Protocolo 0048973749

AVISO DE PUBLICAÇÃO

AVISO DE RETORNO DE FASE

PREGÃO ELETRÔNICO Nº. 666/2023/CEL/SUPEL/RO.

PROCESSO ELETRÔNICO N° 0036.044096/2023-13

OBJETO: Sistema de Registro de Preço (SRP) do tipo menor preço por item/menor preço por Lote, visando à futura e eventual aquisição de Material de Consumo (Material de Consumo: Copos/Tampas; Bobinas/Etiquetas e Ribbon) por um Período de 12 (doze) meses. . A Superintendência Estadual de Licitações – SUPEL, através da Pregoeira nomeada na Portaria nº 36/2024/SUPEL-CI, publicada no DOE de 15/04/2024, torna público aos interessados e em especial às empresas participantes, que está previsto o **RETORNO À FASE DE JULGAMENTO VISANDO A CONVOCAÇÃO DE LICITANTES REMANESCENTES PARA O ITEM: 13** do certame em epígrafe. Ficando a sessão **AGENDADA** para o dia **27/05/2024 às 12h:00min (HORÁRIO DE BRASILIA)**. Endereço Eletrônico: www.comprasnet.gov.br. DISPONIBILIDADE DO EDITAL: Consulta e retirada das 07h:30min. às 13h:30min. (horário de Rondônia), de segunda a sexta-feira, na Sede da SUPEL, ou, gratuitamente no endereço eletrônico https://rondonia.ro.gov.br/supel/. Outras informações através do telefone: (0XX) 69.3212-9243. **Publique-se.**

Porto Velho (RO), 21 de maio de 2024.

BRUNA GONÇALVES APOLINÁRIO

Pregoeira – CEL/SUPEL

Protocolo 0048997096

Portaria nº 50 de 22 de maio de 2024

Designa servidores para atuarem como Agentes de Contratação, bem como a equipe de apoio para auxílio destes em consonância com as disposições contidas na Lei Federal n.º 14.133, de 01 de abril de 2021, bem como Decreto Estadual n.º 28.874, de 25 de janeiro de 2024, no âmbito da Superintendência Estadual de Compras e Licitações - SUPEL/RO, e revoga a Portaria nº 28 de 15 de março de 2024.

O **SUPERINTENDENTE DE COMPRAS E LICITAÇÕES DO ESTADO DE RONDÔNIA**, no uso das atribuições legais e regimentais previstas nos termos do art. 5º, inciso V, do Decreto nº 27.948, de 01 de março de 2023 e do art. 43 da Lei Complementar n. 965, de 20 de dezembro de 2017;

CONSIDERANDO o art. 8º, §5º, da Lei Federal n.º 14.133, de 01 de abril de 2021, que versa sobre à condução da licitação na modalidade pregão, e define que o agente responsável pela condução do certame será designado pregoeiro;

CONSIDERANDO o art. 7º da Portaria nº 184 de 24 de novembro de 2022 (id. 0033911142), que institui a Comissão de Processamento e Apoio para suporte aos servidores responsáveis pela condução técnica da modalidade pregão, e estabelece suas competências, com o fito de proporcionar o processamento dos certames no âmbito da Superintendência Estadual de Compras e Licitações – SUPEL/RO;

CONSIDERANDO o art. 5º e art. 9º do Decreto n.º 28.874, de 25 de Janeiro de 2024, que regulamenta as contratações públicas no âmbito da Administração Pública direta, autárquica e fundacional do Estado de Rondônia, com fundamento na Lei Federal n.° 14.133, de 1° de abril de 2021, Lei de Licitações e Contratos Administrativos;

CONSIDERANDO os autos do Processo Administrativo id. 0043.000304/2024-56,

RESOLVE:

Art. 1º Designar os servidores abaixo para atuarem como agentes de contratação:

I -Aline Lopes Espíndola, matrícula n.º ******588;

II - Bruna Gonçalves Apolinário, matrícula n.º ******033;

III - Bruna Karen Borges Rodrigues, matrícula n.º ******695;

IV - Camila Caroline Rocha Peres, matrícula n.º ******454;

V - Eralda Etra Maria Lessa, matrícula n.º ******483;

VI - Graziela Genoveva Ketes, matrícula n.º ******300;

VII -Ivanir Barreira de Jesus, matrícula n.º ******122;

VIII - Maria do Carmo do Prado, matrícula n.º *****839;

IX - Marina Dias de Moraes Taufmann, matrícula n.º ******886;
X - Maíza Braga Barbeto, matrícula n.º *******844;
XI -Ronaldo Alves dos Santos, matrícula n.º ******353; e
XII -Valdenir Gonçalves Júnior, matrícula n.º ******985.

§ 1º Os servidores indicados entre os incisos I e XII, atuarão como Pregoeiros sempre que a modalidade pregão for indicada para o certame.

§ 2º Ficam designados à função de Pregoeiros Substitutos os servidores abaixo, que desempenharão as atividades de estilo nas ausências e impedimentos de quaisquer titulares:

I - Ayanne Carmencita Ramos Dias, matrícula n.º ******964;
II - Bianca Matias de Souza, matrícula n.º ******123;
III - Elenilson José Satimo Frelik, matrícula n.º ******495;
IV - Josélia Pagani Ferreira, matrícula n.º ******627;
V - João Vítor Rodrigues de Souza, matrícula n.º *****886;
VI - Luciana Pereira de Souza, matrícula n.º ******520;
VII - Letícia Carpina Farias Casara, matrícula n.º ******797;
VIII - Roseanna Nascimento Alves da Silva, matrícula n.º ******478;
IX - Samir Paiva do Espirito Santo, matrícula n.º ******778;
X - Sidmar Wesley Correa dos Santos, matrícula n.º ******595;
XI - Thales Silva Souza, matrícula n.º ******450; e
XII - Yago da Silva Teixeira, matrícula n.º ******800;

Art. 2º Designar os seguintes membros para compor a Equipe de Apoio:

I - Aline Cruz de Oliveira, matrícula n.º ******696;
II - Aline Karen Rodrigues Aguada, matrícula n.º ******237;
III - Ana Nayanne Batista Lemos, matrícula n.º *****137;
IV - Douglas Peixoto Noia, matrícula n.º ******650;
V - Fernanda Kathleen de Oliveira Vicente, matrícula n.º ******234;
VI - Harrisson Lucas Oliveira Rodrigues, matrícula n.º ******731;
VII - Janaina Muniz Lobato, matrícula n.º ******481;
VIII - Josineide Barbosa Leite Anastácio Ferreira, matrícula n.º ******255;
IX - Jonas Nunes Queiroz, matrícula n.º ******438;
X - Krishina Sonniê Teixeira Meneses, matrícula n.º ******433;
XI - Letícia Helen Almeida Ferreira, matrícula n.º *******088;
XII - Maria Carolina de Carvalho, matrícula n.º ******196;
XIII - Matheus Breves Chíxaro Lobo, matrícula n.º ******032;
XIV - Michael Mendes Ribeiro, matrícula n.º ******676;
XV - Marina Sampaio Mouzinho Borges, matrícula n.º ******500;
XVI - Nadiane da Costa Laia, matrícula n.º ******769;
XVII -Roberta Arroio, matrícula n.º ******701;
XVIII - Suélen Torres da Silva, matrícula n.º*******853; e
XIX - Tatiana Christine Rachid Bruxel, matrícula n.º ******493.

Parágrafo único. Os servidores indicados no § 2º, do Art. 1º, desempenharão a função de membros da Equipe de Apoio quando não estiverem representando a função de Pregoeiros Substitutos.

Art. 3º Revogar a Portaria nº 28 de 15 de março de 2024(id. SEI! 0046849690), publicada no DOE n.º 51, pp. 71-73, de 19 de março de 2024.

Art. 4º Esta portaria entra em vigor na data de sua publicação, com efeitos retroativos a 02 de maio de 2024.

Dê-se ciência. Publique-se. Cumpra-se.

Israel Evangelista da Silva

Superintendente de Compras e Licitações do Estado de Rondônia

Protocolo 0049008638

Portaria de férias nº 6851 de 22 de maio de 2024.

GOVERNO DO ESTADO DE RONDÔNIA
Superintendência Estadual de Compras e Licitações - SUPEL

INSTRUMENTO CONVOCATÓRIO

PREGÃO ELETRÔNICO Nº 90285/2024/SUPEL/RO

PARA LOTE ÚNICO, aplica-se a **AMPLA PARTICIPAÇÃO sem** a reserva de cota no total de **até 25% às empresas ME/EPP**

RESUMO DOS DADOS

ABERTURA DA SESSÃO PÚBLICA: 01/10/2024, às 09h (horário de Brasília) sítio: http://www.comprasgovernamentais.gov.br.	Limite para esclarecimentos e impugnações ao edital: 26/09/2024

OBJETO
Aquisição de subscrição de soluções de segurança avançada de endpoints (antivírus) para proteção de servidores, estações de trabalho e plataforma de correio eletrônico, com atualização de base de assinaturas e software, implantação, treinamento e suporte técnico especializado, conforme condições e exigências estabelecidas neste instrumento, por 36 (trinta e seis) meses, visando a proteção da rede lógica, dos equipamentos de TI e das informações. A contratação destina-se ao Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - IPERON e atenderá as demandas da Diretoria de Tecnologia da Informação e Comunicação - DTIC.
FUNDAMENTO: Lei federal nº 14.133, de 01 de Abril de 2021. Decreto estadual nº 28.874, 25 de Janeiro de 2024. dentre outros.
PROCESSO ADMINISTRATIVO : 0016.000487/2024-37
UASG: 925373 **ENDEREÇO ELETRÔNICO :** https://www.gov.br/compras/pt-br.
VALOR ESTIMADO DA CONTRATAÇÃO

ORÇAMENTO ANUAL	R$ 185.336,02 (cento e oitenta e cinco mil trezentos e trinta e seis reais e dois centavos)
VISTORIA	**INSTRUMENTO CONTRATUAL**

Não se aplica	Contrato

DOCUMENTOS DE HABILITAÇÃO (INFORMAR ITEM DO ANEXO I)	
Requisitos Básicos: **1.Regularidade Fiscal e trabalhista**: Conforme estabelecido no item 19.3. do Termo de Referência. **2. Habilitação jurídica**: Conforme estabelecido no item 19.4. do Termo de Referência. **3. Qualificação econômico e financeira**: Conforme estabelecido no item 19.2.2. e 19.5. do Termo de Referência. **4. Qualificação técnica:** Conforme estabelecido no item 19.2.3. e 19.6. do Termo de Referência.	**Requisitos Específicos:**

CONTRATAÇÃO EXCLUSIVA ME/EPP?	**RESERVA COTA ME/EPP?**	**PRIORIDADE ME/EPP LOCAL OU REGIONAL?**	**EXIGE AMOSTRA/DEMONSTRAÇÃO?**
não	não	não	não

CRITÉRIO DE JULGAMENTO	**MODO DE DISPUTA**	**AQUISIÇÃO**
Menor Preço por Lote	Aberto	sim

TELEFONES PARA CONTATO	**E-MAIL PARA CONTATO:**
Telefone: 69.3212-9243	atendimentosupel@gmail.com

OBSERVAÇÕES GERAIS:
1. Maiores informações e esclarecimentos sobre o certame serão prestados nas dependências da Superintendência Estadual Licitações, sito a Av. Farquar, 2986, Bairro: Pedrinhas, Complexo Rio Madeira, Ed. Pacaás Novos, 2º Andar, em Porto Velho/RO - CEP: 76.801-470.
2. Informamos que devido a atualização do sistema compras.gov.br, para fins de pesquisa da licitação deverá ser inserido o número **90000** antes do número do certame. (**ex.: 90001/2024)**

SUMÁRIO

1. DO PREÂMBULO

1.1. A SUPERINTENDÊNCIA ESTADUAL DE LICITAÇÕE S, por meio da **Portaria nº 50/2024/GAB/SUPEL**, publicada no DOE na data 22 de maio de 2024, torna público que se encontra autorizada a realização da licitação na modalidade de **PREGÃO,** na forma **ELETRÔNICA, sob o nº 90285/2024/SUPEL/RO**, do tipo **MENOR PREÇO POR LOTE,** com o **Método de Disputa: ABERTO**, em conformidade com a Lei Federal nº. 14.133, de 2021 e Decreto Estadual nº 28.874/2024, a Lei Complementar nº 123/06 e Decreto Estadual nº 21.675/2017, e suas alterações, e demais legislações vigentes, tendo como interessado (a) Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - IPERON**.**

1.1.1. O instrumento convocatório e todos os elementos integrantes encontram-se disponíveis, para conhecimento e retirada, no endereço eletrônico: https://www.gov.br/compras/pt-br

1.1.2. A sessão inaugural deste PREGÃO ELETRÔNICO dar-se-á por meio do sistema eletrônico, na data e horário estabelecidos.

1.1.3. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a abertura do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário e locais estabelecidos no preâmbulo deste Edital, desde que não haja comunicação do(a) Pregoeiro(a) em contrário.

1.1.4. Os horários mencionados neste Edital de Licitação referem-se ao horário oficial de Brasília/DF.

2. DO OBJETO

2.1. O objeto da presente licitação é a aquisição de subscrição de soluções de segurança avançada de endpoints (antivírus) para proteção de servidores, estações de trabalho e plataforma de correio eletrônico, com atualização de base de assinaturas e software, implantação, treinamento e suporte técnico especializado, conforme condições e exigências estabelecidas neste instrumento, por 36 (trinta e seis) meses, visando a proteção da rede lógica, dos equipamentos de TI e das informações, conforme condições, quantidades e exigências estabelecidas no Termo de Referência Anexo I.

2.2. Em caso de divergência existente entre as especificações do objeto descritas no sistema eletrônico – Portal de Compras do Governo Federal, e as especificações constantes no ANEXO I deste Edital – Termo de Referência, prevalecerão as últimas.

2.3. Das especificações técnicas/quantidades do objeto: Ficam aquelas estabelecidas no item 3.2 e seus subitens do Anexo I – Termo de Referência , as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

2.4. Da entrega/recebimento: Ficam aquelas estabelecidas no item 7. e subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

2.5. Da garantia do objeto: Ficam aquelas estabelecidas no item 10. e seus subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

2.6. Da fiscalização e acompanhamento do recebimento do objeto: Ficam aquelas estabelecidas no item 11.12 a 11.13.10. e 28. e seus subitens do Anexo I – Termo de Referência , as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

2.7. Da obrigação da contratada: Ficam aquelas estabelecidas no item 20.1. e subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

2.8. Da obrigação da contratante: Ficam aquelas estabelecidas no item 20.2. e subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

2.9. Do pagamento: Ficam aquelas estabelecidas no item 21. e subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

2.10. Das condições contratuais: Ficam aquelas estabelecidas no item 23. e seus subitens do Anexo I – Termo de Referência , as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

2.11. Do reajuste e supressão contratual: Ficam aquelas estabelecidas no item 25. e seus subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

2.12. Dos critérios de sustentabilidade: Ficam aquelas estabelecidas no item 31. e subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

3. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

3.1. De acordo com o Art. 164, da Lei nº 14.133, de 2021 e Decreto Estadual nº 28.874 de 2024, qualquer pessoa é parte legítima para impugnar edital de licitação por irregularidade na aplicação desta Lei ou para solicitar esclarecimento sobre os seus termos, devendo protocolar o pedido até 3 (três) dias úteis antes da data de abertura do certame, observado o seguinte procedimento:

3.1.1. Envio exclusivo para o endereço eletrônico, via e-mail**:** atendimentosupel@gmail.com;

3.1.2. Ao transmitir o e-mail, o mesmo deverá ter confirmado o recebimento, pelo mesmo meio de envio recebido, pelo Núcleo de Atendimento, para não tornar sem efeito, pelo telefone **(069) 3212-9243** ou ainda, protocolar o original junto a Sede desta Superintendência, no horário das 07h30min. às 13h30min (horário local), de segunda-feira a sexta-feira, situada na Av. Farquar, 2986 - Bairro: Pedrinhas Complemento: Complexo Rio Madeira, Ed. Pacaás Novos - 2º Andar, em Porto Velho/RO - CEP: 76.801-470;

3.1.3. Mencionar o número do Pregão, o ano e o número do processo licitatório.

3.2. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame, de forma que a concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada nos autos do processo de licitação.

3.3. A decisão do(a) Pregoeiro(a) quanto a impugnação será informada preferencialmente via e-mail (aquele informado na impugnação), e através do campo próprio do Sistema Eletrônico do site

Compras.gov.br, sendo necessariamente 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, ficando o licitante obrigado a acessá-lo para obtenção das informações prestadas pelo(a) Pregoeiro(a), na forma do Art. 164, parágrafo único.

3.4. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

4. DAS CONDIÇÕES DE PARTICIPAÇÃO

4.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Portal de Compras do Governo Federal, por meio de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

4.2. É de responsabilidade do cadastrado conferir a exatidão dos seus dados 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, inobservância que poderá ensejar desclassificação no momento da habilitação.

4.3. Não poderão disputar esta licitação, direta ou indiretamente:

4.3.1. Aquele que não atenda às condições deste Edital e seu(s) anexo(s);

4.3.2. Pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de penalidade que lhe foi imposta de:

4.3.2.1. Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do Estado de Rondônia, nos termos do art. 156, III, § 4º, da Lei n. 14.133/2021;

4.3.2.2. Declarados inidôneos para licitar ou contratar com a Administração Pública, na forma do art. 156, IV, § 5º, da Lei n. 14.133/2021;

4.3.3. Estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa e judicialmente;

4.3.4. Aquele que se enquadre no disposto do art. 14, da Lei n. 14.133, de 2021;

4.3.5. Agente público de órgão ou entidade licitante ou contratante, conforme §§ 1º e 2º do art. 9º da Lei nº 14.133, de 2021.

4.3.6. Pessoas jurídicas reunidas em consórcio observar o art. 15 da Lei n. 14.133, de 2021 e disposição constante no **item 33.** do Anexo I - Termo de Referência.

4.3.7 Da subcontratação: Ficam aquelas estabelecidas no **item 30.** e subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

5. DO BENEFÍCIO ÀS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

5.1. Na forma do Art. 4º, da Lei Federal nº 14.133, de 2021, aplicam-se às licitações e contratos disciplinados por esta Lei as disposições constantes dos arts. 42 a 49 da Lei Complementar nº 123, de 14 de dezembro de 2006, devendo atentar às regras estabelecidas no regramento específico citado.

5.2. Para obtenção de benefícios a que se refere este item, a licitante deverá apresentar:

5.2.1. Declaração, caso se enquadre, 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;

5.2.2. Declaração de que no ano-calendário de realização da licitação ainda não tenha celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, na forma do Art. 4º, § 2º, da Lei nº 14.133, de 2021.

5.3. A falsidade da declaração sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, neste Edital e em normas correlatas.

5.4 Nos itens/lotes destinados à exclusiva participação de Microempresas e Empresas de Pequeno Porte e equiparadas aplica-se o Decreto Estadual nº 21.675/2017, no que couber.

6. DA APRESENTAÇÃO DA PROPOSTA DE PREÇOS E DOS DOCUMENTOS DE HABILITAÇÃO

6.1. A participação no Pregão Eletrônico dar-se-á por meio da digitação da senha privativa do Licitante a partir da data da liberação do Edital, até o horário limite de início da Sessão Pública, horário de Brasília, devendo ser encaminhado, exclusivamente por meio do sistema, os documentos de habilitação e a proposta de preço, conforme exigências do Edital.

6.2. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos: Valor unitário e total do item ou valor global, ou percentual de desconto; descrição detalhada do objeto, contendo as informações conforme à especificação do Termo de Referência.

6.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente no fornecimento dos bens.

6.4. 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.

6.5. As ofertas de propostas dos licitantes devem respeitar os preços máximos estabelecidos neste Edital.

6.6. As propostas terão validade mínima de 90 (noventa) dias, a contar da data de sua apresentação.

6.7. As propostas registradas através do preenchimento no momento do cadastro no Sistema COMPRAS.GOV.BR NÃO DEVEM CONTER NENHUMA IDENTIFICAÇÃO DA EMPRESA PROPONENTE, visando atender o princípio da impessoalidade e preservar o sigilo das propostas.

6.8. Quando da inclusão do anexo da proposta no sistema eletrônico, as empresas deverão fornecer as informações necessárias para a identificação da proposta, que somente será pública após a fase de lances.

6.9. Os licitantes poderão retirar ou substituir a proposta e os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

7. DA FORMULAÇÃO DE LANCES, CONVOCAÇÃO ME/EPP E CRITÉRIO DE DESEMPATE

7.1. 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.

7.2. O lance deverá ser ofertado pelo valor total de cada item.

7.3. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

7.4. O licitante somente poderá oferecer lance de valor inferior ou percentual de desconto superior ao último por ele ofertado e registrado pelo sistema.

7.5. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta, deverá ser de:

a) 1% (um por cento), quando o item licitado possuir valor estimado acima a R$ 1.000.000,00 (um milhão de reais);

b) 2% (dois por cento), quando o item licitado possuir valor estimado de até R$ 1.000.000,00 (um milhão de reais).

7.6. 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.

7.7. O procedimento seguirá de acordo com o modo de disputa adotado no certame.

7.7.1. Os critérios dos modos de disputa estão estabelecidos no Art. 23 e 24 da INSTRUÇÃO NORMATIVA SEGES/ME Nº 73, DE 30 DE SETEMBRO DE 2022.

7.8. Após o encerramento da etapa de lances, será verificado se há empate entre as licitantes que neste caso, por força da aplicação da exclusividade obrigatoriamente se enquadram como Microempresa – ME ou Empresa de Pequeno Porte – EPP, conforme determina a Lei Complementar n. 123/06,CONTROLADO SOMENTE PELO SISTEMA COMPRAS.GOV.BR.

7.9. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021.

7.10. 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 (a) Pregoeiro (a) poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

7.11 Nos itens/lotes destinados à exclusiva participação de Microempresas e Empresas de Pequeno Porte e equiparadas aplica-se o Decreto Estadual nº 21.675/2017, no que couber.

8. DA FASE DE NEGOCIAÇÃO E JULGAMENTO DA PROPOSTA DE PREÇOS

8.1. Encerrada a etapa de envio de lances da sessão pública, 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 4 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação.

8.2. Seguidamente será realizada a negociação e atualização dos preços por meio do CHAT MENSAGEM do sistema Compras.gov.br, devendo o (a) Pregoeiro (a)examinar a compatibilidade dos preços em relação ao estimado para contratação.

8.2.1. Serão aceitos somente preços em moeda corrente nacional (R$), com valores unitários e totais com no máximo 02 (duas) casas decimais, considerando as quantidades constantes no Anexo I – Termo de Referência. Caso seja encerrada a fase de lances, e a licitante divergir com o exigido, o (a) Pregoeiro (a), poderá convocar no chat de mensagens para atualização do referido lance e/ou realizar a atualização dos valores arredondando-os para menos automaticamente caso a licitante permaneça inerte.

8.3. O (a) Pregoeiro (a) não aceitará o item cujo preço seja superior ao estimado (valor de mercado) para a contratação.

8.3.1.O Pregoeiro, antes da aceitação do(s) item(ns), convocará a licitante melhor classificada para que, no prazo de até 2 (duas) horas, se outro prazo não for fixado, envie a proposta adequada ao último valor ofertado, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital.

8.3.1.1. Sob análise do (a) Pregoeiro (a), poderá ser covocada todas as licitantes, que estejam dentro do valor estimado para contratação, para que no prazo máximo de 02 (duas) horas, se outro prazo não for fixado, envie a proposta adequada ao último valor ofertado, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital.

8.3.2. A PROPOSTA DE PREÇOS deverá conter: o valor devidamente atualizado do lance e/ ou da negociação ofertados, com a especificação completa do objeto, contendo marca/modelo/fabricante, SOB PENA DE DESCLASSIFICAÇÃO, em caso de descumprimento das exigências.

8.4. Para fins de aceitação da proposta o (a) Pregoeiro (a) examinará a proposta ajustada quanto à adequação ao objeto e à compatibilidade do preço em relação aos valores estimados para contratação, podendo solicitar manifestação técnica e jurídica de outros setores do órgão, a fim de subsidiar sua decisão.

8.5. Quando houver indícios de inexequibilidade da proposta de preço, será oportunizado ao licitante o Princípio do Contraditório e da Ampla Defesa, para que querendo esclareça a composição do

preço da sua proposta, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do artigo 59 da Lei Federal n° 14.133/2021.

8.6. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do órgão requisitante, ou da área especializada no objeto.

8.7. A PROPOSTA DE PREÇOS, inserida no sistema de Compras.gov.br deverá estar de acordo com o item 15. do Anexo I - termo de Referência.

9. DA FASE DE HABILITAÇÃO

9.1. Os documentos previstos no Termo de Referência, 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.

9.2. Os licitantes poderão deixar de apresentar os documentos de habilitação que constem do SICAF e/ou Cadastro Geral de Fornecedores – CAGEFOR da SUPEL, assegurando aos demais licitantes o direito de acesso aos dados constantes dos sistemas.

9.2.1. Ressalvado os documentos possíveis de verificação conforme item 9.2, os licitantes deverão encaminhar, nos termos deste Edital e anexos, a documentação relacionada nos itens a seguir, para fins de habilitação:

9.3. 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.

9.4. A não observância do disposto no item anterior poderá ensejar inabilitação.

9.5 A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

9.6. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para:

9.6.1. 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

9.6.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

9.7. 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.

9.8. As Microempresas e Empresas de Pequeno Porte deverão encaminhar a documentação de habilitação, ainda que haja alguma restrição de regularidade fiscal e trabalhista, nos termos do art. 43, § 1º da LC n. 123, de 2006 e alterações.

9.8.1. Havendo alguma restrição na comprovação da regularidade fiscal, será assegurado prazo de 5 (cinco) dias úteis para sua regularização pelo licitante, prorrogável por igual período, com início no dia em que o proponente for declarado vencedor do certame.

9.8.2. A prorrogação do prazo previsto no subitem 9.8.1 poderá ser concedida, a critério da Administração Pública, quando requerida pelo licitante, mediante apresentação de justificativa.

9.9. RELATIVOS À REGULARIDADE FISCAL, SOCIAL E TRABALHISTA

a) Comprovação de inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ);

b) Comprovação de inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

c) Prova de regularidade perante a Fazenda federal;

d) Prova de regularidade Estadual e/ou municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

e) Certidão de Regularidade do FGTS, relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

f) Prova de regularidade perante a Justiça do Trabalho, mediante apresentação de Certidão de Regularidade de Débito – CNDT, para comprovar a inexistência de débitos inadimplidos perante a Justiça do Trabalho, admitida comprovação também, por meio de "certidão positiva com efeito de negativo", diante da existência de débito confesso, parcelado e em fase de adimplemento.

9.10. RELATIVOS À HABILITAÇÃO JURÍDICA

a) No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

b) Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio http://www.portaldoempreendedor.gov.br/;

c) No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

d) No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

e) No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971;

f) No caso de agricultor familiar: Declaração de Aptidão ao Pronaf – DAP ou DAP- P válida, ou, ainda, outros documentos definidos pelo Ministério do Desenvolvimento Social, conforme Decreto n° 11.802, de 28/11/2023.

g) No caso de produtor rural: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa RFB nº 2110, de 2022.

h) No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização, e se for o caso, ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

9.10.1. Os documentos acima deverão estar acompanhados da última alteração ou da consolidação respectiva.

9.11. RELATIVOS À QUALIFICAÇÃO ECONÔMICA-FINANCEIRA

a) Certidão Negativa de feitos sobre falência – Lei n°. 11.101/05, expedida pelo distribuidor da sede do licitante, expedida nos últimos **90 (noventa)** dias caso não conste o prazo de validade.

b) Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, ou o Balanço de Abertura, caso a licitante tenha sido constituída em menos de um ano, devidamente autenticado ou registrado no órgão competente, para que o(a) pregoeiro(a) possa aferir se esta possui Patrimônio Líquido (licitantes constituídos há mais de um ano) ou Capital Social (licitantes constituídos há menos de um ano), de 10 % (dez por cento) do valor estimado do item/ lote que o licitante estiver participando.

b.1) No caso do licitante classificado em mais de um item/lote, o aferimento do cumprimento da disposição acima levará em consideração a soma de todos os valores referencias;

b.2) Caso seja constatada a insuficiência de patrimônio líquido ou capital social para a

integralidade dos itens/lotes em que o licitante estiver classificado, o Pregoeiro o convocará para que decida sobre a desistência do(s) item(ns)/lote(s) até o devido enquadramento a regra acima disposta;

b.3) As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

b.4) O balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos. (Lei nº 14.133, de 2021, art. 69, §6º)

9.11.1. As regras descritas nos itens b.1 e b.2 deverão ser observadas em caso de ulterior classificação de licitante que já se consagrou classificado em outro item(ns)/lote(s).

9.12. RELATIVOS À QUALIFICAÇÃO TÉCNICA

9.12.1. Os critérios de qualificação técnica a serem atendidos pelo fornecedor serão aqueles estabelecidos no item 19.2.3. e 19.6. do Anexo I – Termo de Referência deste Edital**.**

9.13. 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.

9.13.1. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcionem 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.

9.14. DAS DECLARAÇÕES:

a) 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).

b) 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.

c) 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.

d) Declaração do cumprimento do disposto no inciso XXXIII do art. 7° da Constituição Federal.

e) Declaração, caso se enquadre, 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; (ME E EPP)

f) Declaração, caso se enquadre, de que no ano-calendário de realização da licitação ainda não tenha celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, na forma do Art. 4º, § 2º, da Lei nº 14.133, de 2021.

10. DO RECURSO

10.1. 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 após a fase de HABILITAÇÃO, declarada a empresa VENCEDORA do certame, qualquer Licitante dentro do prazo poderá manifestar em campo próprio do Sistema Eletrônico, de forma imediata sua intenção de recorrer no prazo mínimo de 10 (dez) minutos.

10.1.1. A intenção de recorrer deverá ser manifestada imediatamente, sob pena de

preclusão.

10.2. As razões do recurso deverão ser apresentadas em momento único, em campo próprio no sistema, no prazo de três dias úteis, contados a partir da data de intimação ou de lavratura da ata de habilitação ou inabilitação ou, na hipótese de adoção da inversão de fases prevista no § 1º do art. 8º, da ata de julgamento.

10.3. Os demais licitantes ficarão intimados para, se desejarem, apresentar suas contrarrazões, no prazo de três dias úteis, contado da data de intimação pessoal ou de divulgação da interposição do recurso.

10.4. Será assegurado ao licitante vista dos elementos indispensáveis à defesa de seus interesses.

10.5. 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.

10.6 . O acolhimento do recurso importará na invalidação apenas dos atos que não possam ser aproveitados.

10.7. Os recursos interpostos fora do prazo não serão conhecidos.

10.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente, nos termos do art. 168, da Lei n. 14.133, de 2021.

11. DA HOMOLOGAÇÃO

11.1. Encerradas as fases de julgamento e habilitação, e exauridos os recursos administrativos, o processo licitatório será encaminhado à autoridade superior para adjudicar o objeto e homologar o procedimento, observado o disposto no art. 71 da Lei nº 14.133, de 2021.

12. DA REVOGAÇÃO E DA ANULAÇÃO

12.1. A autoridade superior poderá revogar o procedimento licitatório de que trata esta Instrução Normativa por motivo de conveniência e oportunidade, e deverá anular por ilegalidade insanável, de ofício ou por provocação de terceiros, assegurada a prévia manifestação dos interessados.

§ 1º O motivo determinante para a revogação do processo licitatório deverá ser resultante de fato superveniente devidamente comprovado.

§ 2º Ao pronunciar a nulidade, a autoridade indicará expressamente os atos com vícios insanáveis, tornando sem efeito todos os subsequentes que deles dependam, e dará ensejo à apuração de responsabilidade de quem lhes tenha dado causa.

§ 3º Na hipótese da ilegalidade de que trata o caput ser constatada durante a execução contratual, aplica-se o disposto no art. 147 da Lei nº 14.133, de 2021.

13. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

13.1. A licitante e o contratado que incorram em infrações sujeitam-se às sanções administrativas previstas nos termos do art. 156 da Lei Federal n.º 14.133, de 2021, sem prejuízo de eventuais implicações penais nos termos do que prevê o Capítulo II-B do Título XI do Código Penal e sanções previstas no item 27. e subitens do Termo de Referência - Anexo ao edital.

13.2. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados à Administração Pública do Estado de Rondônia.

14. DA DOTAÇÃO ORÇAMENTÁRIA

14.1. Os recursos financeiros necessários para acobertar as despesas decorrentes da contratação, estão consignados no orçamento da Instituto de Previdência dos Servidores Públicos**, Unidade Gestora IPERON/RO**, conforme estabelecido no item 8. do Termo de Referência – Anexo I deste Edital.

15. DAS DISPOSIÇÕES GERAIS

15.1. Será divulgada ata da sessão pública nos sistemas eletrônicos O: https://www.comprasgovernamentais.gov.br/ e no no site https://rondonia.ro.gov.br/supel.

15.2. As disposições atinentes à fiscalização e à gestão do contrato, à entrega do objeto e às condições de pagamento deverão ser observadas no Anexo I - Termo de Referência deste Edital.

15.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.

15.4. A homologação do resultado desta licitação não implicará direito à contratação.

15.5. 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.

15.6. 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.

15.7. 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.

15.8. 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.

15.9. 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.

15.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico https://rondonia.ro.gov.br/supel/licitacoes/ https://www.comprasgovernamentais.gov.br/

15.11. Ante eventual ausência de regramento específico em Edital, deverão ser observados os inseridos no Termo de Referência, sempre pautando-se na legislação vigente.

16. DOS ANEXOS

16.1. Fazem parte deste instrumento convocatório, como se nele estivessem transcritos, os seguintes documentos:

ANEXO I - Termo de Referência (0052488109) e Minuta de Contrato anexo I;

ANEXO I.I - Estudo Técnico Preliminar (0048519972);

ANEXO II - Modelo de Minuta de Contrato (Anexo I do Termo de Referência id. (0052488109);

ANEXO III - SAMS (0049290260);

ANEXO IV - Quadro Estimativo de Preços (0050925602);

ANEXO V - Matriz de Risco (0045947969)

Porto Velho-RO, 13 de Setembro de 2024.

GRAZIELA GENOVEVA KETES

Pregoeiro (a) da/SUPEL/RO

Elaborado por:
Ana Nayanne Batista Lemos
Membro da Comissão de Processamento e Apoio - SUPEL/RO
Portaria nº 50/2024/GAB/SUPEL

Revisado por:
Tatiana Christine Rachid Bruxel
Membro da Comissão de Processamento e Apoio - SUPEL/RO
Portaria nº 50/2024/GAB-SUPEL/RO

Documento assinado eletronicamente por **Graziela Genoveva Ketes**, **Pregoeiro(a)**, em 13/09/2024, às 13:10, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0052114038** e o código CRC **AD824163**.

Referência: Caso responda este Instrumento Convocatório, indicar expressamente o Processo nº 0016.000487/2024-37

SEI nº 0052114038

GOVERNO DO ESTADO DE RONDÔNIA
Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - IPERON

TERMO DE REFERÊNCIA

1. IDENTIFICAÇÃO

Unidade Orçamentária: Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - Iperon

Departamento: Diretoria de Administração e Finanças - DAF

2. DA INTRODUÇÃO E BASE LEGAL

2.1. Este termo visa assegurar os melhores resultados possíveis para a referida contratação, sem frustrar o caráter competitivo da sua execução, atendendo e resguardando os interesses da Administração Pública.

2.2. A Administração Pública obedecerá, dentre outros, aos princípios da legalidade, finalidade, motivação, razoabilidade, proporcionalidade, moralidade, ampla defesa, contraditório, segurança jurídica, interesse público e eficiência.

2.3. Em observância ao disposto na Lei, elaboramos o presente Termo de Referência aplicando-se as disposições do Decreto Estadual nº 28.874/24, o qual regulamenta as contratações públicas no âmbito da Administração Pública direta, autárquica e fundacional do Estado de Rondônia, com fundamento na Lei Federal nº 14.133/21.

3. DO OBJETO E OBJETIVO

3.1. **Do Objeto**

3.1.1. Aquisição de subscrição de soluções de segurança avançada de endpoints (antivírus) para proteção de servidores, estações de trabalho e plataforma de correio eletrônico, com atualização de base de assinaturas e software, implantação, treinamento e suporte técnico especializado, conforme condições e exigências estabelecidas neste instrumento, por 36 (trinta e seis) meses, visando a proteção da rede lógica, dos equipamentos de TI e das informações. A contratação destina-se ao Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - Iperon e atenderá as demandas da Diretoria de Tecnologia da Informação e Comunicação - DTIC.

3.2. **Das Especificações Técnicas**

3.3.

LOTE 01				
ITEM	**ESPECIFICAÇÕES**	**CATSERV**	**MÉTRICA**	**QUANTIDADE**
01	Aquisição de subscrição de Proteção de Endpoints (Antivírus) com implementação, atualização e suporte técnico por **36 (trinta e seis) meses**	27502	Licença	400

02	**Serviço de treinamento** da solução de segurança avançada de endpoints (Antivírus) especificada no Item 1, que atenda uma turma com até 03 (três) alunos, incluindo 16 (dezesseis) horas de serviços de instações dos módulos novos.	20052	Turma	01

3.4. **Do Objetivo**

3.4.1. A presente contratação tem como objetivo, promover a segurança, proteção e automação do monitoramento da rede de Unidades do Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - Iperon.

4. JUSTIFICATIVA PARA CONTRATAÇÃO

A aquisição da subscrição de Soluções de Segurança Avançada de Endpoints (Antivírus) é indispensável para prover segurança e proteção dos servidores e equipamentos de informática do Iperon, de forma a minimizar e coibir a infecção dos serviços informativos por programas maliciosos, prejudicando a prestação de serviços à população do Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - Iperon.

Atualmente o Instituto utiliza a Solução de Antivírus Kasperky, cuja garantia de atualização está prevista para expirar em 07 (sete) de agosto de 2024, momento em que as atuais licenças não mais permitirão atualizações de novas versões da solução e das bases de dados (lista de vírus e vacinas), o que pode resultar em vulnerabilidades na rede corporativo, assim como a possibilidade de entrada de malwares, como vírus e worms, capazes de comprometer a integridade e disponibilidade do dispositivos computacionais.

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 negativamente a eficiência da gestão do ambiente de trabalho e a manutenção da qualidade dos serviços prestados, é imprescindível preservar a integridade, confidencialidade e disponibilidade das informações custodiadas neste instituto, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados, acidentais ou intencionais.

Adicionalmente, a renovação do software de antivírus é essencial para viabilizar proteção adequada e atualizada no ambiente computacional das organizações (computadores e servidores da rede), de modo a preservar os ativos corporativo (hardware, software e dados), garantindo a integridade, confidencialidade e segurança das informações institucionais contra as ações de programas maléficos que ponham em risco a segurança e a continuidade das atividades das organizações.

Nos últimos anos, a Solução Corporativa de Antivírus tem desempenhado um papel fundamental na integridade e disponibilidade da segurança da informação do ambiente computacional do Instituto, protegendo a rede corporativa de ataques de malwares originados da Internet e de dispositivos infectados, tal como pendrives.

Os ataques cibernéticos estão cada vez mais sofisticados, adotando várias formas para obter dados sigilosos das instituições, tanto informações dos usuários, quanto 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 as causou.

Nesse contexto, é crucial uma solução específica para garantir a proteção adequada e atualizada no ambiente computacional do Instituto. Ademais, é essencial que a empresa contratada forneça treinamento, com repasse tecnológico para a Equipe de Tecnologia da Informação do Iperon, objetivando o repasse do conhecimento com relação a implantação, utilização e suporte da ferramenta, de modo a utilização do serviço com eficiência.

Em resumo, a aquisição desta solução de segurança avançada visa garantir a integridade, confidencialidade e segurança do ambiente computacional do Instituto, fortalecendo a imagem

institucional e fomentando um ambiente de trabalho colaborativo. Todos esses aspectos estão intrinsecamente alinhados com o interesse público, contribuindo para tornar a organização mais eficaz.

5. CLASSIFICAÇÃO DOS OBJETOS

5.1. Os bens objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.

5.2. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme artigo 20 da Lei nº 14.133/2021 e Decreto Estadual nº 28.874, de 25 de janeiro de 2024, dado que os padrões de desempenho e qualidade são objetivamente definidos, por meio de especificações usuais de mercado.

> Art. 181. Os bens de consumo adquiridos para suprir as demandas das estruturas da Administração Pública deverão ser de qualidade comum, não superior à necessária para cumprir as finalidades às quais se destinam, vedada a aquisição de bem de luxo.
>
> § 1° Considera-se bem de luxo aquele identificável como bens cuja aquisição somente se justifica pela ostentação, opulência, forte apelo estético ou requinte, e que os padrões de qualidade elevados não se justifiquem pela necessidade que dá origem à contratação.

5.3. A aquisição/contratação de bens e serviços comuns, poderá ser adotada a licitação na modalidade pregão, uma vez que consideram-se que os bens e serviços comuns, para os fins de efeitos deste artigo, aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado ou seja, o serviço É COMUM, pois é possível estabelecer, por intermédio de especificações utilizadas no mercado, padrões de qualidade e desempenho peculiares ao objeto, de modo que é possível a decisão entre os serviços ofertados pelos participantes com base no menor preço.

6. DESCRIÇÃO DOS REQUISITOS NECESSÁRIOS DA CONTRATAÇÃO/ DESCRIÇÃO DA SOLUÇÃO - (ART. 6°, DA LF 14.133/21)

6.1. **Requisitos de Negócio:**

6.1.1. Os requisitos de negócio são aqueles que independem de características tecnológicas e que definem as necessidades e os aspectos funcionais da Solução de Tecnologia da Informação.

6.1.2. A motivação para a aquisição e renovação da solução de software de antivírus se dá em função das licenças vigentes estar com data de expiração para Agosto de 2024. A partir desta data todos os computadores – servidores e estações de trabalho, bem como os serviços suportados por estes estarão vulneráveis, tanto a ataques internos, quanto externos.

6.1.3. A contratação em questão visa Garantir o perfeito funcionamento da infraestrutura de rede do Iperon, garantir a segurança das informações do negócio e continuidade dos serviços e manter atualizada a solução de proteção antivírus contra novas ameaças.

6.1.4. Considerando a crescente evolução das ameaças digitais – vírus, malwares e suas variantes – e as descobertas diárias de vulnerabilidades nos sistemas computacionais, as quais são amplamente exploradas por softwares maliciosos, faz-se necessária a aquisição de software especifico e que abranja as mais recentes funcionalidades no que tange a proteção contra esse tipo de ameaça. Tais ameaças podem comprometer em caráter definitivo e de forma irrecuperável o ambiente computacional do instituto, contaminando arquivos e sistemas, capturando dados, causando indisponibilidade e comprometendo a confiabilidade de sistemas, bem como a integridade dos dados armazenados nos computadores e servidores de rede desta Instituição.

6.1.5. De forma a promover a gestão e fomentar os aspectos de segurança da informação, a DTIC - Diretoria de Tecnologia da Informação e Comunicação , no âmbito da rede corporativa do Iperon, deve Instituir uma estrutura para a gestão de segurança da informação e comunicações.

6.2. **Requisitos Gerais:**

6.2.1. Subscrição de proteção de endpoints, com implementação e suporte técnico por **36 (Trinta e Seis) meses**, incluindo treinamento para turma de alunos.

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

6.2.3. 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.

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

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

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

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

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

6.2.9. Proteção contra ameaças sem arquivos (Fileless);

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

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

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

6.2.13. 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.

6.2.14. 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.

6.2.15. 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.

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

6.2.17. 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.

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

6.2.19. Controles de aplicativos,

6.2.20. Controle web e dispositivos

6.2.21. HIPS e Firewall

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

6.2.23. Gerenciamento de criptografia de arquivos e discos;

6.2.24. Controle adaptativo para detecção de anomalias;

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

6.2.26. 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.

6.2.27. A solução proposta deve ter bancos de dados de reputação locais e globais.

6.2.28. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.

6.2.29. A solução proposta deve incluir um módulo capaz, no mínimo, de:

6.2.30. Bloqueio de aplicativos com base em sua categorização.

6.2.31. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.

6.2.32. A adição de sub-redes e a modificação de permissões de atividade.

6.2.33. 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.

6.2.34. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.

6.2.35. 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.

6.2.36. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:

6.2.37. Modo silencioso;

6.2.38. Discos rígidos e dispositivos removíveis;

6.2.39. De todos as contas de usuários do dispositivo.

6.2.40. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:

6.2.41. Exclusão imediata de dados;

6.2.42. Exclusão de dados adiada.

6.2.43. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:

6.2.44. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;

6.2.45. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.

6.2.46. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.

6.2.47. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.

6.2.48. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.

6.2.49. 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.

6.2.50. 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.

6.2.51. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.

6.2.52. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.

6.2.53. 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;

6.2.54. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;

6.2.55. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.

6.2.56. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.

6.2.57. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.

6.2.58. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.

6.2.59. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.

6.2.60. 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.

6.2.61. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.

6.2.62. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.

6.2.63. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.

6.2.64. 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.

6.2.65. A solução proposta deve ter categoria de detecção para bloquear banners de sites.

6.2.66. 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;

6.2.67. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.

6.2.68. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.

6.2.69. 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.

6.2.70. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

6.2.71. 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.

6.2.72. 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.

6.2.73. 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.

6.2.74. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.

6.2.75. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.

6.2.76. A solução proposta deve suportar o controle de scripts executados em PowerShell.

6.2.77. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.

6.2.78. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.

6.2.79. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.

6.2.80. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.

6.2.81. 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.

6.2.82. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.

6.2.83. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:

6.2.84. Filtro de anexos.

6.2.85. Verificação de mensagens de email ao receber, ler e enviar.

6.2.86. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.

6.2.87. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;

6.2.88. 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.);

6.2.89. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registro do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.

6.2.90. 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.

6.2.91. A solução proposta deve incluir suporte ao protocolo IPv6.

6.2.92. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.

6.2.93. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

6.2.94. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.

6.2.95. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

6.2.96. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.

6.2.97. 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.

6.2.98. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.

6.2.99. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram

através de notificação por e-mail.

6.2.100. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.

6.2.101. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.

6.2.102. 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.

6.2.103. 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.

6.2.104. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.

6.2.105. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.

6.2.106. 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.

6.2.107. A solução proposta deve suportar endereços IPv6.

6.2.108. A solução proposta deve suportar verificação em duas etapas (autenticação).

6.2.109. 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.

6.2.110. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.

6.2.111. 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.

6.2.112. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.

6.2.113. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.

6.2.114. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.

6.2.115. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.

6.2.116. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.

6.2.117. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.

6.2.118. 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.

6.2.119. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.

6.2.120. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.

6.2.121. 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.

6.2.122. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.

6.2.123. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.

6.2.124. A solução proposta deve ter a capacidade de excluir atualizações baixadas.

6.2.125. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.

6.2.126. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.

6.2.127. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.

6.2.128. 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.

6.2.129. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.

6.2.130. 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.

6.2.131. 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.

6.2.132. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.

6.2.133. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:

6.2.134. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.

6.2.135. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

6.2.136. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.

6.2.137. A solução proposta deve gerar relatorios de vulnerabilidades encontradas nos dispositivos com sensor de endpoint instalado.

6.3. **Do Módulo de proteção de endpoint:**

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

6.3.2. Windows 7

6.3.3. Windows 8

6.3.4. Windows 8.1

6.3.5. Windows 10

6.3.6. Windows 11

6.3.7. Windows Small Business Server 2011

6.3.8. Windows MultiPoint Server 2011

6.3.9. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

6.3.10. Servidores de terminal Microsoft

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

6.3.12. Sistemas operacionais Linux de 32 bits:
6.3.13. CentOS 6.7 e posterior
6.3.14. Debian GNU/Linux 11.0 e posterior
6.3.15. Debian GNU/Linux 12.0 e posterior
6.3.16. Red Hat Enterprise Linux 6.7 e posterior
6.3.17. Amazon Linux 2.
6.3.18. CentOS 6.7 e mais tarde
6.3.19. CentOS 7.2 e posterior.
6.3.20. CentOS Stream 8.
6.3.21. CentOS Stream 9.
6.3.22. Debian GNU/Linux 11.0 e posterior.
6.3.23. Debian GNU/Linux 12.0 e posterior.
6.3.24. Linux Mint 20.3 e superior.
6.3.25. Linux Mint 21.1 e posterior.
6.3.26. openSUSE Leap 15.0 e posterior.
6.3.27. Oracle Linux 7.3 e posterior.
6.3.28. Oracle Linux 8.0 e posterior.
6.3.29. Oracle Linux 9.0 e posterior.
6.3.30. Red Hat Enterprise Linux 6.7 e posterior
6.3.31. Red Hat Enterprise Linux 7.2 e posterior.
6.3.32. Red Hat Enterprise Linux 8.0 e posterior.
6.3.33. Red Hat Enterprise Linux 9.0 e posterior.
6.3.34. Rocky Linux 8.5 e posterior.
6.3.35. Rocky Linux 9.1.
6.3.36. SUSE Linux Enterprise Server 12.5 ou posterior.
6.3.37. SUSE Linux Enterprise Server 15 ou posterior.
6.3.38. Ubuntu 20.04 LTS.
6.3.39. Ubuntu 22.04 LTS.
6.3.40. CentOS Stream 9.
6.3.41. SUSE Linux Enterprise Server 15.
6.3.42. Ubuntu 22.04 LTS.
6.3.43. macOS 12 – 14
6.3.44. Ferramentas de virtualização MAC OS:
6.3.45. Parallels Desktop 16 para Mac Business Edition
6.3.46. VMware Fusion 11.5 Profissional
6.3.47. VMware Fusion 12 Profissional
6.3.48. A solução proposta deverá suportar as seguintes plataformas virtuais:
6.3.49. VMware Workstation 17.0.2 Pro
6.3.50. VMware ESXi 8.0 Update 2

6.3.51. Microsoft Hyper-V Server 2019

6.3.52. Citrix Virtual Apps e Desktop 7 2308

6.3.53. Citrix Provisioning 2308

6.3.54. Citrix Hypervisor 8.2 Update 1

6.4. **Do Módulo de Gerenciamento Avançado:**

6.4.1. A solução proposta deve suportar arquitetura cloud-native e on-premisse;

6.4.2. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:

6.4.3. Amazon Web Services;

6.4.4. Microsoft Azure;

6.4.5. A solução proposta deve incluir as seguintes opções de integração SIEM:

6.4.6. HP (Microfoco) ArcSight;

6.4.7. IBM QRadar;

6.4.8. Splunk;

6.4.9. Kaspersky KUMA;

6.4.10. 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;

6.4.11. 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;

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

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

6.4.14. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

6.4.15. 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;

6.4.16. 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;

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

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

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

6.4.20. 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:

6.4.21. Status do dispositivo;

6.4.22. Tag;

6.4.23. Diretório ativo;

6.4.24. Proprietários de dispositivos;

6.4.25. Hardware;

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

6.4.27. E-mail;

6.4.28. Registro de sistema;

6.4.29. SMS;

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

6.4.31. Atributos de rede;

6.4.32. Nome;

6.4.33. Domínio e/ou Sufixo de Domínio;

6.4.34. Endereço de IP;

6.4.35. Endereço IP para servidor de gerenciamento;

6.4.36. Localização no Active Directory;

6.4.37. Unidade organizacional;

6.4.38. Grupo;

6.4.39. Sistema operacional;

6.4.40. Número do pacote de serviço;

6.4.41. Arquitetura Virtual;

6.4.42. Registro de aplicativos;

6.4.43. Nome da Aplicação;

6.4.44. Versão do aplicativo;

6.4.45. Fabricante;

6.4.46. Tipo e versão;

6.4.47. Arquitetura;

6.4.48. 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;

6.4.49. 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;

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

6.4.51. Dispositivos Desktop/Servidores

6.4.52. Dispositivos móveis;

6.4.53. Dispositivos de rede;

6.4.54. Dispositivos virtuais;

6.4.55. Componentes OEM;

6.4.56. Periféricos de computador;

6.4.57. Dispositivos IoT conectados;

6.4.58. Telefones VoIP;

6.4.59. Repositórios de rede;

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

6.4.61. Nome da Aplicação;

6.4.62. Caminho do aplicativo;

6.4.63. Metadados do aplicativo;

6.4.64. Aplicativo Certificado digital;

6.4.65. Categorias de aplicativos predefinidas pelo fornecedor;

6.4.66. SHA256 e MD5;

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

6.4.68. Bluetooth;

6.4.69. Dispositivos móveis;

6.4.70. Modems externos;

6.4.71. CD/DVD;

6.4.72. Câmeras e scanners;

6.4.73. MTPs;

6.4.74. E a transferência de dados para dispositivos móveis;

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

6.4.76. 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;

6.4.77. 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:

6.4.78. Estruturas de domínios e grupos de trabalho do Windows;

6.4.79. Estruturas de grupos do Active Directory;

6.4.80. Conteúdo de um arquivo de texto criado manualmente pelo administrador;

6.4.81. 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.

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

6.4.83. Verificação manual;

6.4.84. Verificação no acesso;

6.4.85. Verificação por demanda;

6.4.86. Verificação de arquivos compactados

6.4.87. Verificação de arquivos individuais, pastas e unidades;

6.4.88. Bloqueio e verificação de scripts

6.4.89. Proteção contra alteração de registros;

6.4.90. Proteção contra estouro de buffer;

6.4.91. Verificação em segundo plano/inativa.

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

6.4.93. 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.

6.4.94. 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.

6.4.95. 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.

6.4.96. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.

6.4.97. 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.

6.4.98. A solução proposta deve suportar Windows Failover Cluster.

6.4.99. A solução proposta deve ter um recurso de clustering integrado.

6.4.100. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.

6.4.101. 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.

6.4.102. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.

6.4.103. 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.

6.4.104. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.

6.4.105. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.

6.4.106. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.

6.4.107. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.

6.4.108. A solução proposta deverá possuir controles para download de DLL e drivers.

6.4.109. 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.

6.4.110. 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.

6.4.111. 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).

6.4.112. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.

6.4.113. 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.

6.4.114. 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.

6.4.115. 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.

6.4.116. 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.

6.4.117. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.

6.4.118. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.

6.4.119. 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.

6.4.120. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.

6.4.121. 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.

6.4.122. 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. .

6.4.123. 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.

6.4.124. 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.

6.4.125. A solução proposta deve permitir ao administrador personalizar relatórios.

6.4.126. 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.

6.4.127. 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.

6.4.128. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.

6.4.129. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.

6.4.130. 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.

6.4.131. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.

6.4.132. 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;

6.4.133. 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.

6.4.134. A solução proposta deve suportar integração com solução APT.

6.4.135. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:

6.4.136. Windows;

6.4.137. Linux;

6.4.138. A solução proposta deverá suportar os seguintes servidores de banco de dados:

6.4.139. Microsoft SQL Server;

6.4.140. Microsoft Banco de dados SQL do Azure;

6.4.141. MySQL Standard e Enterprise;

6.4.142. MariaDB;

6.4.143. PostgreSQL;

6.4.144. MySQL;

6.4.145. MariaDB;

6.4.146. PostgreSQL;

6.4.147. A solução proposta deverá suportar as seguintes plataformas virtuais:

6.4.148. VMware vSphere 6.7 e 7.0;

6.4.149. Estação de trabalho VMware 16 Pro;

6.4.150. Servidor Microsoft Hyper-V 2012 de 64 bits;

6.4.151. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;

6.4.152. Microsoft Servidor Hyper -V 2016 de 64 bits;

6.4.153. Servidor Microsoft Hyper-V 2019 de 64 bits;

6.4.154. Servidor Microsoft Hyper-V 2022 de 64 bits;

6.4.155. Citrix XenServer 7.1 LTSR;

6.4.156. Citrix XenServer 8.x;

6.4.157. Oracle VM VirtualBox 6.x;

6.4.158. VMware vSphere 6.7, 7.0 e 8.0;

6.4.159. VMware Desktop 16 Pro e 17 Pro;

6.4.160. Servidor Microsoft Hyper-V 2012 de 64 bits;

6.4.161. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;

6.4.162. Microsoft Servidor Hyper -V 2016 de 64 bits;

6.4.163. Servidor Microsoft Hyper-V 2019 de 64 bits;

6.4.164. Servidor Microsoft Hyper-V 2022 de 64 bits;

6.4.165. Citrix XenServer 7.1 e 8.x;

6.4.166. Oracle VM VirtualBox 6.x e7.x;

6.4.167. A solução proposta deve suportar criptografia em vários níveis:

6.4.168. Criptografia completa do disco – incluindo disco do sistema;

6.4.169. Criptografia de arquivos e pastas;

6.4.170. Criptografia de mídia removível;

6.4.171. Gerenciamento de criptografia BitLocker e MacOS Filevault2;

6.4.172. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:

6.4.173. A criptografia de arquivos em unidades de computador locais;

6.4.174. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões;

6.4.175. A criação de listas criptografadas de pastas em unidades de computador locais;

6.4.176. 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:

6.4.177. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis;

6.4.178. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais;

6.4.179. 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:

6.4.180. A criptografia de todos os arquivos armazenados em unidades removíveis;

6.4.181. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis;

6.4.182. 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

6.4.183. 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.

6.4.184. 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.

6.4.185. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.

6.4.186. 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.

6.4.187. 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.

6.4.188. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.

6.4.189. 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.

6.4.190. 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.

6.4.191. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.

6.4.192. 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.

6.4.193. 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.

6.4.194. A solução proposta deve fornecer um local central para armazenamento de chaves de

criptografia e múltiplas opções de recuperação.

6.4.195. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário.

6.4.196. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.

6.4.197. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.

6.4.198. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:

6.4.199. Uso do Trusted Platform Module e configurações de senha;

6.4.200. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível;

6.4.201. 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);

6.4.202. A solução proposta deve suportar criptografia em Microsoft Surface Tablets;

6.4.203. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:

6.4.204. Instalação remota de software de terceiros;

6.4.205. Relatórios sobre software e hardware existentes;

6.4.206. Monitoramento para instalação de software não autorizado;

6.4.207. Remoção de software não autorizado;

6.4.208. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.

6.4.209. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.

6.4.210. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.

6.4.211. 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.

6.4.212. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.

6.4.213. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.

6.4.214. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.

6.4.215. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança

6.4.216. A solução proposta deve permitir ao administrador aprovar atualizações.

6.4.217. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.

6.4.218. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.

6.4.219. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.

6.4.220. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.

6.4.221. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.

6.4.222. 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).

6.4.223. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.

6.4.224. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.

6.4.225. A solução proposta deve incluir campos dedicados que contenham informações sobre 'Exploração encontrada para a vulnerabilidade'.

6.4.226. A solução proposta deve incluir campos dedicados que contenham informações sobre "Ameaça encontrada para a vulnerabilidade".

6.4.227. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.

6.4.228. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.

6.4.229. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.

6.4.230. A solução proposta deve apoiar a implantação do sistema operacional.

6.4.231. A solução proposta deve suportar Wake-on LAN e UEFI.

6.4.232. 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.

6.4.233. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.

6.4.234. 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.

6.4.235. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.

6.4.236. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.

6.4.237. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.

6.4.238. 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.

6.4.239. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.

6.4.240. 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.

6.4.241. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:

6.4.242. Inicie a instalação ao reiniciar ou desligar o computador;

6.4.243. Instale o gerador necessário todos os pré-requisitos do sistema;

6.4.244. Permitir a instalação de novas versões de aplicativos durante as atualizações;

6.4.245. Baixe atualizações para o dispositivo sem instalá-las;

6.4.246. 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.

6.4.247. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.

6.4.248. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:

6.4.249. CEF;

6.4.250. LEEF;

6.4.251. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.

6.4.252. O relatório da solução proposta deve conter informações CVE.

6.4.253. A solução proposta deve suportar instalação de aplicações e software de terceiros;

6.4.254. **Do Módulo de Gerenciamento Simplificado:**

6.4.255. A solução proposta deve suportar arquitetura cloud;

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

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

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

6.4.259. 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.

6.4.260. A solução proposta deve atender as condições apontadas no item e subintes 6.

6.4.261. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.

6.4.262. A solução proposta deve incluir informações do endpoint:

6.4.263. IP público de internet;

6.4.264. IP interno do dispositivo;

6.4.265. Versão do agente de proteção;

6.4.266. Ultima comunicação com a console, contendo data e hora;

6.4.267. Informações do sistema operacional;

6.4.268. 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.

6.4.269. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.

6.4.270. A solução proposta deve incluir treinamento em segurança cibernética.

6.5. **Do Módulo de Gerenciamento de Dispositivos Móveis:**

6.5.1. O modulo deve ser integrado a console de gerenciamento;

6.5.2. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis,

incluindo Android:

6.5.3. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)

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

6.5.5. iOS 10–17 ou iPadOS 13–17

6.5.6. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.

6.5.7. A solução proposta deve suportar dispositivos iOS supervisionados.

6.5.8. 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.

6.5.9. 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.

6.5.10. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.

6.5.11. 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).

6.5.12. 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.

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

6.5.14. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.

6.5.15. A solução proposta deve ter recursos de conteinerização para dispositivos Android.

6.5.16. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:

6.5.17. Dados em contêineres

6.5.18. Contas de e-mail corporativo

6.5.19. Configurações para conexão à rede Wi-Fi corporativa e VPN

6.5.20. Nome do ponto de acesso (APN)

6.5.21. Perfil do Android for Work

6.5.22. Recipiente KNOX

6.5.23. Chave do gerenciador de licença KNOX

6.5.24. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:

6.5.25. Todos os perfis de configuração instalados

6.5.26. Todos os perfis de provisionamento

6.5.27. O perfil iOS MDM

6.5.28. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas

6.5.29. 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 .

6.5.30. 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:

6.5.31. Critérios de verificação do dispositivo;

6.5.32. 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;

6.5.33. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.

6.5.34. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:

6.5.35. Cartões de memória e outras unidades removíveis

6.5.36. Câmera do dispositivo

6.5.37. Conexões Wi-Fi

6.5.38. Conexões Bluetooth

6.5.39. Porta de conexão infravermelha

6.5.40. Ativação do ponto de acesso Wi-Fi

6.5.41. Conexão de área de trabalho remota

6.5.42. Sincronização de área de trabalho

6.5.43. Definir configurações da caixa de correio do Exchange

6.5.44. Configurar caixa de e-mail em dispositivos iOS MDM

6.5.45. Configure contêineres Samsung KNOX.

6.5.46. Definir as configurações do perfil do Android for Work

6.5.47. Configurar e-mail/calendário/contatos

6.5.48. Defina as configurações de restrição de conteúdo de mídia.

6.5.49. Definir configurações de proxy no dispositivo móvel

6.5.50. Configurar certificados e SCEP

6.5.51. 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 .

6.5.52. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:

6.5.53. Google Play, Huawei App Gallery e Apple App Store

6.5.54. Portal de inscrição móvel KNOX

6.5.55. Pacotes de instalação pré-configurados independentes

6.5.56. 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.

6.5.57. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.

6.5.58. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:

6.5.59. VMware AirWatch 9.3 ou posterior

6.5.60. MobileIron 10.0 ou posterior

6.5.61. IBM MaaS360 10.68 ou posterior

6.5.62. Microsoft Intune 1908 ou posterior

6.5.63. SOTI MobiControl 14.1.4 (1693) ou posterior

6.5.64. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.

6.5.65. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:

6.5.66. Google Play

6.5.67. Galeria de aplicativos Huawei

6.5.68. Loja de aplicativos da Apple

6.5.69. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.

6.5.70. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.

6.5.71. 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.

6.5.72. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.

6.5.73. 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.

6.5.74. 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.

6.5.75. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.

6.5.76. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.

6.5.77. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.

6.5.78. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.

6.5.79. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.

6.5.80. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.

6.5.81. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;

6.5.82. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

6.6. **Do Módulo de EDR:**

6.6.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

6.6.2. 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.

6.6.3. 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;

6.6.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;

6.6.5. Deve apresentar informações detalhadas contendo:

6.6.6. Usuário que executou a ação;

6.6.7. Informações acesso privilegiado;

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

6.6.9. A solução proposta deve suportar integração com serviço de reputação em nuvem.

6.6.10. 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.)

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

6.6.12. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;

6.6.13. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.

6.6.14. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.

6.6.15. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.

6.6.16. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.

6.6.17. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.

6.6.18. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.

6.6.19. 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.

6.6.20. 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.

6.6.21. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.

6.6.22. 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:

6.6.23. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).

6.6.24. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.

6.6.25. Informações gerais sobre a detecção, incluindo modo de detecção.

6.6.26. Alterações no registro associadas à detecção.

6.6.27. Histórico da presença de arquivos no dispositivo.

6.6.28. Ações de resposta executadas pela aplicação.

6.6.29. 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.

6.6.30. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:

6.6.31. Processo

6.6.32. Conexões de rede

6.6.33. Alterações no registro

6.6.34. Detalhes do download de objeto

6.6.35. A solução proposta deve fornecer orientação de resposta (resposta guiada).

6.6.36. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente

6.6.37. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:

6.6.38. Impedir a execução de objetos

6.6.39. Isolamento de host

6.6.40. Excluir objeto do host ou grupo de hosts

6.6.41. Encerrar um processo no dispositivo

6.6.42. Colocar um objeto em quarentena

6.6.43. Execute a verificação do sistema

6.6.44. Execução remota de programa/processo/comando

6.6.45. Iniciar a varredura IoC para um grupo de hosts.

6.7. **Requisitos de Documentação:**

6.7.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:

6.7.2. Ajuda on-line para administradores

6.7.3. Ajuda on-line para melhores práticas de implementação

6.7.4. Ajuda on-line para proteção de servidores de administração

6.7.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.

6.7.6. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

6.8. **Requisitos do Treinamento:**

6.8.1. A licitante deverá realizar treinamento da solução ofertada, com carga horária mínima de 16 (Dezesseis) horas de duração, para turma de no mínimo 3 (Três) alunos.

6.8.2. O treinamento deverá ser realizado em dias úteis, em horário de funcionamento do Iperon das 7:30 as 13:30 (Horário local)

6.8.3. O treinamento pode ser realizado de forma remota (Online).

6.8.4. Deverá ser emitido certificado de participação ao final do curso para cada participante.

6.8.5. O cronograma efetivo do treinamento será definido em conjunto com a CONTRATANTE, após a assinatura do contrato.

6.8.6. Deverá ser abordado em seu conteúdo programático, no mínimo, os seguintes temas:

6.8.7. Solução de Antivírus, Firewall;

6.8.8. Controle de Aplicativos;

6.8.9. Controle de Acesso à WEB;

6.8.10. Controle de Dispositivos (USB);

6.8.11. Gerenciamento de vulnerabilidades e correções;

6.8.12. Console de Gerenciamento Integrada.

6.9. **Requisitos Gerais para a Segurança da Contratação:**

6.9.1. Caso não seja o próprio fabricante, o licitante deverá apresentar Carta do Fabricante específica para este certame, juntamente com a proposta comercial comprovando ser revenda autorizada, certificada e habilitada para fornecer a subscrição destes softwares, bem como prestar serviços de suporte técnico especializado, realizar treinamentos, instalação e configuração.

6.9.2. O licitante deverá apresentar, juntamente com a proposta comercial, documentação de vínculo empregatício de até 2 (dois) profissionais técnicos juntamente com os respectivos certificados, sendo estes profissionais aptos a prestar o serviço de suporte técnico que for necessário.

6.9.3. O licitante vencedor desta licitação, deverá apresentar juntamente com a proposta comercial, certificação de boas práticas ITIL Foundation, de pelo menos um profissional que será responsável por ser o ponto de referência das demandas técnicas desta instituição, durante todo o período de garantia da subscrição deste software.

6.9.4. Deverá ser anexada na proposta comercial a comprovação de certificação do profissional, no produto fornecido.

7. DO LOCAL/PRAZO E CONDIÇÕES DE ENTREGA/RECEBIMENTO

7.1. **Do Local, horário e prazo de entrega**

7.2. Objeto deverá ser entregue de **FORMA INTEGRAL**, a partir da emissão da Ordem de Serviço ou instrumento, **no prazo máximo de 30 (trinta) dias**, salvo em caso devidamente justificado, sendo analisado e aceito pelo demandante.

7.3. A entrega será de forma online, através dos e-mails dtic@iperon.ro.gov.br com cópia para eqinf@iperon.ro.gov.br e eqsup@iperon.ro.gov.br.

7.4. Qualquer solicitação por parte da Contratada deverá ser tratada com a Diretoria de Tecnologia da Informação - DTIC, situado na Av. Sete de Setembro, n.º 2557 – Nossa Sra. das Graças – Porto Velho/RO, de segunda a sexta-feira, no horário das 7h30min às 13h30min. As Dúvidas quanto a entrega do objeto, deverão ser tratadas A entrega será via e-mail dtic@iperon.ro.gov.br com cópia para eqinf@iperon.ro.gov.br e eqsup@iperon.ro.gov.br.

7.5. **Do Treinamento**

7.5.1. Deve ser agendado com a Diretoria de Tecnologia e Informação - DTIC, através dos e-mail's: dtic@iperon.ro.gov.br; gabriel@iperon.ro.gov.br; e jonata@iperon.ro.gov.br.

7.6. **Das Condições de Recebimento**

7.6.1. O recebimento do (s) serviços descritos deste termo de referência, se dará da seguinte forma:

7.6.2. **Provisoriamente** no ato do inicio da execução do serviço, para posterior verificação da conformidade dos serviços com as especificações constantes neste termo de referência; no prazo máximo de até 05 (cinco) dias após a sua entrega total;

7.6.3. **Definitivamente** no prazo máximo de até 10 (dez) dias corridos, contados a partir do recebimento provisório, após verificação de sua compatibilidade com as especificações descritas no termo de referência, e sua consequente aceitação mediante emissão de Termo de Recebimento Definitivo.

7.6.4. Se após o recebimento provisório for identificada qualquer falha na execução, cuja responsabilidade seja atribuída à CONTRATADA, o prazo para a efetivação do recebimento definitivo será interrompido, recomeçando sua contagem após o saneamento das impropriedades detectadas.

7.6.5. O recebimento definitivo do objeto não exclui a responsabilidade da Contratada quanto aos vícios ocultos, ou seja, só manifestados quando da normal utilização dos produtos, nos termos do Código de Defesa do Consumidor.

7.6.6. A recusa injustificada da contratada em entregar os materiais no prazo estipulado caracteriza descumprimento total da obrigação assumida, sujeitando-o às penalidades previstas em lei.

8. DOTAÇÃO ORÇAMENTÁRIA:

Unidade Gestora (UG): 140023 - Instituto de Previdência dos Servidores Públicos - Iperon

Prog. Administrativo (PA): 09.126.1000.2064

Elemento de despesas: 33.90.40

Fonte: 1.802.0.00001;

CNPJ: 15.849.540/0001-11

9. ESTIMATIVA DO PREÇO

9.1. Conforme o Estudo Técnico Preliminar, o valor estimado para a contratação é de R$ 207.548,00 (duzentos e sete mil quinhentos e quarenta e oito reais) para um período de 36 (trinta e seis) meses.

10. DA GARANTIA OBJETO

10.1. A CONTRATADA de acordo com o disposto no art. 96 da Lei Federal nº 14.133/2021 deverá prestar garantia para assegurar o fiel cumprimento das obrigações assumidas, no percentual de 5% (cinco por cento) do valor global do contrato, no prazo improrrogável de 10 (dez) dias úteis, a contar de sua assinatura, sob pena de rescisão unilateral e aplicação da penalidade de suspensão temporária do direito de participar de licitação e impedimento de contratar com a Administração, por prazo não superior a 2 (dois) anos, em uma das seguintes modalidades: Caução em dinheiro ou títulos da dívida pública, Seguro - garantia, Fiança bancária.

10.2. No caso de garantia na modalidade de fiança bancária deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil;

10.3. Em se tratando de garantia prestada por intermédio de caução em dinheiro, esta deverá ser recolhida junto ao Banco indicado pela Administração Pública, em conta específica, a qual será devolvida atualizada monetariamente, conforme art. 100, da Lei Federal nº 14.133/2021;

10.4. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos conforme definido pelo Ministério da Fazenda;

10.5. A garantia, se prestada na forma de fiança bancária ou seguro garantia, deverá ter validade durante a vigência do contrato;

10.6. No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições;

10.7. A garantia responderá pelo inadimplemento das condições contratuais e pelas eventuais multas aplicadas, independentemente de outras cominações legais, quando for o caso;

10.8. No caso de utilização da garantia, para pagamento dos débitos da CONTRATADA, deverá ser providenciada a correspondente reposição no prazo máximo de 05 (cinco) dias úteis, a contar da data em que for notificada;

10.9. A liberação da garantia será procedida no prazo máximo de 10 (dez) dias úteis, contados do recebimento do pedido formulado por escrito pela CONTRATADA, após o cumprimento integral das obrigações pactuadas, e desde que não haja pendências para com a CONTRATANTE.

10.10. O atraso injustificado na apresentação da garantia do contrato poderá acarretar sua rescisão unilateral, sem prejuízo de outras penalidades previstas no contrato e demais cominações legais decorrentes da inexecução total do ajuste;

10.11. Alterado o valor do contrato e/ou prorrogado o prazo de vigência do contrato, fica a CONTRATADA obrigada a apresentar garantia complementar ou substituí-la, no mesmo percentual e modalidades constantes desta Seção, em até 10 (dez) dias úteis, contados da data de publicação do termo

de aditamento na Imprensa Oficial;

10.12. A garantia apresentada em desacordo com os requisitos e coberturas previstas no instrumento de contrato será devolvida à CONTRATADA, que disporá do prazo improrrogável de 10 (dez) dias úteis para a regularização da pendência.

10.13. O atraso injustificado na apresentação da garantia do contrato poderá acarretar sua rescisão unilateral, sem prejuízo de outras penalidades previstas no contrato e demais cominações legais decorrentes da inexecução total do ajuste;

10.14. Alterado o valor do contrato e/ou prorrogado o prazo de vigência do contrato, fica a CONTRATADA obrigada a apresentar garantia complementar ou substituí-la, no mesmo percentual e modalidades constantes desta Seção, em até 10 (dez) dias úteis, contados da data de publicação do termo de aditamento na Imprensa Oficial;

10.15. A garantia apresentada em desacordo com os requisitos e coberturas previstas no instrumento de contrato será devolvida à CONTRATADA, que disporá do prazo improrrogável de 10 (dez) dias úteis para a regularização da pendência.

11. MODELO DE GESTÃO DE CONTRATO

11.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei n. 14.133/21, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

11.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

11.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

11.4. A Administração poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

11.5. Após a assinatura do contrato ou instrumento equivalente, a Administração poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

11.6. A Contratada permitirá e oferecerá condições para a mais ampla e completa fiscalização, durante a vigência do contrato, fornecendo informações, propiciando o acesso à documentação pertinente e atendendo às observações e exigências apresentadas pela fiscalização.

11.7. A Contratada se obriga a permitir que a auditoria interna da Contratante e/ou auditoria externa por ela indicada tenham acesso a todos os documentos que digam respeito ao objeto deste instrumento.

11.8. A Contratante realizará avaliação da qualidade dos serviços, dos resultados concretos dos esforços sugeridos pela Contratada e dos benefícios decorrentes da política de preços por ela praticada.

11.9. A avaliação será considerada pela Contratante para aquilatar a necessidade de solicitar à Contratada que melhore a qualidade dos serviços, para decidir sobre a conveniência de renovar ou, qualquer tempo, rescindir o Contrato ou, ainda, para fornecer, quando solicitado pela Contratada, declarações sobre seu desempenho, a fim de servir de prova de capacidade técnica em licitações públicas.

11.10. Não obstante a Contratada seja a única e exclusiva responsável pela execução de todos os serviços, a Contratante reserva-se o direito de, sem que de qualquer forma restrinja a plenitude desta responsabilidade, exercer a mais ampla e completa fiscalização sobre os serviços, diretamente ou por prepostos designados, podendo propor, fundamentado em fatos, a suspensão dos serviços, total ou parcialmente, em definitivo ou temporariamente, assegurado à Contratada, o direito de ampla defesa e o contraditório.

11.11. As deficiências e irregularidades que forem constatadas serão comunicadas ao preposto pela fiscalização do contrato:

a) Verbalmente, para os casos rotineiros ou urgentes.

b) Por escrito, para as situações complexas, estipulando-se, quando pertinente, prazo certo para a correção da irregularidade. As comunicações formais serão registradas em Processo Acessório ao Principal devendo ser remetido à Contratada através de e-mail no Sistema SEI.

c) Por publicação no Diário Oficial do Estado, no caso de recusa do recebimento da notificação ou insucesso de remessa postal com Aviso de Recebimento.

11.12. **Fiscalização**

11.12.1. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei n. 14.133, de 2021, art. 117, caput c/c o art. 21 ao 28, do Decreto Estadual n.º 28.874/24).

11.13. **Fiscalização Técnica**

11.13.1. A Contratante será responsável pela gestão e fiscalização do contrato decorrente da licitação, sendo responsável por previamente atestar a execução técnica dos serviços contratados, seus níveis mínimos, sempre observando as definições deste Termo de Referência, em conformidade com a legislação e com o próprio Edital/Contrato.

11.13.2. A Comissão de Recebimentos de Materiais Permanentes e Serviços irá realizar a gestão contratual, sendo responsável por coordenar as atividades relacionadas à fiscalização técnica, administrativa e setorial, bem como dos atos preparatórios à instrução processual e ao encaminhamento da documentação pertinente à Diretoria de Administração e Finanças - DAF para formalização dos procedimentos quanto aos aspectos que envolvam a prorrogação, alteração, reequilíbrio, pagamento, elaboração de Parecer Técnico acerca da aplicação de sanções, extinção dos contratos, dentre outros.

11.13.3. O Fiscal do Contrato irá realizar a fiscalização técnica, administrativa e setorial do objeto para fins de avaliação de sua execução nos moldes contratados e, se for o caso, aferir se a quantidade, qualidade, tempo e modo da prestação dos serviços estão compatíveis com os indicadores de níveis mínimos de desempenho estipulados no ato convocatório, para efeito de pagamento conforme o resultado, interagindo diretamente com os servidores do arquivo, determinando ao preposto o que for necessário à regularização das faltas ou defeitos observados, apontar formalmente à Comissão qualquer viés continuo de desconformidade da execução do contrato à qualidade exigida.

11.13.4. Conforme Art. 23 do Decreto Estadual n.º 28.874/24, caberá ao Fiscal técnico:

I - prestar apoio técnico e operacional ao gestor do contrato com informações pertinentes às suas competências;

II - anotar no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados;

III - emitir notificações para a correção de rotinas ou de qualquer inexatidão ou irregularidade constatada, com a definição de prazo para a correção;

IV - informar ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem a sua competência, para que adote as medidas necessárias e saneadoras, se for o caso;

V - comunicar imediatamente ao gestor do contrato quaisquer ocorrências que possam inviabilizar a execução do contrato nas datas estabelecidas;

VI - fiscalizar a execução do contrato para que sejam cumpridas as condições estabelecidas, de modo a assegurar os melhores resultados para a administração, com a conferência das notas fiscais e das documentações exigidas para o pagamento e, após o ateste, que certifica o recebimento provisório, encaminhar ao gestor de contrato para ratificação;

VII - comunicar ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual;

VIII - participar da atualização do relatório de riscos durante a fase de gestão do contrato, em conjunto com o fiscal administrativo e com o setorial, sob coordenação do gestor do contrato;

IX - auxiliar o gestor do contrato com as informações necessárias, na elaboração do documento comprobatório da avaliação realizada na fiscalização do cumprimento de obrigações assumidas pelo contratado;

X - realizar o recebimento provisório do objeto do contrato, mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico;

XI - verificar se estão sendo atendidas as especificações contidas nos planos, projetos, planilhas, memoriais descritivos, especificações técnicas, projeto básico, termo de referência, assim como os prazos de execução e de conclusão, devendo solicitar ao preposto da contratada a correção de imperfeições detectadas; XII - verificar a execução do objeto contratual, proceder a sua medição e recebê-lo, pela formalização da atestação;

XIII - recusar serviço ou fornecimento irregular ou em desacordo com as condições previstas no edital de licitação, na proposta da contratada e no instrumento de contrato e seus Anexos;

XIV - averiguar se é a contratada quem executa o contrato e certificar-se de que não existe cessão ou subcontratação fora das hipóteses legais e previstas no contrato;

XV - dar ciência ao gestor, com antecedência razoável, da possibilidade de não haver a conclusão do objeto na data aprazada, com as justificativas pertinentes;

XVI - comunicar ao gestor de contratos, a necessidade de se realizar acréscimos ou supressões no objeto contratado, com vistas à economicidade e à eficiência na execução contratual;

XVII - confrontar os preços e quantidades constantes da nota fiscal com os estabelecidos no contrato;

XVIII - emitir relatórios circunstanciados e conclusivos quanto à adequação dos serviços prestados de forma a demonstrar a vantajosidade técnica da manutenção da avença, documento condicionante à prorrogação do contrato.

11.13.5. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração.

11.13.6. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das falhas ou dos defeitos observados (Lei n. 14.133, de 2021, de art. 117, §1).

11.13.7. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para correção.

11.13.8. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

11.13.9. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto n. 11.246, de 2022, art. 22, V);

11.13.10. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual.

11.14. **Fiscalização Administrativa**

11.14.1. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

11.14.2. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que toma as providências cabíveis, quando ultrapassar a sua competência.

11.14.3. No processamento do pagamento, a Diretoria de Administração e Finanças - DAF, rejeitará os serviços que não se demonstrarem em consonância com os ditames legais e contratuais, devolvendo os para regularização e justificativas e glosando as parcelas irregulares apontadas pela Comissão, sem prejuízo da apuração de responsabilidade, caso se identifique dano ao erário.

11.14.4. Conforme art. 24 do Decreto Estadual n.º 28.874/24, caberá ao Fiscal administrativo:

11.14.5. Caberá ao fiscal administrativo do contrato e, nos seus afastamentos e seus impedimentos legais, ao seu substituto, em especial:

I - prestar apoio técnico e operacional ao gestor do contrato, com a realização das tarefas relacionadas ao controle dos prazos relacionados ao contrato e à formalização de apostilamentos e de termos aditivos, ao acompanhamento do empenho e do pagamento e ao acompanhamento de garantias e glosas;

II - certificar-se de que a contratada mantém, durante toda execução do contrato, as condições de habilitação e qualificação exigidas na licitação e/ou na contratação, solicitando os documentos necessários a esta constatação, com especial atenção para a regularidade trabalhista e previdenciária nos casos de obras e serviços com dedicação exclusiva (ou predominante) de mão de obra;

III - examinar a regularidade no recolhimento das contribuições fiscais, trabalhistas e previdenciárias;

IV - atuar tempestivamente na solução de eventuais problemas relacionados ao descumprimento das obrigações contratuais e reportar ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência;

V - participar da atualização do relatório de riscos durante a fase de gestão do contrato, em conjunto com o fiscal técnico e com o setorial, sob coordenação do gestor do contrato;

VI - auxiliar o gestor do contrato com as informações necessárias, na elaboração do documento comprobatório da avaliação realizada na fiscalização do cumprimento de obrigações assumidas pelo contratado;

VII - realizar o recebimento provisório do objeto do contrato, mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo;

VIII - receber e conferir a nota fiscal emitida pela contratada, atestando a efetiva realização do objeto contratado, na quantidade e qualidade contratada, para fins de pagamento das faturas correspondentes;

IX - nos casos de requerimento de revisão contratual, exigir a comprovação dos custos suportados pelo contratado através de notas fiscais, realizando análise crítica da compatibilidade dos preços com a realidade de mercado constatada junto a outras fontes;

X - receber todos os documentos necessários, contratualmente estabelecidos, para a liquidação da despesa e encaminhá-los, juntamente com a nota fiscal, para o gestor do contrato que, após conferência, remeterá a documentação para o setor responsável pelo pagamento, em tempo hábil, de modo que o pagamento seja efetuado no prazo adequado;

XI - verificar o cumprimento das normas trabalhistas por parte da contratada, inclusive no que se refere à utilização pelos empregados da empresa dos equipamentos de proteção individual exigidos pela legislação pertinente, a fim de evitar acidentes com agentes administrativos, terceiros e empregados da contratada, e, na hipótese de descumprimento, comunicar ao gestor para impulsionar o procedimento tendente à notificação da contratada para o cumprimento das normas trabalhistas e instauração de processo administrativo para aplicação de sanção administrativa;

XII - certificar-se do correto cálculo e recolhimento das obrigações trabalhistas, previdenciárias e tributárias decorrentes do contrato e, caso necessário, buscar auxílio junto os setores de contabilidade da Administração para a verificação dos cálculos apresentados, observando o disposto no art. 26 deste Decreto

11.15. **Gestor do Contrato**

11.15.1. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração.

11.15.2. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àqueles que ultrapassarem a sua competência.

11.15.3. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

11.15.4. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais

técnicos, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

11.15.5. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei n. 14.133/21, ou pelo setor com competência para tal, conforme o caso.

11.15.6. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

11.15.7. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

11.15.8. O art. 20 do Decreto Estadual n.º 28.874/24, regulamenta a função do gestor do contrato, vejamos:

> Art. 20.O gestor do contrato tem como função administrar o contrato até o término de sua vigência, desempenhando as atribuições administrativas que são inerentes ao controle individualizado de cada contrato, dentre as quais:
>
> I - instruir o processo com os documentos necessários às alterações contratuais, inclusive controlando os limites aplicáveis, e encaminhá-lo à autoridade superior para decisão;
>
> II - encaminhar o requerimento de prorrogação do prazo de execução do objeto ou da vigência do contrato à autoridade competente, instruindo o processo com manifestação conclusiva e dados que comprovem o impedimento do cumprimento do prazo pela contratada;
>
> III - controlar o prazo de vigência do contrato e de execução do objeto, assim como de suas etapas e demais prazos contratuais, recomendando, com antecedência razoável, à autoridade competente, quando for o caso, a deflagração de novo procedimento licitatório ou a prorrogação do prazo, instruindo o processo com a documentação necessária;
>
> IV - prover o fiscal do contrato das informações e dos meios necessários ao exercício das atividades de fiscalização e supervisionar as atividades relacionadas ao adimplemento do objeto contratado;
>
> V - comunicar à autoridade competente as irregularidades cometidas pela contratada, sugerindo, quando for o caso, a imposição de sanções contratuais e/ou administrativas, conforme previsão contida no edital e/ou instrumento contratual ou na legislação de regência;
>
> VI - adotar as medidas preparatórias para a aplicação de sanções e de rescisão contratual, conforme previsão contida no edital e/ou instrumento contratual ou na legislação de regência, cabendo à autoridade competente a deflagração do respectivo procedimento, a notificação da contratada para a apresentação de defesa e a decisão final;
>
> VII - promover o controle das garantias contratuais, inclusive no que se refere à juntada de comprovante de recolhimento e adequação da sua vigência e do seu valor;
>
> VIII - propor, formalmente, à autoridade competente, a liberação da garantia contratual em favor da contratada nos prazos regulamentares;
>
> IX - receber as notas fiscais atestadas pelo(s) fiscal(is) do contrato e encaminhá-las para o setor responsável pelo pagamento, após conferência dos respectivos documentos;
>
> X - manter controle atualizado dos pagamentos efetuados, em ordem cronológica;
>
> XI - documentar nos autos todos os fatos dignos de interesse administrativo;
>
> XII - registrar as informações necessárias nos sistemas informatizados utilizados pelo Poder Executivo do Estado de Rondônia, inclusive inserindo os dados referentes aos contratos administrativos no Portal Nacional de Contratações Públicas- PNCP, e mantê- los atualizados;
>
> XIII - diligenciar para o acompanhamento de situações que possam impactar nos preços contratados, como a criação, alteração ou extinção de tributos ou encargos legais ou a superveniência de disposições legais que repercutam no contrato, na forma do art. 134 da Lei Federal n° 14.133, de 2021;
>
> XIV - elaborar o relatório final de que trata a alínea “d” do inciso VI do § 3º do art. 174 da Lei Federal n° 14.133, de 2021, com as informações obtidas durante a execução do contrato;
>
> XV - tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei Federal

n° 14.133, de 2021, ou pelo agente ou pelo setor competente para tal, conforme o caso;

XVI - realizar o recebimento definitivo do objeto do contrato mediante termo detalhado que comprove o atendimento das exigências contratuais;

XVII - receber os pedidos de reajuste, repactuação e revisão de contratos, devendo emitir parecer quanto ao cabimento.

§ 1°O gestor de contratos e seu substituto deverão ser, preferencialmente, servidores ou empregados públicos efetivos pertencentes ao quadro permanente do órgão ou entidade contratante, e previamente designados pela autoridade administrativa signatária do contrato mediante ato publicado no Diário Oficial do Estado, devendo constar no processo referente à contratação a ciência expressa acerca da designação.

§ 2°É vedado à autoridade máxima do órgão ou entidade o exercício da função de gestor de contrato, salvo nos casos de desligamento extemporâneo e definitivo do gestor e de seus substitutos.

§ 3°A exceção prevista no § 2º deste artigo não poderá perdurar por mais de 60 (sessenta) dias, sob pena de responsabilização funcional.

12. MODELO DE EXECUÇÃO DO OBJETO

12.1. Após homologação da dispensa, a Contratante emitirá uma ordem de serviço para a Contratada, através de endereço eletrônico fornecido na proposta.

12.2. As licenças do software contratado, bem como suas chaves de ativação, deverão ser disponibilizadas em até 5 (cinco) dias corridos após a emissão da Ordem de Serviço, podendo ser prorrogado por igual período desde que justificado pela Contratada e autorizado pela Contratante.

12.3. Os itens deverão ser entregues via download através de link disponibilizado pela Contratada ou encaminhados por e-mail através do endereço eletrônico fornecido pela Diretoria de Tecnologia da Informação e Comunicação do Iperon.

12.4. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência, e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da CONTRATADA, sem prejuízo da aplicação de penalidades.

12.5. Para fins do período de licenciamento, a contagem do prazo iniciará a partir da aplicação da chave de ATIVAÇÃO do software, portanto, não se confunde com a data de fornecimento da licença.

13. PORTARIA DE DESIGNAÇÃO DA EQUIPE DE PLANEJAMENTO

13.1. O Estudo Técnico Preliminar foi elaborado por servidores da área técnica do Instituto, visto que não há equipe de planejamento de contratação, conforme prevê o art. 8º da IN 58/2022.

> Art. 8º O ETP será elaborado conjuntamente por servidores da área técnica e requisitante ou, quando houver, pela equipe de planejamento da contratação.

14. DECRETO ESTADUAL Nº 21.675/2017 (DA PARTICIPAÇÃO DE MICROEMPRESAS – ME E EMPRESAS DE PEQUENO PORTE – EPP)

14.1. Não haverá reserva de cota, pois o objeto da contratação é indivisível.

15. DA PROPOSTA DE PREÇOS

15.1. A proposta de preços a ser elaborada deverá estar em estrita conformidade com a relação do objeto constante no Termo de Referência.

15.2. Estar datada, assinada e identificada (nome e cargo) em sua parte final, pelo representante legal da LICITANTE, e numeradas em ordem crescente, bem como, rubricada em todas as folhas, com o carimbo padronizado do CNPJ, excetuando-se as folhas timbradas que já contenham impressas tais informações;

15.3. Conter os preços unitários em algarismos arábicos, com no máximo duas casas decimais. Preço total expresso em algarismos arábicos e por extenso, em moeda corrente Nacional;

15.4. A empresa deverá indicar em sua Proposta de Preços os Dados Bancários (Banco, Agência e Conta Corrente), onde serão creditados os respectivos pagamentos, caso seja vencedora do certame.

15.5. Nos preços propostos deverão estar computadas todas as despesas necessárias, inclusive custo de materiais, de transportes, seguros de acidentes, de instalações, depreciações, mão-de-obra, impostos, encargos sociais e trabalhistas, remunerações, etc., que constituirão a única, exclusiva e completa remuneração dos serviços;

15.6. O licitante não poderá oferecer proposta em quantitativo inferior ao previsto para contratação.

15.7. O prazo de validade da proposta não poderá ser inferior a 90 (noventa) dias.

15.8. Serão desconsideradas as propostas que deixarem de atender no todo, ou em parte, as disposições dos subitens acima;

16. CRITÉRIO DE JULGAMENTO DAS PROPOSTAS

16.1. O julgamento da Proposta de Preços dar-se-á pelo critério de MENOR PREÇO GLOBAL, observadas as especificações técnicas e os parâmetros mínimos de desempenho definidos neste Instrumento, em conformidade com a Lei Federal n. 14.133/21 e suas alterações.

16.2. Na proposta deverá constar o preço unitário e total, expressos em moeda corrente nacional, nele incluídas todas as despesas com a confecção, impostos, taxas, seguro, frete e embalagem, depreciação, emolumentos e quaisquer outros custos que, direta ou indiretamente venha ocorrer.

17. DA JUSTIFICATIVA PARA O PARCELAMENTO (OU NÃO) DA SOLUÇÃO

17.1. O parcelamento da solução é a prática padrão, devendo a licitação ser conduzida por item sempre que o objeto for divisível, desde que isso não prejudique a integralidade da solução ou a economia de escala. O objetivo é facilitar a participação de diversos licitantes.

17.2. Em regra, os serviços devem ser divididos em tantas parcelas quantas forem técnica e economicamente viáveis, visando o melhor aproveitamento dos recursos disponíveis no mercado e a ampliação da competitividade sem comprometer a economia de escala.

17.3. Contudo, conforme o inciso VIII do § 1º do art. 18 da Lei nº 14.133/2021 e o Decreto Estadual nº 28.874/24, inciso IV, do art. 42, que exigem a inclusão da justificativa para o parcelamento ou não da solução, optou-se pelo não parcelamento. Essa decisão foi tomada porque o parcelamento representaria um risco à implantação do objeto a ser contratado, que envolve a proteção da rede adotada no parque computacional do Iperon. Além disso, o sistema é configurado como único e integrado.

17.4. A padronização almejada também requer a indicação de uma marca específica, o que implica que o fornecimento do objeto deve ser feito por um único fabricante.

17.5. Assim, manter a solução sem parcelamento garante a integridade e a eficiência na implementação, além de assegurar a padronização necessária para o bom funcionamento do sistema integrado do Iperon.

18. DO MODO DE DISPUTA

18.1. Para o presente procedimento, com base no art. 42 do Decreto Estadual nº 28.874/2024, especificamente no inciso XIII, bem como no art. 56 da Lei 14.133/21, o modo de disputa será o ABERTO, conforme as disposições do inciso I do referido artigo.

19. DA HABILITAÇÃO

19.1. Na fase de habilitação das propostas, serão observadas as seguintes disposições:

19.1.1. poderá ser exigida das empresas participantes a declaração de que atendem aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei;

19.1.2. será exigida a apresentação dos documentos de habilitação apenas da empresa vencedora.

19.2. **Da justificativa das exigências dos atestados;**

19.2.1. Em atenção ao Art. 18, inciso IX da Lei Federal 14.133/2021 apresenta-se a seguintes justificativas:

19.2.2. **Em relação a Qualificiação Econômico- Financeira:** Para a aquisição de proteção de endpoints (antivírus) é **importante para garantir que a empresa tenha estabilidade financeira e capacidade de manter a qualidade e continuidade do serviço**. Em contratos de segurança cibernética, essa exigência assegura que o fornecedor possa investir em atualizações e suporte técnico, reduzindo riscos de inadimplência e protegendo a integridade dos sistemas.

19.2.2.1. A exigência de apresentação do balanço patrimonial e a comprovação de patrimônio líquido mínimo de 10% do valor estimado da contratação para a seleção de fornecedores no processo de contratação de serviços de endpoint (antivirus) é uma medida essencial para garantir a segurança e a viabilidade econômica do contrato.

19.2.2.2. O balanço patrimonial e a comprovação de um patrimônio líquido mínimo de 10% do valor da contratação são indicadores cruciais da saúde financeira do fornecedor. Estes documentos demonstram a capacidade da empresa em arcar com os custos necessários para a execução do contrato sem comprometer sua estabilidade financeira. Isso é especialmente importante em contratos de serviços tecnológicos, onde a continuidade e a qualidade dos serviços dependem da solidez financeira do prestador.

19.2.2.3. A contratação de serviços de endpoint (antivirus) envolve a implementação de soluções críticas de segurança cibernética, que são essenciais para a proteção dos ativos digitais do instituto. Garantir que o fornecedor tenha uma base financeira sólida ajuda a mitigar riscos associados à eventual inadimplência, interrupção de serviços ou incapacidade de cumprimento das obrigações contratuais.

19.2.3. **Em relação a Qualificiação Técnica**: A exigência de Declaração(ões) de Capacidade Técnica correspondente a 20% da parcela de maior relevância do objeto licitado, que neste caso é a aquisição de subscrição de proteção de endpoints (antivírus), é fundamental para garantir que a empresa tenha experiência comprovada na implementação e suporte de soluções de segurança cibernética em escala significativa. Isso assegura que o fornecedor possui a expertise necessária para fornecer um serviço eficaz e confiável, reduzindo riscos e garantindo a proteção contínua dos sistemas contra ameaças.

19.2.3.1. Essa exigência revela-se imprescindível, uma vez que envolve a prestação de fornecimentos e serviços que devem ser realizados por profissionais dotados de expertise especializada nos produtos. Estes, por sua vez, são desenvolvidos pelo FABRICANTE dos equipamentos e softwares, de modo a assegurar a validade da garantia fornecida pelo próprio FABRICANTE, além de proporcionar uma segurança acrescida para a CONTRATANTE

19.2.3.2. É **fundamental para garantir que a empresa tenha experiência comprovada na implementação e suporte de soluções de segurança cibernética em escala significativa**. Isso assegura que o fornecedor possui a expertise necessária para fornecer um serviço eficaz e confiável, reduzindo riscos e garantindo a proteção contínua dos sistemas contra ameaças.

19.2.3.3. A exigência da certificação de Parceiro Oficial Kaspersky **garante que o fornecedor possui conhecimento técnico avançado e atualizado sobre as soluções de endpoint da Kaspersky**. Isso assegura que a implementação, configuração e manutenção dos serviços sejam realizadas conforme as melhores práticas estabelecidas pela própria Kaspersky, minimizando riscos de falhas, vulnerabilidades ou incompatibilidades.

19.2.3.4. Além disso, Fornecedores certificados têm acesso direto a suporte técnico especializado da Kaspersky. Em caso de incidentes ou necessidades complexas, isso permite uma resolução mais rápida e eficaz, garantindo a continuidade do negócio e a segurança dos dados corporativos.

19.2.3.5. Cabe lembrar, que a segurança da informação é uma prioridade estratégica do Iperon. Parceiros certificados são regularmente auditados e treinados para assegurar que estão em conformidade com as normas de segurança mais rigorosas, reduzindo o risco de incidentes de segurança que poderiam comprometer a integridade dos dados e a continuidade das operações.

19.2.3.6. Por fim, a exigência de certificação demonstra o compromisso da empresa com a excelência e a qualidade dos serviços contratados. Somente parceiros que investem em certificações e treinamentos contínuos são capazes de oferecer soluções que atendam plenamente às necessidades de segurança cibernética da organização.

19.3. **REGULARIDADE FISCAL, SOCIAL E TRABALHISTA:**

19.3.1. A inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ)

19.3.2. Prova de Inscrição no Cadastro de Contribuintes Estadual ou Municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual.

19.3.3. Certidão de Regularidade de Débitos com a Fazenda Federal (da Secretaria da Receita Federal e da Procuradoria da Fazenda Nacional), admitida comprovação também, por meio de "certidão positiva com efeito de negativo", diante da existência de débito confesso, parcelado e em fase de adimplemento;

19.3.4. Certidão de Regularidade de Débitos com a Fazenda Estadual, admitida comprovação também, por meio de "certidão positiva com efeito de negativo", diante da existência de débito confesso, parcelado e em fase de adimplemento;

19.3.5. Caso o fornecedor seja considerado isento dos tributos estaduais relacionados ao objeto. O licitante deverá comprovar tal condição mediante a apresentação de declaração da Fazenda Estadual do domicílio ou sede do fornecedor, ou outra equivalente, na forma da lei.

19.3.6. Certidão de Regularidade de Débitos com a Fazenda Municipal, admitida comprovação também, por meio de "certidão positiva com efeito de negativo", diante da existência de débito confesso, parcelado e em fase de adimplemento;

19.3.7. Certidão de Regularidade do FGTS, admitida comprovação também, por meio de "certidão positiva com efeito de negativo", diante da existência de débito confesso, parcelado e em fase de adimplemento;

19.3.8. Certidão de Regularidade de Débito - CND, relativa às Contribuições Sociais fornecida pelo INSS - Instituto Nacional do Seguro Social Seguridade Social, admitida comprovação também, por meio de "certidão positiva com efeito de negativo", diante da existência de débito confesso, parcelado e em fase de adimplemento;

19.3.9. Certidão de Regularidade de Débito Trabalhista – CNDT, para comprovar a inexistência de débitos inadimplidos perante a Justiça do Trabalho, admitida comprovação também, por meio de "certidão positiva com efeito de negativo", diante da existência de débito confesso, parcelado e em fase de adimplemento.

19.3.10. Declaração de que atende o disposto no inciso XXXIII do art. 7º da Constituição Federal, ou seja, de que não possui em seu quadro, funcionários menores de dezoito anos que exerçam trabalho noturno, perigoso ou insalubre, bem como não possui nenhum funcionário menor de dezesseis anos, em qualquer trabalho, salvo na condição de aprendiz, a partir de 14 anos. Será aceita declaração eletrônica, realizada no sistema de compras utilizado pelo Estado de Rondônia.

19.4. **HABILITAÇÃO JURÍDICA:**

19.4.1. No caso de empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

19.4.2. Em se tratando de microempreendedor individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio http://www.portaldoempreendedor.gov.br/

19.4.3. No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

19.4.4. No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

19.4.5. No caso de cooperativa: ata de fundação e estatuto social em vigor, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, bem como o registro de que trata o art. 107 da Lei nº 5.764, de 1971 ;

19.4.6. No caso de agricultor familiar: Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pelo Ministério do Desenvolvimento Social, nos termos do art. 2º, §3º do Decreto n° 11.802/2023.

19.4.7. No caso de produtor rural: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa RFB nº 2110, de 2022.

19.4.8. No caso de empresa ou sociedade estrangeira em funcionamento no País: decreto de autorização, e se for o caso, ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

19.4.9. Os documentos acima deverão estar acompanhados da última alteração ou da consolidação respectiva.

19.5. **QUALIFICAÇÃO ECONÔMICO-FINANCEIRA (art. 69 da Lei 14.133/21):**

19.5.1. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais;

19.5.2. Certidão negativa de feitos sobre falência expedida pelo distribuidor da sede do licitante;

19.5.3. Capital Social ou Patrimônio Líquido de 10% (dez por cento) do valor estimado para o ITEM no qual estiver participando.

a) Caso o licitante seja classificado em mais de um item, o aferimento do cumprimento da disposição acima levará em consideração ao valor individual de cada item.

b) Caso seja constatada a insuficiência de patrimônio líquido ou capital social para a integralidade dos itens/lotes em que o licitante estiver classificado, o Pregoeiro o convocará para que decida sobre a desistência do(s) item(ns)/lote(s) até o devido enquadramento a regra acima disposta;

19.5.4. As regras descritas nos itens a) e b) deverão ser observadas em caso de ulterior classificação de licitante que já se consagrou classificado em outro item(ns)/lote(s).

19.6. **QUALIFICAÇÃO TÉCNICA:** (Base Legal: Cap. VI da Lei 14.133/2021);

19.7. A qualificação técnica será exigida em conformidade nos termos do (Art. 67 da Lei nº 14.133/21, art. 18, inciso IX, da Lei nº 14.133/21; art. 37, inciso XXI da Constituição Federal), o licitante deverá apresentar Atestado(s) ou Declaração(ões) de Capacidade Técnica, emitido por um terceiro em seu favor, pessoa física ou jurídica, de direito público ou privado, comprovando sua aptidão de desempenho de atividade condizente com o objeto da respectiva licitação;

19.8. Certificação de Parceiro Oficial Kaspersky.

19.9. Comprovação de que a empresa já executou contratos envolvendo, no mínimo, 20% (vinte) da parcela de maior relevância do objeto licitado, representando pelo ITEM 01.

19.10. Nos casos em que não for possível a divisão por porcentagem, a empresa deverá comprovar a execução integral do serviço.

19.11. Será admitida, para fins de comprovação de quantitativo mínimo do serviço, a apresentação e o somatório de diferentes atestados de serviços executados de forma concomitante, pois essa situação equivale, para fins de comprovação de capacidadetécnico-operacional, a uma única contratação.

19.12. Os atestados de capacidade técnica podem ser apresentados em nome da matriz ou da filial da empresa licitante.

19.13. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando,quando solicitado pela Administração, cópia do contrato que deu suporte à

contratação, endereço atual da contratante e local emque foram prestados os serviços, entre outros documentos.

19.14. Declaração de que o licitante tomou conhecimento de todas as informações e das condições locais para o cumprimento das obrigações objeto da licitação.

20. DAS OBRIGAÇÕES

20.1. **São obrigações da empresa Contratada:**

20.1.1. Além daquelas exigidas em Lei 14.133/21, e demais normas pertinentes, bem como as previstas neste Termo de Referência, deverá:

20.1.2. Cumprir fielmente as normas estabelecidas neste Termo de Referência, executando-os sob sua inteira e exclusiva responsabilidade, de acordo com as especificações constantes no Termo de Referência e na sua proposta.

20.1.3. Reparar, corrigir, remover ou substituir às suas expensas no todo ou em parte, o objeto em que se encontrarem vícios, defeitos ou incorreções resultantes da entrega, transporte (mesmo após de ter sido recebido definitivamente).

20.1.4. Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas e todos os tributos incidentes, sem qualquer ônus à Administração Pública, devendo efetuar os respectivos pagamentos na forma e nos prazos previstos em Lei.

20.1.5. Nos preços ofertados deverão estar incluso todos os impostos, taxas, fretes e demais custos provenientes da entrega do objeto.

20.1.6. Apresentar um preposto devidamente habilitado, com poderes para representá-lo em tudo o que se relacionar com o fornecimento do objeto da aquisição.

20.1.7. Responder pelas despesas resultantes de quaisquer ações, demandas decorrentes de danos seja por culpa sua ou qualquer de seus empregados e prepostos, obrigando-se, outrossim, por quaisquer responsabilidades decorrentes de ações judiciais de terceiros, que lhe venham a ser exigida por força de lei, ligadas ao cumprimento do presente Contrato.

20.1.8. Manter durante toda a execução do contrato compatibilidade com as obrigações assumidas em todas as condições de habilitação e qualificação exigidas na contratação.

20.1.9. Seguir em observância com o Decreto Estadual n. 28.434, de 14 de setembro de 2023 (Código de Ética) no âmbito do Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - Iperon.

20.1.10. Executar os serviços contratados, através de profissionais devidamente credenciados que atuarão na auditoria e qualificá-los em documento assinado e entregue a Contratante no início dos trabalhos;

20.1.11. Garantir que a equipe seja qualificada e capacitada para realização dos serviços contratados, através de currículo e apresentação de pelo menos duas comprovações através de diploma ou certificados.

20.1.12. Garantir à equipe que realizará os trabalhos, equipamentos de informática com configuração que permita a extração e o manuseio de dados dos sistemas.

20.1.13. Responsabilizar-se pelo pagamento das multas eventualmente aplicadas por quaisquer autoridades, Federais, Estaduais ou Municipais, em consequência de fato a ela imputável ou por atos de seu pessoal.

20.1.14. Responder por todos e quaisquer danos pessoais ou materiais causados por seus profissionais ou prepostos às dependências, instalações e equipamentos do CONTRATANTE e de terceiros, a título de culpa ou dolo devidamente comprovados, providenciando a correspondente indenização;

20.1.15. Apresentar cronograma de execução dos serviços descritos neste Termo de Referência;

20.1.16. Manter sigilo das informações colhidas;

20.1.17. Permitir acesso dos supervisores, auditores e avaliadores, que eventualmente ou permanentemente sejam designados pelo Iperon para supervisionar e acompanhar a execução dos serviços;

20.1.18. Apresentar a Declaração de cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal.

20.1.19. Apresentar a Declaração de Fato Superveniente.

20.1.20. Apresentar a Declaração de ME/EPP.

20.1.21. Apresentar a Declaração de Ciência do Edital.

20.1.22. Apresentar a Declaração Independente de Proposta.

20.1.23. Apresentar a Declaração de Acessibilidade.

20.1.24. Apresentar a Declaração de Cota de Aprendizagem.

20.1.25. Apresentar a Declaração de Não Utilização de Trabalho Degradante ou Forçado.

20.2. **São obrigações da Contratante:**

20.2.1. Proporcionar todas as facilidades indispensáveis à boa execução das obrigações contratuais;

20.2.2. Rejeitar, no todo ou em parte, os materiais entregues em desacordo com as obrigações assumidas pelo fornecedor;

20.2.3. Notificar a CONTRATADA de qualquer irregularidade encontrada no fornecimento dos materiais;

20.2.4. Solicitar a substituição dos materiais que apresentarem defeito durante a entrega e a utilização;

20.2.5. Efetuar o pagamento à contratada de acordo com as condições de preços e prazos estabelecidos neste Termo de Referência, desde que em conformidade com o exigido;

20.2.6. Atestar as faturas correspondentes, por servidores designados para esse fim;

20.2.7. Exigir o cumprimento de todos os compromissos assumidos pela CONTRATADA de acordo com este Instrumento;

20.2.8. Prestar às informações e os esclarecimentos necessários à realização do objeto do certame.

20.2.9. As futuras CONTRATADAS ficam obrigadas a aderirem ao Decreto Estadual n. 28.434, de 14 de Setembro de 2023 (Código de Ética do Iperon), de forma a adequarem as suas condutas ao conteúdo dessa disposição normativa.

21. DO PAGAMENTO (BASE LEGAL: ART. 18º, III, E ART. 141 DA LEI FEDERAL Nº 14.133/2021)

21.1. O pagamento será efetuado por ordem bancária em conta corrente da Contratada, no prazo de 15 (quinze) dias, após a habilitação para pagamento e das seguintes certidões, devidamente atualizadas, desde que a documentação da empresa esteja devidamente regularizada. Se a fatura/nota fiscal não for apresentada ou a documentação não esteja regularizada, a contagem dar-se á somente a partir da apresentação de todos os documentos necessários à liquidação, conforme disposto no art. 190 do Decreto Estadual N° 28.874, DE 25 DE JANEIRO DE 2024:

a) Comprovação de regularidade com a Fazenda Federal com Certidão Negativa, ou Certidão Positiva com efeitos de Negativa, de débitos relativos a Tributos Federais e à Dívida Ativa da União;

b) Comprovação de regularidade com a Fazenda Estadual com Certidão Negativa, ou Certidão Positiva com efeitos de Negativa, emitida pelo Estado relativo ao domicílio ou sede da Contratante, relativa a tributos estaduais;

c) Comprovação de regularidade com a Fazenda Municipal com Certidão Negativa de Débito - CND, ou Certidão Positiva com efeitos de Negativa, emitida pelo Município relativo ao domicílio ou sede da Contratante;

d) Comprovação de regularidade com a Justiça do Trabalho com Certidão Negativa de Débitos Trabalhistas - CNDT, ou Certidão Positiva com efeitos de Negativa;

e) De regularidade com o FGTS, com Certificado de Regularidade de Situação do FGTS – CRS, emitido pela Caixa Econômica Federal – CEF, comprovando a regularidade perante o Fundo de Garantia por Tempo de Serviço.

21.2. A Nota Fiscal/Fatura deverá ser preenchida, conforme a Unidade Orçamentária que emitir a Nota de Empenho respectiva, sendo:

a) **Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - Iperon** - CNPJ nº 15.849.540/0001-11

21.3. A contratada fará constar no documento fiscal, além das especificações e quantitativos do objeto, o número da NOTA DE EMPENHO, o NÚMERO DO PROCESSO, e as informações relativas aos seus dados bancários para pagamento do faturamento

21.4. Na hipótese da Nota Fiscal/Fatura apresentar erros ou dúvidas quanto à exatidão ou documentação, a Contratante poderá pagar apenas as partes não controvertidas no prazo fixado para pagamento;

21.5. O pagamento decorrente de contratações públicas será feito após a habilitação para pagamento, no prazo máximo de 15 (quinze) dias úteis, conforme art. 190 do Decreto Estadual N° 28.874, DE 25 DE JANEIRO DE 2024.

21.6. Na hipótese de haver irregularidades no cumprimento das obrigações da(s) Contratada(s), a Secretaria de Estado do Desenvolvimento Econômico reterá os créditos a que aquela teria direito, até o limite do valor dos prejuízos causados à Administração, sem prejuízo das penalidades aplicáveis previstas nos art. 162 da Lei nº 14.133 de 01 de abril de 2021.

21.7. Qualquer atraso ocorrido, por parte da Contratada, na apresentação da Nota Fiscal/Fatura, ou dos documentos exigidos como condição para pagamento, importará em prorrogação automática do prazo de vencimento da obrigação da Contratante.

21.8. Os eventuais encargos financeiros decorrentes da inobservância, pela contratada, de prazo de pagamento, serão de sua exclusiva responsabilidade.

21.9. A administração não pagará nenhum compromisso que lhe venha a ser cobrado diretamente por terceiros, seja ou não instituições financeiras, à exceção de determinações judiciais, devidamente protocoladas no órgão.

21.10. A administração efetuará retenção, na fonte, dos tributos e contribuições sobre todos os pagamentos à Contratada quando legalmente exigidos.

21.11. Ocorrendo atraso no pagamento, desde que a CONTRATADA não tenha concorrido, de alguma forma, para o atraso, fica convencionado que a taxa de compensação financeira (encargos moratórios) devida, entre a data referenciada e a correspondente ao efetivo adimplemento da obrigação, calculada com a aplicação da seguinte fórmula:

EM = I x N x VP

Onde:

EM = Encargos Moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela em atraso;

I = Índice de compensação financeira = 0,00016438, assim, apurado:

I = i/365 I = (6/100)/365 I = 0,00016438

Onde i = taxa percentual anual no valor de 6%.

22. PRAZO DE VIGÊNCIA CONTRATUAL

22.1. A vigência será de 36 (trinta e seis) meses, prorrogáveis até o limite previsto no art. 107, da Lei n. 14.133/2021 e alterações.

23. DAS CONDIÇÕES CONTRATUAIS

23.1. Formalizado o Contrato Administrativo, a Contratante convocará regularmente o interessado para assinar o termo de contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo de 10 dias úteis, ficará estabelecido em cláusulas as condições e responsabilidades entre as partes, para fornecimento do serviço, em conformidade com este instrumento e com a proposta da empresa, sob o crivo da Procuradoria Geral do Estado – PGE-RO.

23.2. O instrumento contratual será(rão) elaborado e formalizado(s) pela Procuradoria Geral do Estado - PGE/RO, conforme modelo da mesma.

23.3. Para a fiel execução do serviço, obedecerá ao disposto na Lei n 14.133/2021, e demais dispositivos legais e dispostos nas Instruções Normativas em Vigência Geral.

24. DA GARANTIA CONTRATUAL

24.1. Não haverá exigência de garantia contratual da execução, tendo em vista da menor complexidade da contratação.

25. DA RESCISÃO CONTRATUAL

25.1. O Contrato poderá ser rescindido nas hipóteses previstas no art. 137, da Lei nº 14.133/21, sem prejuízo das sanções aplicáveis.

25.2. Os casos de rescisão contratual serão formalmente motivados, assegurando-se o direito à prévia e ampla defesa.

26. DO REAJUSTE DO CONTRATO

26.1. Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas, de acordo com o art. 2º, da Lei Federal nº 10.192/01 e do Decreto Estadual n° 28.874/2024.

26.2. É nula de pleno direito qualquer estipulação de reajuste com periodicidade inferior a 1 (um) ano.

26.3. O pedido relacionado ao reequilíbrio econômico-financeiro deverá ser apresentado pela contratada no prazo máximo de 30 (trinta) dias, contados do fato gerador de seu direito.

26.4. Apresentado no prazo estipulado no caput deste artigo, os efeitos financeiros retroagirão à data-base.

26.5. Caso o pedido seja feito fora do prazo previsto, os efeitos financeiros serão contados a partir da data de recebimento do pedido pela contratante, sendo vedado ao ordenador de despesa conceder efeito retroativo aos efeitos financeiros.

26.6. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, aplicando-se o Índice Nacional de Preços ao Consumidor Amplo – IPCA/IBGE ou outro índice que venha a substituí-lo exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

26.7. Em caso de eventual reajuste contratual, a Contratada fica sujeita a atender as disposições contidas na Seção III Decreto Estadual n° 28.874/2024 e demais disposições, no que couber.

27. DA ALTERAÇÃO DOS CONTRATOS E DOS PREÇOS

27.1. O art. 124, I, da Lei Nº 14.133/21, prescreve exaustivamente as situações em que se tornam possíveis as alterações unilaterais pela Administração, que irão ocorrer quando houver modificação do projeto ou das especificações (alteração qualitativa); ou quando for necessária a modificação do valor

contratual em decorrência de acréscimo ou diminuição do objeto (alteração quantitativa). Há de se frisar que apenas nessas hipóteses é que poderão ocorrer alterações unilaterais pelo ente público, quando não houver alternativa para a fiel execução do objeto do contrato, cabe ao Poder Público, dentro dos limites da lei e de forma vinculada, realizar a alteração unilateral.

27.2. Nesse contexto, os contratos regidos por esta Lei poderão ser alterados, com as devidas justificativas, nos seguintes casos:

> I - unilateralmente pela Administração:
>
> a) quando houver modificação do projeto ou das especificações, para melhor adequação técnica a seus objetivos;
>
> b) quando for necessária a modificação do valor contratual em decorrência de acréscimo ou diminuição quantitativa de seu objeto, nos limites permitidos por esta Lei.
>
> II - por acordo entre as partes:
>
> a) quando conveniente a substituição da garantia de execução;
>
> b) quando necessária a modificação do regime de execução da obra ou do serviço, bem como do modo de fornecimento, em face de verificação técnica da inaplicabilidade dos termos contratuais originários;
>
> c) quando necessária a modificação da forma de pagamento por imposição de circunstâncias supervenientes, mantido o valor inicial atualizado e vedada a antecipação do pagamento em relação ao cronograma financeiro fixado sem a correspondente contraprestação de fornecimento de bens ou execução de obra ou serviço;
>
> d) para restabelecer o equilíbrio econômico-financeiro inicial do contrato em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução do contrato tal como pactuado, respeitada, em qualquer caso, a repartição objetiva de risco estabelecida no contrato.
>
> § 1º Se forem decorrentes de falhas de projeto, as alterações de contratos de obras e serviços de engenharia ensejarão apuração de responsabilidade do responsável técnico e adoção das providências necessárias para o ressarcimento dos danos causados à Administração;
>
> § 2º Será aplicado o disposto na alínea "d" do inciso II do caput deste artigo às contratações de obras e serviços de engenharia, quando a execução for obstada pelo atraso na conclusão de procedimentos de desapropriação, desocupação, servidão administrativa ou licenciamento ambiental, por circunstâncias alheias ao contratado;

27.3. Segundo a Lei nº 14.133/2021, em seu art. 125, tanto as alterações quantitativas como as qualitativas devem estar delimitadas pelos percentuais de até 25% do valor inicial atualizado do contrato, seja para acréscimos ou supressões, que se fizerem nas obras, nos serviços ou nas compras, e, no caso de reforma de edifício ou de equipamento, o limite para os acréscimos será de 50% (cinquenta por cento).

27.4. Por fim, outras limitações das alterações unilaterais também se encontram presentes no art. 127 da Lei nº 14.133/21, que abarca as situações em que o contrato não contemple preços unitários para obras ou serviços que necessitem de aditamento. Esses serão fixados por meio da aplicação da relação geral entre os valores da proposta e o do orçamento - base da Administração sobre os preços referenciais ou de mercado vigentes na data do aditamento, respeitados os limites estabelecidos no art. 125 desta mesma lei.

27.5. O Termo de Contrato poderá ser rescindido nas hipóteses previstas no art. 137 da Lei nº. 14.133/21, sem prejuízo das sanções aplicáveis.

27.6. Poderá a extinção contratual se dar, de acordo com o art. 138, II, da Lei n° 14.133/21:

> II - consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração;

27.7. Os casos de rescisão contratual serão formalmente motivados, assegurando-se à CONTRATADA o direito à prévia e ampla defesa.

27.8. A CONTRATADA reconhece os direitos da CONTRATANTE em caso de rescisão administrativa prevista no art. 104 da Lei nº. 14.133/21.

28. DAS PENALIDADES E SANÇÕES ADMINISTRATIVAS

28.1. Sem prejuízo das sanções cominadas no art. 156, I, II, III e IV, da Lei nº 14.133,21, pela inexecução total ou parcial do contrato, a Contratante poderá, garantida a prévia e ampla defesa, aplicar à Contratada multa de até 10% (dez por cento) sobre o valor do instrumento contratual.

28.2. Se a adjudicatária recusar-se a retirar o instrumento contratual injustificadamente ou se não apresentar situação regular na ocasião dos recebimentos, garantida a prévia e ampla defesa, aplicar à Contratada multa de até 10% (dez por cento) sobre o valor adjudicado.

28.3. A sanção prevista no inciso III do **caput** do artigo 156 da Lei 14.133/21 será aplicada ao responsável pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do **caput** do art. 155 da Lei, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos.

28.4. A multa, eventualmente imposta à Contratada, será automaticamente descontada da fatura a que fizer jus, acrescida de juros moratórios de 1% (um por cento) ao mês. Caso a contratada não tenha nenhum valor a receber do Estado, ser-lhe-á concedido o prazo de 05 (cinco) dia úteis, contados de sua intimação, para efetuar o pagamento da multa. Após esse prazo, não sendo efetuado o pagamento, serão deduzidos da garantia. Mantendo-se o insucesso, seus dados serão encaminhados ao órgão competente para que seja inscrita na dívida ativa, podendo, ainda a Contratante proceder à cobrança judicial.

28.5. As multas previstas nesta seção não eximem a adjudicatária ou contratada da reparação dos eventuais danos, perdas ou prejuízos que seu ato punível venha causar à Contratante.

28.6. De acordo com a gravidade do descumprimento, poderá ainda a licitante se sujeitar à Declaração de inidoneidade para licitar ou contratar com a Administração Pública enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que o contratado ressarcir a Contratante pelos prejuízos resultantes e depois de decorrido o prazo da sanção aplicada com base na legislação vigente.

28.7. A sanção denominada “Advertência” só terá lugar se emitida por escrito e quando se tratar de faltas leves, assim entendidas como aquelas que não acarretarem prejuízos significativos ao objeto da contratação, cabível somente até a segunda aplicação (reincidência) para a mesma infração, caso não se verifique a adequação da conduta por parte da Contratada, após o que deverão ser aplicadas sanções de grau mais significblzativo.

28.8. As sanções serão aplicadas sem prejuízo da responsabilidade civil e criminal que possa ser acionada em desfavor da Contratada, conforme infração cometida e prejuízos causados à administração ou a terceiros;

28.9. Para efeito de aplicação de multas, às infrações são atribuídas graus, com percentuais de multas conforme a tabela a seguir, que elenca apenas as principais situações previstas, não eximindo de outras equivalentes que surgirem, conforme o caso:

ITEM	DESCRIÇÃO DA INFRAÇÃO	GRAU	MULTA*
1	Permitir situação que crie a possibilidade ou cause dano físico, lesão corporal ou consequências letais, por ocorrência.	06	4% por dia
2	Usar indevidamente informações sigilosas a que teve acesso, por ocorrência.	06	4% por dia
3	Suspender ou interromper, salvo por motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento.	05	4% por dia
4	Destruir ou danificar documentos por dolo de seus agentes, por ocorrência.	05	3,2% por dia
5	Recusar-se a executar o serviço determinado pela fiscalização sem motivo justificado, por ocorrência	04	1,6% por dia
6	Executar serviço incompleto, paliativo substitutivo como por caráter permanente, ou deixar de providenciar recomposição complementar, por ocorrência.	02	0,4% por dia

7	Fornecer informação pérfida de serviço ou substituição de Cartão/equipamento/software, por ocorrência.	02	0,4% por dia
8	Manter funcionário sem qualificação para executar os serviços contratados, por empregado e por dia;	03	0,8% por dia
9	Retirar funcionários ou encarregados do serviço durante o expediente, sem a anuência prévia da CONTRATANTE, por empregado e por dia;	03	0,8% por dia

Para os itens a seguir deixar de:

ITEM	DESCRIÇÃO DA INFRAÇÃO	GRAU	MULTA*
10	Cumprir prazo previamente estabelecido para execução de serviços, por dia;	02	0,4% por dia
11	Efetuar o pagamento de seguros, encargos, fiscais e sociais, assim como quaisquer despesas diretas e/ou indiretas relacionadas à execução do contrato, por dia e por ocorrência.	05	3,2% por dia
12	Cumprir quaisquer dos itens do edital e seus anexos, mesmo que não previstos nesta tabela de multas, após reincidência formalmente notificada pela fiscalização, por ocorrência	03	0,8% por dia
13	Cumprir determinação formal ou instrução complementar da fiscalização, por ocorrência.	03	0,8% por dia
14	Iniciar os serviços nos prazos estabelecidos, observados os limites mínimos estabelecidos por este Termo de Referência, por serviço, por ocorrência.	02	0,4% por dia
15	Disponibilizar equipe de profissionais completa conforme determinado para execução do serviço, por dia	02	0,4% por dia
16	Ressarcir o órgão por eventuais danos causados por sua culpa, em veículos, equipamentos, dados etc	02	0,4% por dia
17	Realizar os serviços solicitados e de entregar os respectivos produtos, por tipo e por ocorrência	02	0,4% por dia
18	Apresentar, quando solicitado, documentação fiscal, trabalhista e previdenciária, por ocorrência;	02	0,2% por dia
19	Fornecer suporte técnico à contratante, por ocorrência e por dia.	01	0,2% por dia
20	Substituir funcionário que se conduza de modo inconveniente ou não atenda às necessidades do órgão, por funcionário e por dia.	01	0,2% por dia

*Incidente sobre o valor total do contrato**

28.10. Na aplicação da sanção prevista no inciso II do caput do art. 156 da Lei nº 14.133/2021, será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação;

28.11. A aplicação das sanções previstas nos incisos III e IV do caput do art. 156 desta Lei requererá a instauração de processo de responsabilização, a ser conduzido por comissão composta de 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o contratado para, no prazo de 15 (quinze) dias úteis, contado da data de intimação, apresentar defesa escrita e especificar as provas que pretenda produzir;

28.12. Em órgão ou entidade da Administração Pública cujo quadro funcional não seja formado de servidores estatutários, a comissão a que se refere o caput deste artigo será composta de 2 (dois) ou mais empregados públicos pertencentes aos seus quadros permanentes, preferencialmente com, no mínimo, 3 (três) anos de tempo de serviço no órgão ou entidade;

28.13. Na hipótese de deferimento de pedido de produção de novas provas ou de juntada de provas julgadas indispensáveis pela comissão, o licitante ou o contratado poderá apresentar alegações finais no prazo de 15 (quinze) dias úteis, contado da data da intimação;

28.14. Serão indeferidas pela comissão, mediante decisão fundamentada, provas ilícitas, impertinentes, desnecessárias, protelatórias ou intempestivas;

28.15. A prescrição ocorrerá em 5 (cinco) anos, contados da ciência da infração pela Administração, e será:

I - interrompida pela instauração do processo de responsabilização a que se refere o caput deste artigo;

II - suspensa pela celebração de acordo de leniência previsto na Lei nº 12.846, de 1º de agosto de 2013;

III - suspensa por decisão judicial que inviabilize a conclusão da apuração administrativa.

29. ACOMPANHAMENTO E FISCALIZAÇÃO

29.1. A entrega será acompanhada e fiscalizada por servidores do Iperon ou, na impossibilidade, por seus substitutos, todos devidamente designados para esse fim, que determinarão o que for necessário para a regularização de faltas ou defeitos, permitida a assistência de terceiros, nos termos do art. 117 da Lei n. 14.133/2021.

29.2. Em caso do produto não estar em conformidade com este Termo de Referência, a fiscalização discriminará por meio de relatório as falhas ou irregularidades encontradas, e com o recebimento do relatório, a empresa Contratada dará ciência das irregularidades apontadas e de que estará, conforme o caso, passível das sanções cabíveis, cabendo a regularização dos apontamentos, submetendo para posterior verificação da fiscalização.

29.3. A fiscalização de que trata o subitem acima não exclui nem reduz a responsabilidade da Contratada pelos danos causados diretamente à Iperon ou a terceiros, decorrentes de sua culpa ou dolo na execução do futuro instrumento contratual, conforme Art. 120 da Lei n. 14.133/2021.

30. SUBCONTRATAÇÃO

30.1. Fica vedada a subcontratação nos termos do § 2º, art. 122 da Lei n. 14.133/21.

30.2. A análise de conformidade exige um elevado grau de especialização e qualificação técnica. Além disso, a vedação da subcontratação assegura a responsabilidade direta da empresa contratada, facilitando o monitoramento e a cobrança de resultados, e evitando a diluição da responsabilidade entre diversas partes.

30.3. Portanto, é vedada a subcontratação, cessão e/ou transferência total ou parcial do objeto deste termo, nos termos do § 2º, art. 122 da Lei n. 14.133/21.

31. DAS PRÁTICAS DE SUSTENTABILIDADE NA EXECUÇÃO DOS SERVIÇOS

31.1. A CONTRATADA deverá atender, no que couber, o critério de sustentabilidade ambiental prevista na Instrução normativa SLTI/MPOG nº 01 de 19/01/2010, em conformidade com o art. 144 da Lei n. 14.133/21.

31.2. Os materiais a serem fornecidos deverão ter sido produzidos de acordo com os Critérios de Sustentabilidade Ambiental;

31.3. É de total responsabilidade da CONTRATADA o cumprimento das normas ambientais vigentes, no que diz respeito à poluição ambiental e destinação de resíduos;

31.4. A CONTRATADA deverá tomar todos os cuidados necessários para que não decorra qualquer degradação ao meio ambiente;

31.5. A CONTRATADA deverá assumir todas as responsabilidades e tomar as medidas cabíveis para a correção dos danos que vierem a ser causados, caso ocorra passivo ambiental, em decorrência da execução de suas atividades objeto desta licitação.

32. DA PARTICIPAÇÃO DE COOPERATIVAS

32.1. Fica vedada a participação de cooperativas, em atenção ao disposto no art. 16 da Lei Federal 14.133/21.

33. PARTICIPAÇÃO DE EMPRESAS REUNIDAS EM FORMA DE CONSÓRCIO

33.1. Fica vedada a participação de empresas sob a forma de consórcio, tendo em vista o objeto da licitação não ser de grande porte, complexo tecnicamente, e tampouco operacionalmente inviável de ser executado por apenas uma empresa, portanto, não é o caso da aplicação do art. 15 da Lei Federal 14.133/2021.

34. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

34.1. Considerando o artigo 40, § 3º, inciso II e III da lei 14133, o parcelamento da solução não será adotado por representar risco à implantação do objeto a ser contratado (proteção de rede adotada no parque computacional do Iperon, além do mesmo ser configurado como sistema único e integrado.

34.2. A padronização almejada também requer a indicação de marca, de modo que o fornecimento do objeto leva a fabricante único.

35. EXCLUSÃO DE PARTICIPAÇÃO DE PESSOAS FÍSICAS NA LICITAÇÃO

35.1. A exclusão de participação de Pessoas Físicas é respaldada pela necessidade de garantir a qualidade, durabilidade e conformidade dos produtos adquiridos.

35.2. Considerando que Pessoas Jurídicas, possuem uma estrutura mais sólida para atender às exigências técnicas e de fornecimento em larga escala. Além disso, a capacidade financeira das empresas contribui para a oferta de garantias contratuais e assegura a disponibilidade de recursos para atender às demandas da Administração Pública.

35.3. Ao restringir a participação a entidades jurídicas, busca-se fomentar a competitividade entre empresas que possuam a expertise necessária para fornecer licenças de endpoint (antivírus) de alta qualidade, contribuindo para a eficácia do processo licitatório e a satisfação das necessidades da instituição contratante. Essa medida visa a otimização dos recursos públicos e a garantia de uma aquisição que atenda aos padrões de desempenho e durabilidade requeridos.

36. DA PROTEÇÃO DAS INFORMAÇÕES

36.1. O Contratante e Contratada devem estar cientes dos direitos, obrigações e penalidades aplicáveis constantes da Lei Geral de Proteção de Dados Pessoais - Lei 13.709/2018, e obrigam-se a adotar todas as medidas razoáveis para garantir, por si, bem como seu pessoal, colaboradores, empregados que utilizem os Dados Protegidos na extensão autorizada na referida LGPD.

37. DA ARBITRAGEM

37.1. A Administração utilizar-se-á da aplicação de juízo arbitral para dirimir conflitos relativos a direitos patrimoniais disponíveis, conforme disposto na Lei Estadual 4.007 e Lei n. 9.307, de 1996, alterada pela Lei Federal n. 13.129, de 2015. Tal medida visa o cumprimento ao Art. 11, do referido diploma legal.

38. DAS CONDIÇÕES GERAIS

38.1. Fica estabelecido, caso venha ocorrer algum fato não previsto neste projeto básico/termo de referência e seus anexos, os chamados casos omissos, estes serão dirimidos respeitado o objeto dessa licitação, por meio de aplicação da legislação e demais normas reguladoras da matéria, em especial a Lei nº 14.133/21, aplicando-se paralelamente, quando for o caso, supletivamente, os princípios da teoria geral dos contratos estabelecidos na legislação civil brasileira e as disposições de direito privado.

38.2. As questões suscitadas que não possam ser dirimidas administrativamente serão

processadas e julgadas no foro da Comarca de Porto Velho/RO, com a exclusão de qualquer outro, por mais privilegiado que seja, salvo nos casos previstos no art. 102, I, 'd', da Constituição Federal.

38.3. Qualquer tolerância da Administração Pública quanto a eventuais infrações não implicará renúncia a direitos e não pode ser entendida como aceitação, novação ou precedente.

38.4. Cumprir e fazer cumprir, todas as diretrizes, normas, regulamentos impostas por este Termo de Referência.

38.5. As omissões dúvidas e casos não previstos neste instrumento serão resolvidos e decididos aplicando as regras contratuais e a Lei 14.133/21 e suas alterações, e/ou subsidiariamente no disposto acima, caso persista a pendência pelos Técnicos desta unidade.

38.6. O serviço ofertado deverá atender aos dispositivos da Lei nº. 8.078/90 (Código de Defesa do Consumidor) e às demais legislações pertinentes.

Porto Velho, data e hora do sistema.

Elaborado por:

Cibely dos Santos Leite
Assessora EQCOM

Revisado por:

MARIA GABRIELA DA SILVA SILVEIRA
Gerente Administrativa do Iperon

Aprovado por :

TIAGO CORDEIRO NOGUEIRA
Presidente do Iperon

DELNER DO CARMO AZEVEDO
Diretor de Administração e Finanças do Iperon

RUDNY WALLAS ALVES
Diretor de Tecnologia da Informação e Comunicação - DTIC

ANEXO I - MINUTA DE CONTRATO

CONTRATO Nº XXXX/IPERON/PGE/2024

CONTRATO DE AQUISIÇÃO DE SUBSCRIÇÃO DE PROTEÇÃO DE ENDPOINTS (ANTIVÍRUS), para atendimento as necessidades deste Instituto, QUE ENTRE SI CELEBRAM o Instituto de Previdência dos Servidores Públicos do Estado de Rondônia – IPERON, e a empresa XXXXXXXXXXXXXXXXX.

CONTRATANTE: O **INSTITUTO DE PREVIDÊNCIA DOS SERVIDORES PÚBLICOS DO ESTADO DE RONDÔNIA (Iperon)**, inscrito no CNPJ/MF sob o n. 15.849.540/0001-11, com sede na Avenida 7 de Setembro, n. 2.557, Bairro Nossa Senhora das Graças, na cidade de Porto Velho, Estado de Rondônia, representado pelo seu Presidente Tiago Cordeiro Nogueira, portador do CPF/MF n. 816.XXX.502-XX, e pelo Diretor de Administração e Finanças Delner do Carmo Azevedo, portador do CPF/MF n. 962.XXX.722-XX.

CONTRATADA: A empresa **XXXXXXXXXXXXXXXXXXXXXXXX**, CNPJ/MF n.º XX.XXX.XXX/XXXX-XX, estabelecida na Rua XXXXXXXXXXXX, nº XXX, bairro XXXXXXXXXX, CEP XXXXX-XXX, doravante denominada **CONTRATADA**, neste ato representada pelo Sr. **XXXXXXXXXXXXXXXXX**, CPF XXX.XXX.XXX-XX, de acordo com a representação legal que lhe é outorgada.

Os contratantes celebram o presente **CONTRATO ADMINISTRATIVO**, decorrente do Processo Administrativo nº 0016.000487/2024-37, que deu origem ao Pregão, na forma Eletrônica, de nº XXX/2023, homologado pelo Autoridade Competente, regido pelo Decreto Estadual nº. 28.874/2024, aplicando-se, subsidiariamente, no que couber, a Lei Federal nº. 14.133/21, com suas alterações e legislação correlata, sujeitando-se às normas dos supramencionados diplomas legais, mediante as cláusulas e condições a seguir estabelecidas:

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O objeto do presente instrumento é a aquisição de subscrição de proteção de endpoints (Antivírus) com implementação, atualização e suporte técnico por 36 (trinta e seis) meses, incluindo treinamento para turma de alunos, conforme condições estabelecidas neste Termo de Referência, visando aperfeiçoar a segurança da informação do Iperon.

1.2. Integram este Contrato além do Termo de Referência, as normas do Edital de Licitação do Pregão Eletrônico n. XXX/XXX e a proposta da CONTRATADA, independentemente de transcrição.

2. CLÁUSULA SEGUNDA – DO DETALHAMENTO DO OBJETO

2.1. Ficam aquelas estabelecidas no item 3 do Termo de Referência (Id. 0052488109) e seus anexos.

3. CLÁUSULA TERCEIRA – DO FORNECIMENTO DO OBJETO

3.1. Ficam aquelas estabelecidas no item 7 do Termo de Referência (Id. 0052488109) e seus anexos.

4. CLÁUSULA QUARTA – DAS CONDIÇÕES DE RECEBIMENTO DO OBJETO

4.1. Ficam aquelas estabelecidas no item 7.6 do Termo de Referência (Id. □□□□□□□□□□□□□□□□□□□□□□0052488109) e seus anexos.

5. CLÁUSULA QUINTA – DA GARANTIA

5.1. Ficam aquelas estabelecidas no item 24 do Termo de Referência (Id. □□□□□□□□□□□□□□□□□□□□□□□□□□□□□0052488109) e seus anexos.

6. CLÁUSULA SEXTA – DA VIGÊNCIA

6.1. Ficam aquelas estabelecidas no item 22 do Termo de Referência (Id. □□□□□□□□□□□□□□□□□□□□□□□□□□□□□0052488109) e seus anexos.

7. CLÁUSULA SÉTIMA – DO VALOR E DOTAÇÃO ORÇAMENTÁRIA

7.1. O valor desta contratação é de XXXXXXXXXXXXXX, conforme o Termo de Homologação (id. XXXXXXX), já estando nele incluídos os custos indiretos sobre a execução do serviço, tais como: tributos, seguros, impostos, taxas, serviços, encargos sociais e trabalhistas, previdenciários, fiscais e quaisquer despesas resultantes da entrega dos itens propostos, inclusive licença em repartições públicas e registros, se necessário e quaisquer outras que forem devidas.

7.2. As despesas com a prestação de que trata o objeto deste Contrato sairão do seguinte crédito orçamentário: Cód. U.O.: XXXXX - Programa de Trabalho: XXXXXXXXXXXXXX - Natureza de Despesa: XXXXXX - Fonte de Recursos: XXXXXX, conforme Declaração de Adequação Financeira (id. XXXXXXX).

8. CLÁUSULA OITAVA – DAS CONDIÇÕES DE PAGAMENTO

8.1. As formas e condições de pagamento estão descritas no item 21 do Termo de Referência (id. □□□□□□□□□□□□□□□□□□□□□□□□□□□□□0052488109) e seus anexos.

9. CLÁUSULA NONA – DA FISCALIZAÇÃO

9.1. O acompanhamento e fiscalização do Contrato serão realizados conforme descritos no item 27 do Termo de Referência (Id. 0052488109) e seus anexos.

10. CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATADA

10.1. Além daquelas determinadas por leis, decretos, regulamentos e demais dispositivos legais, nas obrigações da Contratada também se incluem o disposto no item 20.1 do Termo de Referência (id.

□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□0052488109) e seus anexos.

11. CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DA CONTRATANTE

11.1. Além daquelas determinadas por leis, decretos, regulamentos e demais dispositivos legais, nas obrigações da Contratante também se incluem o disposto no item 20.2 do Termo de Referência (id. □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□0052488109) e seus anexos.

12. CLÁUSULA DÉCIMA SEGUNDA – DAS SANÇÕES E PENALIDADES

12.1. Ficam aquelas estabelecidas no item 28 do Termo de Referência (Id. □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□0052488109) e seus anexos.

13. CLÁUSULA DÉCIMA TERCEIRA – DO REAJUSTE, ACRÉSCIMO E SUPRESSÃO

13.1. Os valores contratados serão fixos e irreajustáveis pelo período de sua vigência inicialmente prevista.

14. CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO CONTRATUAL

14.1. Ficam aquelas estabelecidas no item 25 do Termo de Referência (Id. □□□□□□□□□□□□□□□□□0052488109) e seus anexos.

15. CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS

15.1. As omissões, dúvidas e casos não previstos neste instrumento, serão resolvidos e decididos aplicando-se as regras da Lei Federal nº 14.133/21 e suas alterações, bem como demais ordenamentos jurídicos correlatos, levando-se sempre em consideração os princípios que regem a administração pública.

16. CLÁUSULA DÉCIMA SEXTA – DA PUBLICAÇÃO

16.1. Incumbirá à CONTRATANTE, por meio do Procuradoria Geral do Estado de Rondônia, providenciar a publicação deste instrumento, por extrato, no Diário Oficial do Estado de Rondônia, no prazo previsto na Lei Federal n. 14.133/21.

17. CLÁUSULA DÉCIMA SÉTIMA – DO FORO

17.1. As questões decorrentes da execução deste Instrumento que não possam ser dirimidas administrativamente serão processadas e julgadas no Foro de Porto Velho, capital do Estado de Rondônia, que prevalecerá sobre qualquer outro, por mais privilegiado que seja para dirimir quaisquer dúvidas oriundas do presente Contrato.

18. CLÁUSULA DÉCIMA OITAVA - DAS ASSINATURAS, DATA DA CELEBRAÇÃO E VISTO DA PROCURADORIA GERAL DO ESTADO

18.1. Considerando que a presente avença é celebrada no bojo de processo virtual que tramita no âmbito do Sistema Eletrônico de Informações - SEI, a data de celebração será correspondente a da aposição da assinatura eletrônica mais recente de qualquer das partes qualificadas no preâmbulo.
18.2. Instrumento jurídico elaborado na forma do artigo 23, inciso I, da Lei Complementar Estadual n. 620/2011, segundo as informações e documentos constantes dos autos do processo identificado neste instrumento.

19. CLÁUSULA DÉCIMA NONA - DAS DISPOSIÇÕES GERAIS

19.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente. Para firmeza e como prova do acordado, é lavrado o presente Contrato, o qual, depois de lido e achado conforme, vai assinado pelas partes, dele sendo extraídas as cópias que se fizerem necessárias para sua publicação e execução, devidamente certificadas pelo Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - IPERON.

Porto Velho-RO, data do sistema.

Tiago Cordeiro Nogueira
Presidente do Iperon

Delner do Carmo Azevedo
Diretor de Administração e Finanças

XXXXXXXXXXXXXXXXXX
Representante Legal da Contratada

VISTO DA PGE-IPERON

Documento assinado eletronicamente por **cibely dos santos leite**, **Assessor(a)**, em 06/09/2024, às 10:06, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **Maria Gabriela da Silva Silveira**, **Gerente**, em 06/09/2024, às 10:07, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **DELNER DO CARMO AZEVEDO**, **Diretor(a)**, em 06/09/2024, às 10:34, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **Tiago Cordeiro Nogueira**, **Presidente**, em 06/09/2024, às 12:35, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0052488109** e o código CRC **9E94FB64**.

Referência: Caso responda este Termo de Referência, indicar expressamente o Processo nº 0016.000487/2024-37 SEI nº 0052488109

GOVERNO DO ESTADO DE RONDÔNIA
Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - IPERON

ESTUDO TÉCNICO PRELIMINAR

1. INTRODUÇÃO

1.1. O presente documento caracteriza a primeira etapa da fase de planejamento e apresenta os devidos estudos para Aquisição de subscrição de Proteção de Endpoints com implementação e suporte técnico por **36 (Trinta e Seis) meses**, incluindo treinamento para turma de alunos , para fins de proteção da rede lógica, equipamentos de TI e informações do Iperon.

1.1.1. O Iperon é a autarquia previdenciária do Estado de Rondônia, com sede em Porto Velho além de 6 regionais distribuídas nos municípios de Guajará-Mirim, Ariquemes, Ji-Parana, Cacoal, Rolim de Moura e Vilhena e atualmente possui aproximadamente 350 equipamentos (Computadores, Notebooks e Servidores de aplicação) que necessitam de proteção contra ameaças digitais (Vírus, Ransomware, Trojans etc.).

1.1.2. As boas práticas relacionadas a segurança da informação determinam que um ambiente computacional deve dispor de proteções para os mais diversos tipos de ameaças virtuais. Entre essas ameaças uma das mais evidentes são os vírus de computador, que em seus vários tipos, podem causar desde aborrecimentos de lentidão em máquinas até a perda total da informação institucional.

1.1.3. Dessa forma, é indispensável que existam, tanto nas estações de trabalho, como nos servidores e dispositivos móveis que eventualmente ingressam à rede, softwares antivírus instalados, licenciados e constantemente atualizados, visto que ameaças virtuais surgem a todo momento e, em um mundo globalizado, onde a informação é um dos bens mais importantes das instituições, um incidente envolvendo esse tipo de software pode representar prejuízos incalculáveis.

2. ALINHAMENTO COM OS INSTRUMENTOS DE PLANEJAMENTO ORGANIZACIONAL

PLANEJAMENTO ESTRATÉGICO

A2 - PROVER INOVAÇÕES E TECNOLOGIAS INTEGRADAS

3. DESCRIÇÃO DA NECESSIDADE

3.1. Do Objeto

3.2. Aquisição de subscrição de Proteção de Endpoints com implementação e suporte técnico por **36 (Trinta e Seis) meses**, incluindo treinamento para turma de alunos , para fins de proteção da rede lógica, equipamentos de TI e informações do Iperon.

3.3. Da Necessidade

3.3.1. Atualmente o Iperon utiliza a Solução de Antivirus Kaspersky (adquirida no processo 0016.181935/2020-61, contudo, sua garantia de atualização expira em 07 de agosto de 2024, momento em que as atuais licenças não mais permitirão atualização de novas versões da solução e das bases de dados (lista de vírus e vacinas), o que pode acarretar em vulnerabilidades na rede corporativa, assim como a possibilidade de entrada de malwares, como vírus e worms, capazes de comprometer a integridade e disponibilidade do dispositivos computacionais.

3.3.2. 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 neste instituto, resguardando a conduta de manuseio, controle e proteção das informações contra destruição, modificação, comercialização, divulgação indevida e acessos não autorizados,

acidentais ou intencionais.

3.3.3. A renovação do software de antivírus é essencial para viabilizar proteção adequada e atualizada no ambiente computacional das organizações (computadores e servidores da rede), de modo a preservar os ativos corporativos (hardware, software e dados), garantindo a integridade, confidencialidade e segurança das informações institucionais contra as ações de programas maléficos que ponham em risco a segurança e a continuidade das atividades das organizações.

3.3.4. Neste Processo pede-se também a contratação de treinamento para equipe de TI para atualização dos conhecimentos.

3.3.5. Ao longo dos últimos anos, a Solução Corporativa de Antivírus tem contribuído para a integridade e disponibilidade da segurança da informação do ambiente computacional do Iperon, protegendo a rede corporativa de ataques de malwares originados da Internet e de dispositivos infectados, tal como pendrives.

3.3.6. 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.

3.3.7. O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda id 0045747604, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação, destacando ainda que a contratação está prevista no Plano de Anual de Contratações (PAC) 2024.

3.4. DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

3.4.1. Contratação de **subscrição de** Soluções de Segurança Avançada de Endpoints (Antivírus) para proteção de servidores, estações de trabalho e plataforma de correio eletrônico, incluindo atualização de base de assinaturas, atualização de software, implantação, incluindo treinamento e suporte técnico especializado por 36(Trinta e Seis) meses, visando atender as demandas da Diretoria de Tecnologia da Informação e Comunicação - DTIC, nas condições e forma descritas neste instrumento e seus anexos.

3.4.2. O contrato de antivírus do Iperon, número 002/2020 (ID 0012742450), firmado no ano de 2020, contempla atualmente 250 licenças.

3.4.3. Diante da previsão de aumento de servidores e estagiários, torna-se imperativo o aumento do quantitativo para 400 (Quatrocentas) licenças, conforme justificativa a seguir:

3.4.4. Atualmente, 105 servidores do instituto estão cedidos para outros órgãos e boa parte deles está em fase de retorno para o Iperon, gerando a necessidade de contemplá-los com equipamentos protegidos com antivírus;

3.4.5. Adicionalmente, está em trâmite o processo 0016.002368/2023-38 que prevê a contratação de agente de integração para prestação de serviços de recrutamento de estagiários, com previsão de até 100 (Cem) vagas, que colabora para o aumento da demanda de licenças de antivírus;

3.4.6. É importante lembrar também, que está em andamento processo para deflagração de concurso público, conforme Portaria nº 297 de 03 de maio de 2024 (ID 0048365067), e com isso haverá necessidade de aumento do quantitativo de licenças.

3.4.7. Diante do exposto, a ampliação do quantitativo de licenças é de extrema necessidade e visa assegurar a proteção adequada dos sistemas e dispositivos contra ameaças cibernéticas, garantindo a integridade e segurança das operações realizadas pelo Iperon.

LOTE	Código SIASG/CATMAT	ITEM	OBJETO	MÉTRICA	QTD
	27502	1	Aquisição de subscrição de Proteção de Endpoints (Antivírus) com implementação, atualização e suporte técnico por **36 (Trinta e Seis) meses**	Licença	400

1	20052	2	Treinamento remoto na Proteção de Endpoints fornecida no item 1, para turma de no mínimo 3 (três) alunos, incluindo 16 (dezesseis) horas de serviços de instalação dos módulos novos.	Turma	1

3.4.8. O objeto da licitação tem a natureza de serviço comum de Tecnologia da Informação.

3.4.9. A presente contratação adotará como regime de execução por Preço Unitário.

3.4.10. O prazo de vigência da contratação é de **36 (Trinta e Seis) meses** contados da data da sua publicação, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

3.4.11. As licenças e certificados de garantia devem estar aderentes às especificações técnicas, funcionalidades e pré-requisitos definidos pelo Iperon.

4. REQUISITOS NECESSÁRIOS

4.1. Requisitos de Negócio

4.1.1. Os requisitos de negócio são aqueles que independem de características tecnológicas e que definem as necessidades e os aspectos funcionais da Solução de Tecnologia da Informação.

4.1.2. A motivação para a aquisição e renovação da solução de software de antivírus se dá em função das licenças vigentes estar com data de expiração para Agosto de 2024. A partir desta data todos os computadores – servidores e estações de trabalho, bem como os serviços suportados por estes estarão vulneráveis, tanto a ataques internos, quanto externos.

4.1.3. A contratação em questão visa Garantir o perfeito funcionamento da infraestrutura de rede do Iperon, garantir a segurança das informações do negócio e continuidade dos serviços e manter atualizada a solução de proteção antivírus contra novas ameaças.

4.1.4. Considerando a crescente evolução das ameaças digitais – vírus, malwares e suas variantes – e as descobertas diárias de vulnerabilidades nos sistemas computacionais, as quais são amplamente exploradas por softwares maliciosos, faz-se necessária a aquisição de software especifico e que abranja as mais recentes funcionalidades no que tange a proteção contra esse tipo de ameaça. Tais ameaças podem comprometer em caráter definitivo e de forma irrecuperável o ambiente computacional do instituto, contaminando arquivos e sistemas, capturando dados, causando indisponibilidade e comprometendo a confiabilidade de sistemas, bem como a integridade dos dados armazenados nos computadores e servidores de rede desta Instituição.

4.1.5. De forma a promover a gestão e fomentar os aspectos de segurança da informação, a DTIC - Diretoria de Tecnologia da Informação e Comunicação , no âmbito da rede corporativa do Iperon, deve Instituir uma estrutura para a gestão de segurança da informação e comunicações.

4.2. Requisitos Gerais:

4.2.1. Subscrição de proteção de endpoints, com implementação e suporte técnico por **36 (Trinta e Seis) meses**, incluindo treinamento para turma de alunos.

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

4.2.3. 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.

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

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

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

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

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

4.2.9. Proteção contra ameaças sem arquivos (Fileless);

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

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

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

4.2.13. 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.

4.2.14. 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.

4.2.15. 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.

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

4.2.17. 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.

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

4.2.19. Controles de aplicativos,

4.2.20. Controle web e dispositivos

4.2.21. HIPS e Firewall

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

4.2.23. Gerenciamento de criptografia de arquivos e discos;

4.2.24. Controle adaptativo para detecção de anomalias;

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

4.2.26. 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.

4.2.27. A solução proposta deve ter bancos de dados de reputação locais e globais.

4.2.28. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.

4.2.29. A solução proposta deve incluir um módulo capaz, no mínimo, de:

4.2.30. Bloqueio de aplicativos com base em sua categorização.

4.2.31. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.

4.2.32. A adição de sub-redes e a modificação de permissões de atividade.

4.2.33. 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.

4.2.34. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.

4.2.35. 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.

4.2.36. A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:

4.2.37. Modo silencioso;

4.2.38. Discos rígidos e dispositivos removíveis;

4.2.39. De todos as contas de usuários do dispositivo.

4.2.40. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:

4.2.41. Exclusão imediata de dados;

4.2.42. Exclusão de dados adiada.

4.2.43. A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:

4.2.44. Excluir usando os recursos do sistema operacional - os arquivos são excluídos;

4.2.45. Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.

4.2.46. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.

4.2.47. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.

4.2.48. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.

4.2.49. 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.

4.2.50. 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.

4.2.51. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.

4.2.52. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.

4.2.53. 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;

4.2.54. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;

4.2.55. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.

4.2.56. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.

4.2.57. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.

4.2.58. A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.

4.2.59. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.

4.2.60. 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.

4.2.61. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.

4.2.62. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.

4.2.63. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.

4.2.64. 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.

4.2.65. A solução proposta deve ter categoria de detecção para bloquear banners de sites.

4.2.66. 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;

4.2.67. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.

4.2.68. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.

4.2.69. 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.

4.2.70. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

4.2.71. 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.

4.2.72. 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.

4.2.73. 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.

4.2.74. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.

4.2.75. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.

4.2.76. A solução proposta deve suportar o controle de scripts executados em PowerShell.

4.2.77. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.

4.2.78. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.

4.2.79. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.

4.2.80. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.

4.2.81. 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.

4.2.82. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.

4.2.83. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:

4.2.84. Filtro de anexos.

4.2.85. Verificação de mensagens de email ao receber, ler e enviar.

4.2.86. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.

4.2.87. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;

4.2.88. 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.);

4.2.89. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registro do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.

4.2.90. 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.

4.2.91. A solução proposta deve incluir suporte ao protocolo IPv6.

4.2.92. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.

4.2.93. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

4.2.94. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.

4.2.95. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

4.2.96. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.

4.2.97. 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.

4.2.98. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.

4.2.99. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.

4.2.100. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.

4.2.101. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.

4.2.102. 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.

4.2.103. 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.

4.2.104. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.

4.2.105. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.

4.2.106. 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.

4.2.107. A solução proposta deve suportar endereços IPv6.

4.2.108. A solução proposta deve suportar verificação em duas etapas (autenticação).

4.2.109. 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.

4.2.110. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.

4.2.111. 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.

4.2.112. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.

4.2.113. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.

4.2.114. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.

4.2.115. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.

4.2.116. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.

4.2.117. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.

4.2.118. 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.

4.2.119. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.

4.2.120. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.

4.2.121. 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.

4.2.122. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.

4.2.123. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.

4.2.124. A solução proposta deve ter a capacidade de excluir atualizações baixadas.

4.2.125. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.

4.2.126. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.

4.2.127. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.

4.2.128. 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.

4.2.129. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.

4.2.130. 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.

4.2.131. 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.

4.2.132. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.

4.2.133. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:

4.2.134. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.

4.2.135. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

4.2.136. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.

4.2.137. A solução proposta deve gerar relatorios de vulnerabilidades encontradas nos dispositivos com sensor de endpoint instalado.

4.3. **Do Módulo de proteção de endpoint:**

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

4.3.2. Windows 7

4.3.3. Windows 8

4.3.4. Windows 8.1

4.3.5. Windows 10

4.3.6. Windows 11

4.3.7. Windows Small Business Server 2011

4.3.8. Windows MultiPoint Server 2011

4.3.9. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

4.3.10. Servidores de terminal Microsoft

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

4.3.12. Sistemas operacionais Linux de 32 bits:

4.3.13. CentOS 6.7 e posterior

4.3.14. Debian GNU/Linux 11.0 e posterior

4.3.15. Debian GNU/Linux 12.0 e posterior

4.3.16. Red Hat Enterprise Linux 6.7 e posterior

4.3.17. Amazon Linux 2.

4.3.18. CentOS 6.7 e mais tarde

4.3.19. CentOS 7.2 e posterior.

4.3.20. CentOS Stream 8.

4.3.21. CentOS Stream 9.

4.3.22. Debian GNU/Linux 11.0 e posterior.

4.3.23. Debian GNU/Linux 12.0 e posterior.

4.3.24. Linux Mint 20.3 e superior.

4.3.25. Linux Mint 21.1 e posterior.

4.3.26. openSUSE Leap 15.0 e posterior.

4.3.27. Oracle Linux 7.3 e posterior.

4.3.28. Oracle Linux 8.0 e posterior.

4.3.29. Oracle Linux 9.0 e posterior.

4.3.30. Red Hat Enterprise Linux 6.7 e posterior

4.3.31. Red Hat Enterprise Linux 7.2 e posterior.

4.3.32. Red Hat Enterprise Linux 8.0 e posterior.

4.3.33. Red Hat Enterprise Linux 9.0 e posterior.

4.3.34. Rocky Linux 8.5 e posterior.

4.3.35. Rocky Linux 9.1.

4.3.36. SUSE Linux Enterprise Server 12.5 ou posterior.

4.3.37. SUSE Linux Enterprise Server 15 ou posterior.

4.3.38. Ubuntu 20.04 LTS.

4.3.39. Ubuntu 22.04 LTS.

4.3.40. CentOS Stream 9.

4.3.41. SUSE Linux Enterprise Server 15.

4.3.42. Ubuntu 22.04 LTS.

4.3.43. macOS 12 – 14

4.3.44. Ferramentas de virtualização MAC OS:

4.3.45. Parallels Desktop 16 para Mac Business Edition

4.3.46. VMware Fusion 11.5 Profissional

4.3.47. VMware Fusion 12 Profissional

4.3.48. A solução proposta deverá suportar as seguintes plataformas virtuais:

4.3.49. VMware Workstation 17.0.2 Pro

4.3.50. VMware ESXi 8.0 Update 2

4.3.51. Microsoft Hyper-V Server 2019

4.3.52. Citrix Virtual Apps e Desktop 7 2308

4.3.53. Citrix Provisioning 2308

4.3.54. Citrix Hypervisor 8.2 Update 1

4.4. **Do Módulo de Gerenciamento Avançado:**

4.4.1. A solução proposta deve suportar arquitetura cloud-native e on-premisse;

4.4.2. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:

4.4.3. Amazon Web Services;

4.4.4. Microsoft Azure;

4.4.5. A solução proposta deve incluir as seguintes opções de integração SIEM:

4.4.6. HP (Microfoco) ArcSight;

4.4.7. IBM QRadar;

4.4.8. Splunk;

4.4.9. Kaspersky KUMA;

4.4.10. 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;

4.4.11. 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;

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

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

4.4.14. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

4.4.15. 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;

4.4.16. 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;

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

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

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

4.4.20. 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:

4.4.21. Status do dispositivo;

4.4.22. Tag;

4.4.23. Diretório ativo;

4.4.24. Proprietários de dispositivos;

4.4.25. Hardware;

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

4.4.27. E-mail;

4.4.28. Registro de sistema;

4.4.29. SMS;

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

4.4.31. Atributos de rede;

4.4.32. Nome;

4.4.33. Domínio e/ou Sufixo de Domínio;

4.4.34. Endereço de IP;

4.4.35. Endereço IP para servidor de gerenciamento;

4.4.36. Localização no Active Directory;

4.4.37. Unidade organizacional;

4.4.38. Grupo;

4.4.39. Sistema operacional;

4.4.40. Número do pacote de serviço;

4.4.41. Arquitetura Virtual;

4.4.42. Registro de aplicativos;

4.4.43. Nome da Aplicação;

4.4.44. Versão do aplicativo;

4.4.45. Fabricante;

4.4.46. Tipo e versão;

4.4.47. Arquitetura;

4.4.48. 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;

4.4.49. 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;

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

4.4.51. Dispositivos Desktop/Servidores

4.4.52. Dispositivos móveis;

4.4.53. Dispositivos de rede;

4.4.54. Dispositivos virtuais;

4.4.55. Componentes OEM;

4.4.56. Periféricos de computador;

4.4.57. Dispositivos IoT conectados;

4.4.58. Telefones VoIP;

4.4.59. Repositórios de rede;

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

4.4.61. Nome da Aplicação;

4.4.62. Caminho do aplicativo;

4.4.63. Metadados do aplicativo;

4.4.64. Aplicativo Certificado digital;

4.4.65. Categorias de aplicativos predefinidas pelo fornecedor;

4.4.66. SHA256 e MD5;

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

4.4.68. Bluetooth;

4.4.69. Dispositivos móveis;

4.4.70. Modems externos;

4.4.71. CD/DVD;

4.4.72. Câmeras e scanners;

4.4.73. MTPs;

4.4.74. E a transferência de dados para dispositivos móveis;

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

4.4.76. 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;

4.4.77. 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:

4.4.78. Estruturas de domínios e grupos de trabalho do Windows;

4.4.79. Estruturas de grupos do Active Directory;

4.4.80. Conteúdo de um arquivo de texto criado manualmente pelo administrador;

4.4.81. 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.

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

4.4.83. Verificação manual;

4.4.84. Verificação no acesso;

4.4.85. Verificação por demanda;

4.4.86. Verificação de arquivos compactados

4.4.87. Verificação de arquivos individuais, pastas e unidades;

4.4.88. Bloqueio e verificação de scripts

4.4.89. Proteção contra alteração de registros;

4.4.90. Proteção contra estouro de buffer;

4.4.91. Verificação em segundo plano/inativa.

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

4.4.93. 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.

4.4.94. 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.

4.4.95. 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.

4.4.96. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.

4.4.97. 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.

4.4.98. A solução proposta deve suportar Windows Failover Cluster.

4.4.99. A solução proposta deve ter um recurso de clustering integrado.

4.4.100. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.

4.4.101. 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.

4.4.102. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.

4.4.103. 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.

4.4.104. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.

4.4.105. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.

4.4.106. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.

4.4.107. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.

4.4.108. A solução proposta deverá possuir controles para download de DLL e drivers.

4.4.109. 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.

4.4.110. 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.

4.4.111. 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).

4.4.112. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.

4.4.113. 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.

4.4.114. 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.

4.4.115. 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.

4.4.116. 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.

4.4.117. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.

4.4.118. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.

4.4.119. 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.

4.4.120. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.

4.4.121. 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.

4.4.122. 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. .

4.4.123. 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.

4.4.124. 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.

4.4.125. A solução proposta deve permitir ao administrador personalizar relatórios.

4.4.126. 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.

4.4.127. 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.

4.4.128. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.

4.4.129. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.

4.4.130. 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.

4.4.131. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.

4.4.132. 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;

4.4.133. 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.

4.4.134. A solução proposta deve suportar integração com solução APT.

4.4.135. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:

4.4.136. Windows;

4.4.137. Linux;

4.4.138. A solução proposta deverá suportar os seguintes servidores de banco de dados:

4.4.139. Microsoft SQL Server;

4.4.140. Microsoft Banco de dados SQL do Azure;

4.4.141. MySQL Standard e Enterprise;

4.4.142. MariaDB;

4.4.143. PostgreSQL;

4.4.144. MySQL;

4.4.145. MariaDB;

4.4.146. PostgreSQL;

4.4.147. A solução proposta deverá suportar as seguintes plataformas virtuais:

4.4.148. VMware vSphere 6.7 e 7.0;

4.4.149. Estação de trabalho VMware 16 Pro;

4.4.150. Servidor Microsoft Hyper-V 2012 de 64 bits;

4.4.151. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;

4.4.152. Microsoft Servidor Hyper -V 2016 de 64 bits;

4.4.153. Servidor Microsoft Hyper-V 2019 de 64 bits;

4.4.154. Servidor Microsoft Hyper-V 2022 de 64 bits;

4.4.155. Citrix XenServer 7.1 LTSR;

4.4.156. Citrix XenServer 8.x;

4.4.157. Oracle VM VirtualBox 6.x;

4.4.158. VMware vSphere 6.7, 7.0 e 8.0;

4.4.159. VMware Desktop 16 Pro e 17 Pro;

4.4.160. Servidor Microsoft Hyper-V 2012 de 64 bits;

4.4.161. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;

4.4.162. Microsoft Servidor Hyper -V 2016 de 64 bits;

4.4.163. Servidor Microsoft Hyper-V 2019 de 64 bits;

4.4.164. Servidor Microsoft Hyper-V 2022 de 64 bits;

4.4.165. Citrix XenServer 7.1 e 8.x;

4.4.166. Oracle VM VirtualBox 6.x e7.x;

4.4.167. A solução proposta deve suportar criptografia em vários níveis:

4.4.168. Criptografia completa do disco – incluindo disco do sistema;

4.4.169. Criptografia de arquivos e pastas;

4.4.170. Criptografia de mídia removível;

4.4.171. Gerenciamento de criptografia BitLocker e MacOS Filevault2;

4.4.172. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:

4.4.173. A criptografia de arquivos em unidades de computador locais;

4.4.174. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões;

4.4.175. A criação de listas criptografadas de pastas em unidades de computador locais;

4.4.176. 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:

4.4.177. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis;

4.4.178. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais;

4.4.179. 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:

4.4.180. A criptografia de todos os arquivos armazenados em unidades removíveis;

4.4.181. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis;

4.4.182. 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

4.4.183. 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.

4.4.184. 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.

4.4.185. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.

4.4.186. 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.

4.4.187. 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.

4.4.188. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.

4.4.189. 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.

4.4.190. 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.

4.4.191. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.

4.4.192. 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.

4.4.193. 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.

4.4.194. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.

4.4.195. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário.

4.4.196. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.

4.4.197. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.

4.4.198. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:

4.4.199. Uso do Trusted Platform Module e configurações de senha;

4.4.200. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível;

4.4.201. 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);

4.4.202. A solução proposta deve suportar criptografia em Microsoft Surface Tablets;

4.4.203. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:

4.4.204. Instalação remota de software de terceiros;

4.4.205. Relatórios sobre software e hardware existentes;

4.4.206. Monitoramento para instalação de software não autorizado;

4.4.207. Remoção de software não autorizado;

4.4.208. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.

4.4.209. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.

4.4.210. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.

4.4.211. 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.

4.4.212. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.

4.4.213. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.

4.4.214. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.

4.4.215. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança

4.4.216. A solução proposta deve permitir ao administrador aprovar atualizações.

4.4.217. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.

4.4.218. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.

4.4.219. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.

4.4.220. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.

4.4.221. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.

4.4.222. 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).

4.4.223. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.

4.4.224. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.

4.4.225. A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’.

4.4.226. A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”.

4.4.227. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.

4.4.228. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.

4.4.229. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.

4.4.230. A solução proposta deve apoiar a implantação do sistema operacional.

4.4.231. A solução proposta deve suportar Wake-on LAN e UEFI.

4.4.232. 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.

4.4.233. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.

4.4.234. 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.

4.4.235. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.

4.4.236. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.

4.4.237. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.

4.4.238. 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.

4.4.239. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.

4.4.240. 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.

4.4.241. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:

4.4.242. Inicie a instalação ao reiniciar ou desligar o computador;

4.4.243. Instale o gerador necessário todos os pré-requisitos do sistema;

4.4.244. Permitir a instalação de novas versões de aplicativos durante as atualizações;

4.4.245. Baixe atualizações para o dispositivo sem instalá-las;

4.4.246. 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.

4.4.247. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.

4.4.248. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:

4.4.249. CEF;

4.4.250. LEEF;

4.4.251. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.

4.4.252. O relatório da solução proposta deve conter informações CVE.

4.4.253. A solução proposta deve suportar instalação de aplicações e software de terceiros;

4.5. **Do Módulo de Gerenciamento Simplificado:**

4.5.1. A solução proposta deve suportar arquitetura cloud;

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

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

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

4.5.5. 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.

4.5.6. A solução proposta deve atender as condições apontadas no item e subintes 6.

4.5.7. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.

4.5.8. A solução proposta deve incluir informações do endpoint:

4.5.9. IP público de internet;

4.5.10. IP interno do dispositivo;

4.5.11. Versão do agente de proteção;

4.5.12. Ultima comunicação com a console, contendo data e hora;

4.5.13. Informações do sistema operacional;

4.5.14. 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.

4.5.15. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.

4.5.16. A solução proposta deve incluir treinamento em segurança cibernética.

4.6. **Do Módulo de Gerenciamento de Dispositivos Móveis:**

4.6.1. O modulo deve ser integrado a console de gerenciamento;

4.6.2. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

4.6.3. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)

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

4.6.5. iOS 10–17 ou iPadOS 13–17

4.6.6. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.

4.6.7. A solução proposta deve suportar dispositivos iOS supervisionados.

4.6.8. 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.

4.6.9. 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.

4.6.10. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.

4.6.11. 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).

4.6.12. 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.

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

4.6.14. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.

4.6.15. A solução proposta deve ter recursos de conteinerização para dispositivos Android.

4.6.16. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:

4.6.17. Dados em contêineres

4.6.18. Contas de e-mail corporativo

4.6.19. Configurações para conexão à rede Wi-Fi corporativa e VPN

4.6.20. Nome do ponto de acesso (APN)

4.6.21. Perfil do Android for Work

4.6.22. Recipiente KNOX

4.6.23. Chave do gerenciador de licença KNOX

4.6.24. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:

4.6.25. Todos os perfis de configuração instalados

4.6.26. Todos os perfis de provisionamento

4.6.27. O perfil iOS MDM

4.6.28. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas

4.6.29. 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 .

4.6.30. 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:

4.6.31. Critérios de verificação do dispositivo;

4.6.32. 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;

4.6.33. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.

4.6.34. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:

4.6.35. Cartões de memória e outras unidades removíveis

4.6.36. Câmera do dispositivo

4.6.37. Conexões Wi-Fi

4.6.38. Conexões Bluetooth

4.6.39. Porta de conexão infravermelha

4.6.40. Ativação do ponto de acesso Wi-Fi

4.6.41. Conexão de área de trabalho remota

4.6.42. Sincronização de área de trabalho

4.6.43. Definir configurações da caixa de correio do Exchange

4.6.44. Configurar caixa de e-mail em dispositivos iOS MDM

4.6.45. Configure contêineres Samsung KNOX.

4.6.46. Definir as configurações do perfil do Android for Work

4.6.47. Configurar e-mail/calendário/contatos

4.6.48. Defina as configurações de restrição de conteúdo de mídia.

4.6.49. Definir configurações de proxy no dispositivo móvel

4.6.50. Configurar certificados e SCEP

4.6.51. 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 .

4.6.52. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:

4.6.53. Google Play, Huawei App Gallery e Apple App Store

4.6.54. Portal de inscrição móvel KNOX

4.6.55. Pacotes de instalação pré-configurados independentes

4.6.56. 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.

4.6.57. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.

4.6.58. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:

4.6.59. VMware AirWatch 9.3 ou posterior

4.6.60. MobileIron 10.0 ou posterior

4.6.61. IBM MaaS360 10.68 ou posterior

4.6.62. Microsoft Intune 1908 ou posterior

4.6.63. SOTI MobiControl 14.1.4 (1693) ou posterior

4.6.64. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.

4.6.65. A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:

4.6.66. Google Play

4.6.67. Galeria de aplicativos Huawei

4.6.68. Loja de aplicativos da Apple

4.6.69. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.

4.6.70. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.

4.6.71. 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.

4.6.72. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.

4.6.73. 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.

4.6.74. 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.

4.6.75. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.

4.6.76. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.

4.6.77. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.

4.6.78. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.

4.6.79. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.

4.6.80. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.

4.6.81. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;

4.6.82. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

4.7. **Do Módulo de EDR**

4.7.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

4.7.2. 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.

4.7.3. 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;

4.7.4. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;

4.7.5. Deve apresentar informações detalhadas contendo:

4.7.6. Usuário que executou a ação;

4.7.7. Informações acesso privilegiado;

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

4.7.9. A solução proposta deve suportar integração com serviço de reputação em nuvem.

4.7.10. 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.)

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

4.7.12. Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;

4.7.13. A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.

4.7.14. A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.

4.7.15. A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.

4.7.16. A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.

4.7.17. A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.

4.7.18. A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.

4.7.19. 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.

4.7.20. 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.

4.7.21. A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.

4.7.22. 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:

4.7.23. Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).

4.7.24. Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.

4.7.25. Informações gerais sobre a detecção, incluindo modo de detecção.

4.7.26. Alterações no registro associadas à detecção.

4.7.27. Histórico da presença de arquivos no dispositivo.

4.7.28. Ações de resposta executadas pela aplicação.

4.7.29. 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.

4.7.30. A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:

4.7.31. Processo

4.7.32. Conexões de rede

4.7.33. Alterações no registro

4.7.34. Detalhes do download de objeto

4.7.35. A solução proposta deve fornecer orientação de resposta (resposta guiada).

4.7.36. A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente

4.7.37. A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:

4.7.38. Impedir a execução de objetos

4.7.39. Isolamento de host

4.7.40. Excluir objeto do host ou grupo de hosts

4.7.41. Encerrar um processo no dispositivo

4.7.42. Colocar um objeto em quarentena

4.7.43. Execute a verificação do sistema

4.7.44. Execução remota de programa/processo/comando

4.7.45. Iniciar a varredura IoC para um grupo de hosts.

4.8. **Requisitos de Documentação**

4.8.1. A documentação da solução de proteção de endpoint incluindo ferramentas de administração, deve incluir os seguintes documentos:

4.8.2. Ajuda on-line para administradores

4.8.3. Ajuda on-line para melhores práticas de implementação

4.8.4. Ajuda on-line para proteção de servidores de administração

4.8.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.

4.8.6. Deve estar disponível página com informações de ciclo de vida das soluções e módulos;

4.9. **Requisitos do Treinamento:**

4.9.1. A licitante deverá realizar treinamento da solução ofertada, com carga horária mínima de 16 (Dezesseis) horas de duração, para turma de no mínimo 3 (Três) alunos.

4.9.2. O treinamento deverá ser realizado em dias úteis, em horário de funcionamento do Iperon das 7:30 as 13:30 (Horário local)

4.9.3. O treinamento pode ser realizado de forma remota (Online).

4.9.4. Deverá ser emitido certificado de participação ao final do curso para cada participante.

4.9.5. O cronograma efetivo do treinamento será definido em conjunto com a CONTRATANTE, após a assinatura do contrato.

4.9.6. Deverá ser abordado em seu conteúdo programático, no mínimo, os seguintes temas:

4.9.7. Solução de Antivírus, Firewall;

4.9.8. Controle de Aplicativos;

4.9.9. Controle de Acesso à WEB;

4.9.10. Controle de Dispositivos (USB);

4.9.11. Gerenciamento de vulnerabilidades e correções;

4.9.12. Console de Gerenciamento Integrada.

4.10. **Requisitos Gerais para a Segurança da Contratação:**

4.10.1. Caso não seja o próprio fabricante, o licitante deverá apresentar Carta do Fabricante específica para este certame, juntamente com a proposta comercial comprovando ser revenda autorizada, certificada e habilitada para fornecer a subscrição destes softwares, bem como prestar serviços de suporte técnico especializado, realizar treinamentos, instalação e configuração.

4.10.2. O licitante, deverá apresentar atestado de capacidade técnica que comprove o fornecimento de subscrição destes softwares ou softwares similares (proteção de endpoints/antivírus) , para o setor público ou privado, bem como que demonstre prestação de serviços de suporte técnico especializado, realização de treinamentos, instalação e configuração para no mínimo 50% do quantitativo deste edital.

4.10.3. O licitante deverá apresentar, juntamente com a proposta comercial, documentação de vínculo empregatício de até 2 (dois) profissionais técnicos juntamente com os respectivos certificados, sendo estes profissionais aptos a prestar o serviço de suporte técnico que for necessário.

4.10.4. O licitante vencedor desta licitação, deverá apresentar juntamente com a proposta comercial, certificação de boas práticas ITIL Foundation, de pelo menos um profissional que será responsável por ser o ponto de referência das demandas técnicas desta instituição, durante todo o período de garantia da subscrição deste software.

4.10.5. Deverá ser anexada na proposta comercial a comprovação de certificação do profissional, no produto fornecido.

5. ESTIMATIVA DA DEMANDA

5.1. Considerando os números atuais de dispositivos presentes da rede do Iperon, bem como perspectiva de evolução do parque de dispositivos, devido a instalação de novos computadores, estima-se o seguinte volume de licença de antivírus e serviços:

5.2. Considerando que as aquisições realizadas no ano de 2023 visou substituir equipamentos obsoletos, o quantitativo de licenças adquirido permanece suficiente para cobrir todo o parque computacional da Iperon.

5.3. Para o treinamento pretendido, estimamos que o mesmo deve possuir pelo menos 12 (doze) horas para 02 (dois) servidores da Diretoria de Tecnologia da Informação e Comunicação - DTIC e os tópicos que devem ser abordados serão pormenorizados no Termo de Referência.

6. LEVANTAMENTO DAS DIFERENTES SOLUÇÕES QUE ATENDAM À DEMANDA

6.1. Considerando o inciso I, do artigo 41, da Lei 14.133/2021, faz-se necessária a padronização e indicação de marca para a manutenção da proteção atual de ativos de rede (Antivírus), de forma homogênea, no parque computacional do Iperon. Dito isso, justifica-se a manutenção da marca KASPERSKY devido ao/à:

6.2. **Gerenciamento:** Todas as configurações do software de gerenciamento centralizado da solução atual poderão ser aproveitadas sem nenhuma janela de migração, bem como todos os equipamentos que atualmente são gerenciados irão manter as informações de conexão, gerenciamento e sincronização podem ser configurados e administrados por uma única console proporcionando;

6.3. **Configuração e conhecimento:** A padronização dos equipamentos auxilia e facilita a administração da rede, devido a utilização de apenas um sistema operacional em todos os equipamentos, ou seja, uma única interface de comandos a serem utilizados para configuração de toda a rede. Com isso, torna-se mais fácil o treinamento, a gestão do conhecimento, e auxilia na redução do tempo de configuração e reparo.

6.4. **Desempenho:** soluções de mesmo fabricante permitem a utilização de recursos proprietários, ou seja, recursos que garantem maior desempenho dos equipamentos, mas que só podemos utilizá-los com a homogeneidade da malha, como configurações de alta disponibilidade
essenciais às necessidades do instituto.

6.5. Além do exposto, considerando o levantamento realizado, observamos que o serviço utilizado por outros entes públicos para a proteção de suas unidades administrativas é majoritariamente o Software da

empresa Kaspersky, o mesmo serviço em funcionamento atualmente no Iperon e que se pretende adquirir novas licenças.

6.6. Embora existam no mercado outras soluções renomadas, pelos fatores já expostos, busca-se adquirir novas licenças do mesmo software, reduzindo os custos que a contratação de soluções diferentes trariam.

7. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

7.1. Durante o estudo em questão, foi identificado necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas:

UNIDADE	PROCESSO	OBJETIVO	QTD	PERÍODO	VALOR
IDARON	0015.076396 /2022-11	Renovar Antivirus	1200	36 Meses	R$ 252.996,00
SEFIN	0030.065871/2022-35	Renovar Antivirus	900	36 Meses	R$ 141.696,00
DER	0009.068736/2022-19	Renovar Antivirus	500	36 Meses	R$ 61.720,00
SEOSP	0069.000418/2023-27	Aquisição Antivírus	300	36 Meses	R$ 47.232,00

8. PORTAL DO SOFTWARE PÚBLICO

8.1. O Software Público Brasileiro é um tipo específico de software livre que atende às necessidades de modernização da administração pública. Há no portal 69 (sessenta e nove) sistemas, no entanto, não foram identificados softwares que possam atender às necessidades dos setores demandantes.

9. ESTIMATIVAS PRELIMINARES DE PREÇO

9.1. As estimativas preliminares de preço foram feitas considerando contratos de objetos semelhantes firmados por entes públicos nos últimos 02 anos. Nesse sentido, os objetos foram listados nas planilhas abaixo:

9.2. Atualmente o Iperon utiliza a versão "kaspersky Endpoint Security for Business Advanced", que atualmente está descontinuada pelo fabricante, e considerando todas as especificações técnicas, a que mais de adequa a necessidade do instituto seria a versão **"kaspersky Next EDR Optimum Plus"**

9.3. Em consulta junto à fornecedores de endpoint obtivemos os seguintes valores:

PROPOSTA - VALORES DO LICENCIAMENTO PROTEÇÃO NEXT EDR – CONSOLE EM NUVEM OU ON-PREMISE					
Item	**Descrição**	**Unid.**	**Quant.**	**Valor Unitário(R$)**	**Valor Total (R$)**
1	Licenças de Antivírus Corporativo *Kaspersky* Kaspersky Next EDR **Optimum** – *PLUS - Suporte do Fabricante* ***(36 meses de garantia).***	Licença	400	R$473,87	R$189.548,00
2	Licenças de Antivírus Corporativo *Kaspersky* Next EDR **Foundation** – *PLUS – Suporte do Fabricante* ***(36 meses de garantia)***.	Licença	400	R$359,06	R$143.624,00
3	Licenças de Antivírus Corporativo *Kaspersky Endpoint Security for Business* ***ADVANCED*** *– PLUS – Suporte do Fabricante* ***(36 meses de garantia)*** – ***PRODUTO DESCONTINUADO – APENAS PARA REFERÊNCIA***	Licença	400	R$342,35	R$136.940,00
4	Treinamento remoto na Proteção de Endpoints fornecida, para turma de até 3 (três) alunos, incluido 16 (dezesseis) horas de serviços de instalação dos módulos novos.	Serviço	1	R$18.000,00	R$18.000,00

9.4. Diante dos valores acima, a estimativa de custo para a presente contratação para **36 (Trinta e Seis) meses**) ficaria da seguinte forma:

LOTE	ITEM	OBJETO	UNIDADE DE MEDIDA	CATSERV	QTD	VLR UNITÁRIO	VLR TOTAL

1	1	**Aquisição de subscrição** de Proteção de Endpoints (Antivírus) com implementação, atualização e suporte técnico por **36 (Trinta e Seis) meses**)	Licença	27502	400	473,87	189.548,00
	2	**Treinament**o remoto na Proteção de Endpoints fornecida no item 1, para turma de até 3 (três) alunos, incluíndo 16 (dezesseis) horas de serviços de **instalação dos módulos novos.**	Turma	17256	1	18.000,00	18.000,00
VALOR TOTAL DA AQUISIÇÃO							207.548,00

9.5. Diante das demonstrações acima, a contratação em questão está estimada em **R$ 207.548,00 (duzentos e sete mil quinhentos e quarenta e oito reais).**

10. AS NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE DO ÓRGÃO OU ENTIDADE PARA VIABILIZAR A EXECUÇÃO CONTRATUAL (EXEMPLO: MOBILIÁRIO, INSTALAÇÃO ELÉTRICA, ESPAÇO ADEQUADO PARA PRESTAÇÃO DO SERVIÇO, ETC)

10.1. Reforçamos que manter o software Kaspersky não terá impacto nos itens infraestrutura tecnológica, e logística de implantação, tais como:

10.2. **Infraestrutura tecnológica:** Não há necessidade de adequação da infraestrutura tecnológica do Iperon.

10.3. **Infraestrutura elétrica:** Não se aplica.

10.4. **Logística de implantação:** Não se aplica.

10.5. **Espaço físico:** Não se aplica.

10.6. **Mobiliário:** Não se aplica.

10.7. **Impacto ambiental:** Não se aplica.

11. POSSÍVEIS IMPACTOS AMBIENTAIS

11.1. As licenças de software são contratadas com base na funcionalidade, desempenho, custo e suporte técnico oferecido pelo produto, portanto questões ambientais não são aplicáveis ao objeto em questão.

12. BENEFÍCIOS A SEREM ALCANÇADOS

12.1. Proteger os dispositivos e dados da instituição, contra ameaças conhecidas e avançadas, como ransomware, malware e ataques de dia zero;

12.2. Detectar, entender e responder a ataques sofisticados, realizando análise de causa raiz e remediação;

12.3. Economizar recursos e simplificar o gerenciamento de soluções de Segurança da Informação;

12.4. Garantir a conformidade com as normas e regulamentos de segurança cibernética do setor público.

13. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

13.1. Considerando o artigo 40, § 3º, inciso II e III da lei 14133, o parcelamento da solução não será adotado por representar risco à implantação do objeto a ser contratado (proteção de rede adotada no parque computacional do Iperon, além do mesmo ser configurado como sistema único e integrado.

13.2. A padronização almejada também requer a indicação de marca, de modo que o fornecimento do objeto leva a fabricante único.

14. ANALISE DE RISCO E GRAVIDADE DAS CONSEQUÊNCIAS

14.1. O mapa de risco está disposto no anexo ID 0045947969

15. JUSTIFICATIVA PARA A EXCLUSÃO DE PARTICIPAÇÃO DE PESSOAS FÍSICAS NA LICITAÇÃO

15.1. A exclusão de participação de Pessoas Físicas pode ser respaldada pela necessidade de garantir a qualidade, durabilidade e conformidade dos produtos adquiridos.

15.2. Pessoas Jurídicas, muitas vezes, possuem uma estrutura mais sólida para atender às exigências técnicas e de fornecimento em larga escala. Além disso, a capacidade financeira das empresas contribui para a oferta de garantias contratuais e assegura a disponibilidade de recursos para atender às demandas da Administração Pública.

15.3. Ao restringir a participação a entidades jurídicas, busca-se fomentar a competitividade entre empresas que possuam a expertise necessária para fornecer licenças de endpoint (antivírus) de alta qualidade, contribuindo para a eficácia do processo licitatório e a satisfação das necessidades da instituição contratante. Essa medida visa a otimização dos recursos públicos e a garantia de uma aquisição que atenda aos padrões de desempenho e durabilidade requeridos.

16. DECLARAÇÕES DE VIABILIDADE OU NÃO DA CONTRATAÇÃO

16.1. Após estudo e análise por parte da equipe de planejamento, **verificou-se, por todo exposto no estudo técnico, a viabilidade da contratação** para atender as necessidades do Iperon no intuito prover tecnologia da informação e comunicação, TIC, para o fornecimento de solução de endpoint para os equipamentos de TIC do instituto.

16.2. Os levantamentos realizados neste Estudo Técnico Preliminar – ETP **estão alinhados com os requisitos tecnológicos atualmente utilizados no Iperon** e estabelecem uma relação de paridade com as demandas do instituto.

16.3. Benefícios Diretos e Indiretos que Resultarão da Aquisição: segurança cibernética no ambiente tecnológico do Iperon.

Porto Velho, data e hora do sistema.

ELABORADO POR

GABRIEL VAZ SEVERO
Assessor

REVISADO POR

EZEQUIEL NASCIMENTO DA SILVA
Assessor

APROVADO POR

RUDNY WALLAS ALVES
Diretor de Tecnologia da Informação e Comunicação - DTIC/Iperon

Documento assinado eletronicamente por **Gabriel Vaz Severo**, **Analista**, em 13/05/2024, às 13:00, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **EZEQUIEL NASCIMENTO DA SILVA** , **Assessor(a)**, em 13/05/2024, às 13:02, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **Rudny Wallas Alves**, **Diretor(a)**, em 13/05/2024, às 13:02, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0048519972** e o código CRC **E2D87C36**.

Referência: Caso responda este(a) Estudo Técnico Preliminar, indicar expressamente o Processo nº 0016.000487/2024-37 SEI nº 0048519972

GOVERNO DO ESTADO DE RONDÔNIA
Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - IPERON

SAMS

Órgão Solicitante: **Instituto de Previdência dos Servidores Públicos do Estado de Rondônia (Iperon)** Processo n. 0016.000487/2024-37 - Contratação de **subscrição de** Soluções de Segurança Avançada de Endpoints (Antivírus). Fonte do Recurso: 1.802.0.00001; – Arrecadação Própria Indireta Programa de Trabalho: 09.126.1000.2064. Natureza da Despesa: 33.90.40; Exposição de Motivo: Atender ao Iperon

ITEM	ESPECIFICAÇÃO	CATSERV	UNID.	QUANT.	MARCA	VALOR UNITÁRIO	VALOR TOTAL
01	Aquisição de subscrição de Proteção de Endpoints (Antivírus) com implementação, atualização e suporte técnico por **36 (trinta e seis) meses**	27502	LICENÇA	400			
02	**Serviço de treinamento** da solução de segurança avançada de endpoints (Antivírus) especificada no Item 1, que atenda uma turma com até 03 (três) alunos, incluindo 16 (dezesseis) horas de serviços de instações dos módulos novos.	20052	TURMA	01			
OBS.							

Carimbo do CNPJ/CPF-ME	**Local:**	**Responsável para Cotação da Empresa:**	**USO EXCLUSIVO DO ÓRGÃO COTANTE**	**Valor Da Proposta**
	Data:	**Fone:**	**Responsável pela Cotação**	**Validade Da Proposta**
	Banco: **Agência:** **C/C:**	**Assinatura**	**Nome do Servidor:** **Matrícula Nº**	**Prazo De Entrega**

OBS: As empresas vencedoras deverão apresentar no ato da entrega do objeto, juntamente com a Nota Fiscal/Fatura, os seguintes documentos: Certidões Negativas de Débitos junto ao INSS. Certidões Negativas de Débitos junto ao FGTS. Certidões Negativas de Débitos Trabalhistas. Certidões Negativas de Débito junto a Fazenda Pública. Certidões Negativas de Débitos Estaduais. Certidões Negativas de Débitos Municipais.

TIAGO CORDEIRO NOGUEIRA
Presidente do Iperon

Documento assinado eletronicamente por **Tiago Cordeiro Nogueira**, **Presidente**, em 10/06/2024, às 16:43, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0049290260** e o código CRC **95330ADC**.

Governo do Estado de RONDÔNIA

Superintendência Estadual de Compras e Licitações
Coordenadoria de Pesquisa e Análise de Preços

ITEM	DESCRIÇÃO	UNID	QUANT.(A)	EMP 1	EMP 2	EMP 3	EMP 4	EMP 5	PREÇO MÍNIMO (D)	PREÇO MÉDIO (E)	PREÇO MEDIANO (F)	DESVIO PADRÃO	COEFICIENTE DE VARIAÇÃO	PARAMETRO UTILIZADO (MÍNIMO/MÉDIO)	SUBTOTAL GERAL [F + G]
LOTE ÚNICO															
1	**Aquisição de subscrição de Proteção de Endpoints (Antivírus) com implementação, atualização e suporte técnico por 36 (trinta e seis) meses**	**LICENÇAS**	**400**	365,00	386,70	457,50	R$ 379,90	490,00	R$ 365,00	**R$ 415,82**	R$ 386,70	**54,68**	**13,15%**	**MÉDIO**	**R$ 166.328,00**
2	**Serviço de treinamento da solução de segurança avançada de endpoints (Antivírus) especificada no Item 1, que atenda uma turma com até 2 alunos de 12 horas.**	**TURMAS**	**1**	20.000,00	19.000,00	16.332,09	NC	20.700,00	R$ 16.332,09	**R$ 19.008,02**	R$ 19.500,00	**1.915,51**	**10,08%**	**MÉDIO**	**R$ 19.008,02**
VALOR DO LOTE ÚNICO															**R$ 185.336,02**

VALOR TOTAL	**R$ 185.336,02**
VALOR DO LOTE ÚNICO	**R$ 185.336,02**

LEGENDA:
NC = Não encontrado

NOTA EXPLICATIVA: FOI EFETUADO O CÁLCULO PARA A EQUIVALÊNCIA DOS PREÇOS DE 24 PARA 36 MESES

IDENTIFICAÇÃO DAS COTAÇÕES
EMP1 BANCO DE PREÇOS
EMP2 BANCO DE PREÇOS
EMP3 BANCO DE PREÇOS
EMP4 ATA DE REGISTRO DE PREÇOS Nº 01/2024 - ITI
EMP5 MICROHARD - CNPJ: 42.832.691/0001-30

1) As descrições foram reduzidas neste quadro comparativo, porém se encontra completas no termo de referência ().

GOVERNO DO ESTADO DE RONDÔNIA
Instituto de Previdência dos Servidores Públicos do Estado de Rondônia - IPERON

MAPA DE RISCO

1. INFORMAÇÕES BÁSICAS

1.1. Objeto da Matriz de Riscos: Aquisição de subscrição de Proteção de Endpoints com implementação e suporte técnico por 60 (sessenta) meses, incluindo treinamento para turma de alunos.

2. RISCOS IDENTIFICADOS

NÚMERO	RISCO	CAUSA	FASE	PORTABILIDADE	IMPACTO
R-01	Escolha da solução ineficaz e ou descrição dos serviços de forma incompleta	Falta de conhecimento técnico da área demandante	Planejamento	Baixa	Alto
Impactos					
01	Valor de referência equivocado, frustrando o certame ou gerando contratação com sobre preço				
Ações Preventivas					
P-01	Qualificação dos servidores da área demandante				**Responsáveis**: DTIC
P-02	Levantamento técnico com fornecedores do mercado e com outros órgãos publico				**Responsáveis**: DTIC
Ações de Contingência					
C-01	Reparação do ETP e TR com atualizações das informações necessárias e retificação do edita				**Responsáveis**: DTIC e EQCOM

NÚMERO	RISCO	CAUSA	FASE	PORTABILIDADE	IMPACTO
R-02	Licitação deserta ou fracassada	Não haver fornecedores interessados ou não atenderem as exigências do TR	Seleção do Fornecedor	Médio	Médio
Impactos					
01	Prejuízo no planejamento				
Ações Preventivas					
P-01	Verificar a existência de empresas interessadas no objeto da licitação				
P-02	Assegurar que seja realizada ETP com antecedência para verificar todos os critérios técnicos da contratação				**Responsáveis:** DTIC
Ações de Contingência					

C-01	Refazer o ETP e TR solicitando uma nova licitação	**Responsáveis:** DTIC e EQCOM

NÚMERO	RISCO	CAUSA	FASE	PORTABILIDADE	IMPACTO
R-03	Estimativa de preço	ETP e TR com informações que não refletem os valores praticados no mercado	Planejamento	Baixo	Médio
Impactos					
1	Valor de referência equivocado				
Ações Preventivas					
P-01	Elaborar as estimativas de preço conforme determinado na IN 65/2022				**Responsáveis:** EQCOM
Ações de Contingência					
C-01	Suspensão do processo licitatório				**Responsáveis:** EQCOM e SUPEL
C-02	Realização de cotação de preço				**Responsáveis:** EQCOM e SUPEL

NÚMERO	RISCO	CAUSA	FASE	PORTABILIDADE	IMPACTO
R-04	Serviço prestado de forma insatisfatória	Contratada não apta a cumprir os serviços licitados	Gestão de Contrato	Baixa	Alto
Impactos					
1	Interrupção do serviço				
Ações Preventivas					
P-01	Gestão e fiscalização efetiva dos serviços prestados, a fim de prevenir possíveis problemas				**Responsáveis:** DTIC e GAD
P-02	Prever no TR documentos que comprove a capacidade técnica da empresa a ser contratada				**Responsáveis:** DTIC e EQCOM
P-03	Prever no TR aplicação de sanções				**Responsáveis:** EQCOM
Ações de Contingência					
C-01	Formalização de notificação e aplicação de sanções previstas no instrumento licitatório.				**Responsáveis:** DTIC e GAD

NÚMERO	RISCO	CAUSA	FASE	PORTABILIDADE	IMPACTO
R-05	Não formalização do contrato ou não renovação contratual	Fornecedor não aceita a renovação contratual	Gestão de Contrato	Baixo	Médio
Impactos					
1	Necessidade de novo processo licitatório				

Ações Preventivas		
P-01	Entrar em contato com a Contratada com antecedência mínima de 03 meses antes do término do contrato	**Responsáveis:** DTIC e GAD
Ações de Contingência		
C-01	Formalização de novo processo licitatório	**Responsáveis:** DTIC e GAD
C-02	Rescisão contratual com ou sem aplicação de sanções	**Responsáveis:** GAD

NÚMERO	RISCO	CAUSA	FASE	PORTABILIDADE	IMPACTO
R-06	Falta de recurso financeiro	Falta de disponibilidade orçamentária durante a execução contratual	Planejamento	Baixa	Médio
Impactos					
1	Necessidade de novo processo licitatório				
Ações Preventivas					
P-01	Planejamento na fase interna da licitação				**Responsáveis:** DTIC e GAD
P-02	Obter orçamentos fidedignos				**Responsáveis:** DTIC e COPLAG
Ações de Contingência					
C-01	Realização de remanejamento orçamentário para acobertar a prestação do serviço				**Responsáveis:** COPLAG

NÚMERO	RISCO	CAUSA	FASE	PORTABILIDADE	IMPACTO
R-07	Fiscalização deficiente	Falta de acompanhamento dos serviços	Gestão de Contrato	Baixa	Médio
Impactos					
1	Entrega de serviço abaixo da qualidade contratada				
Ações Preventivas					
P-01	Promover curso para os fiscais e gestores de contratos				**Responsáveis:** DAF
P-02	Nomear servidores que possuam capacidade técnica para exercer tal função				**Responsáveis:** DTIC e GAD
Ações de Contingência					
C-01	Adotar uso de documentos de controle				**Responsáveis:** DTIC e GAD

3. MATRIZ DE RISCO

MATRIZ DE RISCO						
	Muito Alto 5					

IMPACTO (I)	Alto 4					
	Médio 3			R-02		
	Baixo 2			R-03 R-05 R-06 R-07	R-01 R-04	
	Muito Baixo 1					
		Muito Baixa 1	Baixa 2	Média 3	Alta 4	Muito Alta 5
		PROBABILIDADE (P)				

ESCALA PARA CLASSIFICAÇÃO DE NÍVEIS DE RISCO			
RB (Risco Baixo)	**RM** (Risco Médio)	**RA** (Risco Alto)	**RE** (Risco Extremo)
1 - 4	**5 - 10**	**12 - 16**	**20 - 25**

Porto Velho, data e hora do sistema.

ELABORADO POR

GABRIEL VAZ SEVERO
Assessor

APROVADO POR

RUDNY WALLAS ALVES
Diretor de Tecnologia da Informação e Comunicação - DTIC/Iperon

Documento assinado eletronicamente por **Gabriel Vaz Severo**, **Analista**, em 19/02/2024, às 12:05, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **Rudny Wallas Alves**, **Diretor(a)**, em 19/02/2024, às 13:49, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0045947969** e o código CRC **B80211AE**.