Públicas - PNCP.
Dúvidas: Por e-mail: licita@mcr.pr.gov.br ou pelo Fone: (45) 3284-8828 ou 3284-8865, no horário normal de expediente. Publique-se. Marechal Cândido Rondon-PR, em 28 de outubro de 2024. (a.a.) Marcio Andrei Rauber–**PREFEITO.**

Município de Missal
ESTADO DO PARANÁ

AVISO DE LICITAÇÃO
PREGÃO ELETRÔNICO Nº 108/2024

Torna-se público que o **Município de Missal**, Estado do Paraná, CNPJ nº 78.101.847/0001-50, sito à Rua Nossa Senhora da Conceição, nº 555, Centro, no Município de Missa/Pr, CEP 85.890-000, por meio de seu Pregoeiro e Equipe de Apoio, designados pela **Portaria nº 393, de 04 de Junho de 2024**, realizará licitação na modalidade **PREGÃO**, na forma **ELETRÔNICA**, no critério de julgamento **MENOR PREÇO POR ITEM,** no modo de disputa **ABERTO**, nos termos da Lei nº 14.133 de 01 de Abril de 2021, e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital, visando a **AQUISIÇÃO DE APARELHOS DE AR-CONDICIONADO PARA A SECRETARIA MUNICIPAL DE SAÚDE,** valor máximo de **R$ 90.042,53**.
ABERTURA DA SESSÃO DE LANCES: 13 DE NOVEMBRO DE 2024 ÀS 14H 20MIN. (HORÁRIO DE BRASÍLIA-DF);
REALIZAÇÃO: Por meio do Site bllcompras.com;
ÍNTEGRA DO EDITAL: Disponível no Portal Nacional de Contratações Públicas - PNCP (https://pncp.gov.br/app/editais?q=&status=recebendo_proposta&pagina=1), na plataforma da BLL (https://bll.org.br/) e no endereço eletrônico do Município (https://transparencia.missal.pr.gov.br/licitacoes), ou ainda, pode ser solicitado pelo e-mail licitacao@missal.pr.gov.br.

Missal - PR, 28 de Outubro de 2024.
Adilto Luis Ferrari - **Prefeito Municipal**

RERRATIFICAÇÃO

Referente à publicação do AVISO DE DISPENSA ELETRÔNICA Nº 015/2024, publicado no "Diário Oficial do Município de Missal", Página 6, no dia 24 de Outubro de 2024, Edição nº 3406 - Ano XIV, e no "Jornal do Oeste", Publicações Legais, Edição 11.362, Página 11, no dia 26 de Outubro de 2024, onde se lê "**RECEBIMENTO DAS PROPOSTAS: Ocorrerá das 17h30min do dia 24 de Outubro de 2024, até às 08h50min do dia 04 de Novembro de 2024**" leia-se "**RECEBIMENTO DAS PROPOSTAS: Ocorrerá das 08h00min do dia 25 de Outubro de 2024, até às 08h50min do dia 04 de Novembro de 2024**", ficando o restante ratificado.

Missal/Pr, 28 de Outubro de 2024.
Ana Caroline Kochemborger - AGENTE DE CONTRATAÇÃO - Portaria nº 393, de 04 de Junho de 2024

RESULTADO DO EDITAL DE CHAMAMENTO PÚBLICO Nº 024/2024
PROCESSO DE INEXIGIBILIDADE Nº 100/2024
PROCESSO ADMINISTRATIVO Nº 227/2024

A **PREFEITURA MUNICIPAL DE MISSAL** informa o resultado do Edital de Chamamento Público nº 024/2024, **CREDENCIAMENTO DE EMPRESAS ESPECIALIZADAS PARA A PRESTAÇÃO DE SERVIÇOS DE METALÚRGICA E FORNECIMENTO DE MATERIAL, PARA MANUTENÇÕES DIVERSAS**, em conformidade com o **inciso I do art. 78, da Lei nº 14.133 de 1º de abril de 2021, do Decreto Municipal nº 5966 de 31 de Março de 2023** e nos termos e condições estabelecidas neste Edital e seus anexos, segundo critérios, termos e condições estabelecidos neste edital e nos seus anexos, sendo credenciada as seguintes empresas:

EMPRESA	LOTE	DATA/PROTOCOLO (PROCESSO)
DARLES JUNIOR VOGEL LTDA - ME, CNPJ Nº 40.694.392/0001-50	001	07/10/2024 – PROCESSO: 5747/2024, ÀS 10:20

Missal - PR, 28 de Outubro de 2024.
Adilto Luis Ferrari **- Prefeito Municipal**

EXTRATO DE CONTRATO DE FORNECIMENTO

ESPÉCIE CONTRATO DE FORNECIMENTO
LICITAÇÃO PREGÃO ELETRÔNICO Nº 102/2024
OBJETO AQUISIÇÃO DE PRODUTOS DE LIMPEZA PARA AS NOVE INSTITUIÇÕES MUNICIPAIS DE ENSINO.

FORNECEDOR	CNPJ	CONTRATO Nº	VALOR TOTAL
MULTISUL COMÉRCIO E DISTRIBUIÇÃO LTDA	12.811.487/0001-71	583	R$ 224,70

ENTREGA 15 (QUINZE) DIAS DE PRAZO
DOTAÇÕES 07 SECRETARIA DE EDUCAÇÃO, CULTURA E ESPORTE
GESTÃO DO ENSINO FUNDAMENTAL
MATERIAL DE CONSUMO
01480 E 00103 – 5% SOBRE TRANSFERÊNCIAS CONSTITUCIONAIS FUNDEB
01480 EA 00103 – 5% SOBRE TRANSFERÊNCIAS CONSTITUCIONAIS FUNDEB
GESTÃO DA EDUCAÇÃO INFANTIL
MATERIAL DE CONSUMO
01920 E 00104 – DEMAIS IMPOSTOS VINCULADOS À EDUCAÇÃO BÁSICA
DATA 25 DE OUTUBRO DE 2024

AVISO DE SUSPENSÃO TEMPORÁRIA AO CONTRATO Nº 149/2023

ESPÉCIE CONTRATO DE PRESTAÇÃO DE SERVIÇOS
LICITAÇÃO PREGÃO ELETRÔNICO Nº016/2023
PARTES MUNICÍPIO DE MISSAL.
JOSE ATIRIO FREISLEBEN KAUTZMANN 07797123900
OBJETO CONTRATAÇÃO DE EMPRESA(S) ESPECIALIZADA(S) PARA MINISTRAR OFICINAS CULTURAIS, SENDO: INSTRUMENTO MUSICAL - TECLADO (20 HORAS SEMANAIS); FANFARRA (06 HORAS SEMANAIS), E INSTRUTOR PARA OFICINA DE ACORDEON (GAITA PIANADA), DIRECIONADA PARA CRIANÇAS, JOVENS E ADULTOS
OBJETIVO ATRAVÉS DO PRESENTE TERMO COMUNICADO AS PARTES RESOLVEM AMIGAVELMENTE PROMOVER A SUSPENSÃO TEMPORÁRIA DO CONTRATO A PARTIR DO DIA 30 DE NOVEMBRO DE 2024, COM RETORNO EM DATA A SER DEFINIDA, CONFORME MEMORANDO Nº034/2024 SECE E AVISO DE SUSPENSÃO ASSINADA EM ANEXO.
DATA 17 DE OUTUBRO DE 2024

EXTRATO DO ADITIVO Nº 02
ADITIVO DE PRAZO E REPOSIÇÃO INFLACIONÁRIA AO CONTRATO DE TRANSPORTE ESCOLAR Nº 600/2023

ESPÉCIE PRESTAÇÃO DE SERVIÇOS
LICITAÇÃO PREGÃO ELETRÔNICO N°100/2023
PARTES MUNICÍPIO DE MISSAL
BRUNO HENRIQUE ARENHARDT TRANSPORTES LTDA -ME
CNPJ Nº23.701.076/0001-40
OBJETO CONSTITUI O OBJETO DO PRESENTE CONTRATO, E, PORTANTO, OBRIGAÇÃO PRINCIPAL DA CONTRATADA, A PRESTAÇÃO DE SERVIÇOS DE TRANSPORTE ESCOLAR PARA O MUNICÍPIO DE MISSAL, PELO PRAZO DE 12 (DOZE) MESES, CONFORME TERMO DE REFERÊNCIA, PODENDO SER PRORROGADO NAS FORMAS DA AUTORIZAÇÃO CONTIDA NO ARTIGO 57, II, DA LEI 8666/93 E ALTERAÇÕES POSTERIORES
OBJETIVO ATRAVÉS DO PRESENTE TERMO ADITIVO AS PARTES RESOLVEM AMIGAVELMENTE PROMOVER O A PRORROGAÇÃO DE PRAZO DO CONTRATO PARA MAIS 12 (DOZE) MESES, E EFETUAR A REPOSIÇÃO INFLACIONÁRIA PELO INPC ACUMULADO DO PERÍODO EM 4,09% (QUATRO VÍRGULA ZERO NOVE POR CENTO), DA LINHA 14 PASSANDO DE R$ 3,88 (TRÊS REAIS E OITENTA E OITO CENTAVOS) PARA O VALOR DE R$ 4,04 (QUATRO REAIS E QUATRO CENTAVOS) O KM RODADO, CONFORME PARECER JURÍDICO E MEMORANDO Nº452/2024 SECE EM ANEXO.
DATA 23 DE OUTUBRO DE 2024

AVISO DE SUSPENSÃO TEMPORÁRIA AO CONTRATO Nº 156/2022

ESPÉCIE CONTRATO DE PRESTAÇÃO DE SERVIÇOS
LICITAÇÃO PREGÃO ELETRÔNICO Nº026/2022
PARTES MUNICÍPIO DE MISSAL.
CLECI LUFT 88636089972
OBJETO CONTRATAÇÃO DE UMA EMPRESA PARA FORNECER UM PROFISSIONAL ESPECIALIZADO PARA COORDENAR E REGER O CORAL MUNICIPAL DE MISSAL
OBJETIVO ATRAVÉS DO PRESENTE TERMO COMUNICADO AS PARTES RESOLVEM AMIGAVELMENTE PROMOVER A SUSPENSÃO TEMPORÁRIA DO CONTRATO A PARTIR DO DIA 30 DE NOVEMBRO DE 2024, COM RETORNO EM DATA A SER DEFINIDA, CONFORME MEMORANDO Nº034/2024 SECE E AVISO DE SUSPENSÃO ASSINADA EM ANEXO.
DATA 17 DE OUTUBRO DE 2024

AVISO DE SUSPENSÃO TEMPORÁRIA AO CONTRATO Nº 148/2021

ESPÉCIE CONTRATO DE PRESTAÇÃO DE SERVIÇOS
LICITAÇÃO PREGÃO ELETRÔNICO Nº043/2021
PARTES MUNICÍPIO DE MISSAL.
WANDO MUELLER NOS 05400466982
OBJETO CONTRATAÇÃO DE EMPRESA PARA PRESTAÇÃO DE SERVIÇOS NO DEPARTAMENTO DE CULTURA, COM PROFISSIONAL HABILITADO PARA OFERECER AULAS DE VIOLÃO.
OBJETIVO ATRAVÉS DO PRESENTE TERMO COMUNICADO AS PARTES RESOLVEM AMIGAVELMENTE PROMOVER A SUSPENSÃO TEMPORÁRIA DO CONTRATO A PARTIR DO DIA 30 DE NOVEMBRO DE 2024, COM RETORNO EM DATA A SER DEFINIDA, CONFORME MEMORANDO Nº034/2024 SECE E AVISO DE SUSPENSÃO ASSINADA EM ANEXO.
DATA 17 DE OUTUBRO DE 2024

AVISO DE SUSPENSÃO TEMPORÁRIA AO CONTRATO Nº 533/2023

ESPÉCIE CONTRATO DE PRESTAÇÃO DE SERVIÇOS
LICITAÇÃO PREGÃO ELETRÔNICO Nº098/2023
PARTES MUNICÍPIO DE MISSAL.
SILVIA CRISTINA PUCINELI PAULI-MEI
OBJETO CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA MINISTRAR OFICINAS CULTURAIS, SENDO: PINTURA EM TELA À BASE DE TINTA ÓLEO E DESENHO ARTÍSTICO (30 HORAS SEMANAIS),
OBJETIVO ATRAVÉS DO PRESENTE TERMO COMUNICADO AS PARTES RESOLVEM AMIGAVELMENTE PROMOVER A SUSPENSÃO TEMPORÁRIA DO CONTRATO A PARTIR DO DIA 30 DE NOVEMBRO DE 2024, COM RETORNO EM DATA A SER DEFINIDA, CONFORME MEMORANDO Nº034/2024 SECE E AVISO DE SUSPENSÃO ASSINADA EM ANEXO.
DATA 17 DE OUTUBRO DE 2024

AVISO DE SUSPENSÃO TEMPORÁRIA AO CONTRATO Nº 268/2023

ESPÉCIE CONTRATO DE PRESTAÇÃO DE SERVIÇOS
LICITAÇÃO PREGÃO ELETRÔNICO Nº047/2023
PARTES MUNICÍPIO DE MISSAL
TONI ALEX RODRIGUES 81022948091 – ME
OBJETO CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA MINISTRAR OFICINA CULTURAL DE DANÇAS TRADICIONALISTAS GAUCHESCAS (10 HORAS SEMANAIS)
OBJETIVO ATRAVÉS DO PRESENTE TERMO COMUNICADO AS PARTES RESOLVEM AMIGAVELMENTE PROMOVER A SUSPENSÃO TEMPORÁRIA DO CONTRATO A PARTIR DO DIA 30 DE NOVEMBRO DE 2024, COM RETORNO EM DATA A SER DEFINIDA, CONFORME MEMORANDO Nº034/2024 SECE E AVISO DE SUSPENSÃO ASSINADA EM ANEXO.
DATA 17 DE OUTUBRO DE 2024

EXTRATO DE CONTRATO DE FORNECIMENTO

ESPÉCIE CONTRATO DE FORNECIMENTO
LICITAÇÃO PREGÃO ELETRÔNICO Nº 106/2024
OBJETO AQUISIÇÃO DE 01 (UMA) MOTO OFF ROAD, NOVA, 0KM, DE ACORDO COM O DECRETO LEGISLATIVO Nº 009/2024.

FORNECEDOR	CNPJ	CONTRATO Nº	VALOR TOTAL
MOTOPARK COMÉRCIO DE VEÍCULOS LTDA	76.078.823/0003-63	582	R$ 22.990,00

ENTREGA 30 (TRINTA) DIAS DE PRAZO
DOTAÇÕES 10 SECRETARIA DE INDÚSTRIA, COMÉRCIO E TURISMO
EVENTOS OFICIAIS
PREMIAÇÕES CULTURAIS, ARTÍSTICAS, CIENTÍFICAS, DESPORTIVAS E OUTRAS
03740 E 00505 – ROYALTIES TRATADO DE ITAIPU BINACIONAL
DATA 28 DE OUTUBRO DE 2024

MUNICÍPIO DE ENTRE RIOS DO OESTE
Estado do Paraná

EXTRATO DO CONTRATO
Nº DO CONTRATO: 168/2024
PROCESSO LICITATÓRIO: INEXIGIBILIDADE Nº 47/2024
CONTRATADO: 31.644.353/0001-58 - ICGP - TREINAMENTOS LTDA
VALOR TOTAL REGISTRADO: R$ 3.150,00
VIGÊNCIA: 25/10/2024 A 25/12/2024.
REGISTRE-SE E PUBLIQUE-SE. ENTRE RIOS DO OESTE-PR, EM 25/10/2024.

TERMO DE HOMOLOGAÇÃO E ADJUDICAÇÃO
REFERENTE A DISPENSA DE LICITAÇÃO Nº 27/2024 - PROCESSO Nº 153/2024
O Município de Entre Rios do Oeste, Estado do Paraná, torna a público que:
Fica homologado o procedimento licitatório em epígrafe e a adjudicação dos objetos as empresas abaixo relacionadas, para a plena consolidação do previsto neste Certame e depois de cumpridas as formalidades legais.
Resultou como DESERTO o item 1.
VALOR TOTAL HOMOLOGADO: R$ 2.928,00
REGISTRE-SE E PUBLIQUE-SE. Entre Rios do Oeste/PR, em 28 de outubro de 2024.

EXTRATO DAS ATAS DE REGISTRO DE PREÇOS
Nº DA ATA DE REGISTRO DE PREÇOS: 178/2024
PROCESSO LICITATÓRIO: PREGÃO ELETRÔNICO Nº 58/2024
CONTRATADO: 06.194.440/0001-03 - ODONTOMEDI - PRODUTOS ODONTOLOGICOS E HOSPITALARES LTDA - EPP
VALOR TOTAL REGISTRADO: R$ 17.452,19
VIGÊNCIA: 29/10/2024 A 29/10/2025.

Nº DA ATA DE REGISTRO DE PREÇOS: 179/2024
PROCESSO LICITATÓRIO: PREGÃO ELETRÔNICO Nº 58/2024
CONTRATADO: 50.567.060/0001-69 - DENTAL IPO LTDA
VALOR TOTAL REGISTRADO: R$ 9.789,78
VIGÊNCIA: 29/10/2024 A 29/10/2025.

Nº DA ATA DE REGISTRO DE PREÇOS: 180/2024
PROCESSO LICITATÓRIO: PREGÃO ELETRÔNICO Nº 58/2024
CONTRATADO: 16.366.888/0001-10 - DIPROM - DISTRIBUIDORA DE PRODUTOS ODONTOLOGICOS E MATERIAIS LTDA
VALOR TOTAL REGISTRADO: R$ 10.476,54
VIGÊNCIA: 29/10/2024 A 29/10/2025.

Nº DA ATA DE REGISTRO DE PREÇOS: 181/2024
PROCESSO LICITATÓRIO: PREGÃO ELETRÔNICO Nº 58/2024
CONTRATADO: 08.849.206/0001-00 - DENTAL OPEN - COMERCIO DE PRODUTOS ODONTOLÓGICOS LTDA
VALOR TOTAL REGISTRADO: R$ 6.635,51
VIGÊNCIA: 29/10/2024 A 29/10/2025.

Nº DA ATA DE REGISTRO DE PREÇOS: 182/2024
PROCESSO LICITATÓRIO: PREGÃO ELETRÔNICO Nº 58/2024
CONTRATADO: 10.633.441/0001-84 - FUSAO COMERCIO DE PRODUTOS ODONTOLOGICOS LTDA - EPP
VALOR TOTAL REGISTRADO: R$ 16.286,95
VIGÊNCIA: 29/10/2024 A 29/10/2025.

Nº DA ATA DE REGISTRO DE PREÇOS: 183/2024
PROCESSO LICITATÓRIO: PREGÃO ELETRÔNICO Nº 58/2024
CONTRATADO: 72.150.550/0001-06 - JULIANO DE COSTA LTDA
VALOR TOTAL REGISTRADO: R$ 6.698,00
VIGÊNCIA: 29/10/2024 A 29/10/2025.

Nº DA ATA DE REGISTRO DE PREÇOS: 184/2024
PROCESSO LICITATÓRIO: PREGÃO ELETRÔNICO Nº 58/2024
CONTRATADO: 05.291.541/0001-30 - TY BORTHOLIN COMERCIAL LTDA
VALOR TOTAL REGISTRADO: R$ 3.139,20
VIGÊNCIA: 29/10/2024 A 29/10/2025.

Nº DA ATA DE REGISTRO DE PREÇOS: 185/2024
PROCESSO LICITATÓRIO: PREGÃO ELETRÔNICO Nº 58/2024
CONTRATADO: 10.566.711/0001-81 - DIFE DISTRIBUIDORA DE MEDICAMENTOS LTDA
VALOR TOTAL REGISTRADO: R$ 3.180,00
VIGÊNCIA: 29/10/2024 A 29/10/2025.

Nº DA ATA DE REGISTRO DE PREÇOS: 186/2024
PROCESSO LICITATÓRIO: PREGÃO ELETRÔNICO Nº 58/2024
CONTRATADO: 02.228.938/0001-99 - D-X INDUSTRIA, COMERCIO, IMPORTACAO E EXPORTACAO LTDA
VALOR TOTAL REGISTRADO: R$ 1.378,62
VIGÊNCIA: 29/10/2024 A 29/10/2025.

Nº DA ATA DE REGISTRO DE PREÇOS: 187/2024
PROCESSO LICITATÓRIO: PREGÃO ELETRÔNICO Nº 58/2024
CONTRATADO: 43.388.441/0001-15 - RAVACHE COMERCIAL MEDICA E HOSPITALAR LTDA
VALOR TOTAL REGISTRADO: R$ 629,30
VIGÊNCIA: 29/10/2024 A 29/10/2025.

Nº DA ATA DE REGISTRO DE PREÇOS: 188/2024
PROCESSO LICITATÓRIO: PREGÃO ELETRÔNICO Nº 58/2024
CONTRATADO: 20.669.174/0001-59 - K2 INDUSTRIA, COMERCIO, IMPORTACAO E EXPORTACAO LTDA
VALOR TOTAL REGISTRADO: R$ 2.306,00
VIGÊNCIA: 29/10/2024 A 29/10/2025.

Nº DA ATA DE REGISTRO DE PREÇOS: 189/2024
PROCESSO LICITATÓRIO: PREGÃO ELETRÔNICO Nº 58/2024
CONTRATADO: 26.686.422/0001-56 - PIUNATURE COMERCIO DE COSMETICOS E ALIMENTOS LTDA
VALOR TOTAL REGISTRADO: R$ 330,00
VIGÊNCIA: 29/10/2024 A 29/10/2025.
REGISTRE-SE E PUBLIQUE-SE. ENTRE RIOS DO OESTE-PR, EM 28/10/2024

ARI ALOISIO MALDANER
PREFEITO
*Documentos na integra disponíveis no diário oficial eletrônico no sítio: www.entreriosdooeste.pr.gov.br

Proc. Administrativo 37- 279/2024

De: CARLOS K. - AGCONT

Para: Envolvidos internos acompanhando

Data: 25/10/2024 às 09:27:36

Certifico, por fim, que foi dada publicação junto ao sítio eletrônico desta Casa de Leis na data de hoje .

–

Carlos Alberto Kasper
Analista Legislativo
Setor de Compras