

§ 2º Fica designado como pregoeiro substituto o servidor indicado no inciso II, alínea *a*), deste artigo, o qual desempenhará as atividades de estilo da pregoeira em suas ausências ou impedimentos legais.

Art. 2º Esta portaria entra em vigor na data de sua publicação, com efeitos retroativos a contar do dia 22 de abril de 2025, para os incisos atualizados por este ato normativo. As demais disposições em contrário ficam revogadas.

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

**Márcia Rocha de Oliveira Francelino**

Superintendente Estadual de Compras e Licitações (SUPEL/RO)

Protocolo 0060011817

Portaria nº 74 de 12 de maio de 2025

Altera a Portaria n.º 60, que reformula as equipes de licitações e designa servidores para compor a Comissão de Educação, Cultura, Lazer e Turismo, no âmbito da Superintendência Estadual de Compras e Licitações – SUPEL/RO.

A 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 a Portaria 63/2025 (0059510290) que institui a Comissão de Educação, Cultura, Lazer e Turismo, no âmbito da Superintendência de Compras e Licitações do Estado de Rondônia - SUPEL/RO, com objetivo de aplicar celeridade e eficiência na tramitação de processos de compras públicas; e

CONSIDERANDO a necessidade de reestruturação organizacional das atividades relacionadas à condução de certames no âmbito da Superintendência Estadual de Compras e Licitações – SUPEL,  
RESOLVE:

**Art. 1º** Reformular no âmbito do Sistema Eletrônico de Informações (SEI) a Equipe de Licitação (SUPEL-ÔMEGA), instituída para atuação interna no âmbito da Superintendência Estadual de Compras e Licitações, denominada Comissão de Educação, Cultura, Lazer e Turismo (SUPEL-COEDU) e designa os servidores abaixo relacionados para sua composição:

I - Agente de contratação:

a) Roger Martins Cardoso, matrícula n.º \*\*\*\*\*961.

II - Equipe de Apoio:

a) Josélia Pagani Ferreira, matrícula n.º \*\*\*\*\*627.

b) Suélen Torres da Silva, matrícula n.º \*\*\*\*\*853; e

c) Franciara Sobrinho do Nascimento Ximenes, matrícula n.º \*\*\*\*\*832.

§ 1º O servidor indicado no inciso I, alínea *a*), atuará como pregoeiro, sempre que a modalidade de licitação escolhida for pregão eletrônico, conforme previsto no art. 8º, § 5º da Lei Federal nº 14.133/2021.

§ 2º Fica designada como pregoeira substituta a servidora indicada no inciso II, alínea *a*), deste artigo, a qual desempenhará as atividades de estilo do pregoeiro em suas ausências ou impedimentos legais.

Art. 2º Esta portaria entra em vigor na data de sua publicação, com efeitos retroativos a contar do dia 22 de abril de 2025, para os incisos atualizados por este ato normativo. As demais disposições em contrário ficam revogadas.

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

**Márcia Rocha de Oliveira Francelino**

Superintendente Estadual de Compras e Licitações (SUPEL/RO)

Protocolo 0060060731

Portaria nº 75 de 13 de maio de 2025

Altera a Portaria n.º 59, que reformula as equipes de licitações e designa servidores para compor a Comissão Especial de Licitações, no âmbito da Superintendência Estadual de Compras e Licitações – SUPEL/RO.

A 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 a Portaria 63/2025 (0059510290) que institui a Comissão Especial de Licitações, no âmbito da Superintendência de Compras e Licitações do Estado de Rondônia - SUPEL/RO, com objetivo de aplicar celeridade e eficiência na tramitação de processos de compras públicas; e

CONSIDERANDO a necessidade de reestruturação organizacional das atividades relacionadas à condução de certames no âmbito da Superintendência Estadual de Compras e Licitações – SUPEL,

**RESOLVE:**

**Art. 1º** Reformular no âmbito do Sistema Eletrônico de Informações (SEI) a Equipe de Licitação (SUPEL-CEL), instituída para atuação interna no âmbito da Superintendência Estadual de Compras e Licitações, denominada Comissão Especial de Licitações (SUPEL-COESP) e designa os servidores abaixo relacionados para sua composição:

I - Agente de contratação:

a) Bruna Gonçalves Apolinário, matrícula n.º \*\*\*\*\*033.

II - Equipe de Apoio:

a) Letícia Helen Almeida Ferreira, matrícula n.º \*\*\*\*\*088; e

b) Jessica Saraiva Guimarães, matrícula n.º \*\*\*\*\*606.

§ 1º A servidora indicada no inciso I, alínea a), atuará como pregoeira, sempre que a modalidade de licitação escolhida for pregão eletrônico, conforme previsto no art. 8º, § 5º da Lei Federal nº 14.133/2021.

§ 2º Fica designada como pregoeira substituta a servidora indicada no inciso II, alínea a), deste artigo, a qual desempenhará as atividades de estilo da pregoeira em suas ausências ou impedimentos legais.

Art. 2º Esta portaria entra em vigor na data de sua publicação, com efeitos retroativos a contar do dia 22 de abril de 2025, para os incisos atualizados por este ato normativo. As demais disposições em contrário ficam revogadas.

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

**Márcia Rocha de Oliveira Francelino**

Superintendente Estadual de Compras e Licitações (SUPEL/RO)

Protocolo 0060098744

Portaria nº 76 de 13 de maio de 2025

Altera a Portaria n.º 57, que reformula as equipes de licitações e designa servidores para compor a Comissão de Segurança Pública, no âmbito da Superintendência Estadual de Compras e Licitações – SUPEL/RO.

A 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 a Portaria 63/2025 (0059510290) que institui a Comissão de Segurança Pública, no âmbito da Superintendência de Compras e Licitações do Estado de Rondônia - SUPEL/RO, com objetivo de aplicar celeridade e eficiência na tramitação de processos de compras públicas; e

CONSIDERANDO a necessidade de reestruturação organizacional das atividades relacionadas à condução de certames no âmbito da Superintendência Estadual de Compras e Licitações – SUPEL,

**RESOLVE:**

**Art. 1º** Reformular no âmbito do Sistema Eletrônico de Informações (SEI) a Equipe de Licitação (SUPEL-ALFA), instituída para atuação interna no âmbito da Superintendência Estadual de Compras e Licitações, denominada Comissão de Segurança Pública (SUPEL-COSEG) e designa os servidores abaixo relacionados para sua composição:

I - Agente de contratação:

a) Nadiane da Costa Laia, matrícula n.º \*\*\*\*\*769.

II - Equipe de Apoio:

a) Matheus Breves Chixaro Lobo, matrícula n.º \*\*\*\*\*032; e

b) Ingrid Tainara Xavier Pedroza, matrícula n.º \*\*\*\*\*608.

§ 1º A servidora indicada no inciso I, alínea a), atuará como pregoeira, sempre que a modalidade de licitação escolhida for pregão eletrônico, conforme previsto no art. 8º, § 5º da Lei Federal nº 14.133/2021.

§ 2º Fica designado como pregoeiro substituto o servidor indicado no inciso II, alínea a), deste artigo, o qual desempenhará as atividades de estilo da pregoeira em suas ausências ou impedimentos legais.

Art. 2º Esta portaria entra em vigor na data de sua publicação, com efeitos retroativos a contar do dia 22 de abril de 2025, para os incisos atualizados por este ato normativo. As demais disposições em contrário ficam revogadas.

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

**Márcia Rocha de Oliveira Francelino**

Superintendente Estadual de Compras e Licitações (SUPEL/RO)

Protocolo 0060101929

Portaria nº 77 de 13 de maio de 2025

Altera a Portaria n.º 51, que reformula as equipes de licitações e designa servidores para compor a 4ª Comissão de Saúde, no âmbito da Superintendência Estadual de Compras e Licitações – SUPEL/RO.



**GOVERNO DO ESTADO DE RONDÔNIA**  
Superintendência Estadual de Compras e Licitações - SUPEL  
Comissão Especial de Licitações - SUPEL-COESP

**INSTRUMENTO CONVOCATÓRIO**

**PREGÃO ELETRÔNICO Nº 90077/2025/SUPEL/RO**

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

**RESUMO DOS DADOS**

<b>ABERTURA DA SESSÃO PÚBLICA: 30/05/2025, às 10h</b> (horário de Brasília) sítio: <a href="http://www.comprasgovernamentais.gov.br">http://www.comprasgovernamentais.gov.br</a> .	Limite para esclarecimentos e impugnações ao edital: <b>26/05/2025</b> .
---	--

OBJETO	
Contratação de empresa para fornecimento de <b>solução de proteção para estações de trabalho e servidores contra ataques cibernéticos</b> , visando atender as necessidades básicas da Secretaria de Estado do Desenvolvimento Ambiental – SEDAM.	
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 : 0028.020065/2024-49	
UASG: 925373 ENDEREÇO ELETRÔNICO : <a href="https://www.gov.br/compras/pt-br">https://www.gov.br/compras/pt-br</a> .	
VALOR ESTIMADO DA CONTRATAÇÃO	
ORÇAMENTO ANUAL	R\$ 586.087,90 (quinhentos e oitenta e seis mil, oitenta e sete reais e noventa centavos)
VISTORIA	INSTRUMENTO CONTRATUAL
Não aplicável	Contrato

DOCUMENTOS DE HABILITAÇÃO ( INFORMAR ITEM DO ANEXO I)		
<b>Requisitos Básicos:</b> <b>1. Habilitação jurídica:</b> Conforme estabelecido no <u>item 16.3 do Termo de Referência</u> . <b>2. Qualificação econômico e financeira:</b> Conforme estabelecido no <u>item 16.5 do Termo de Referência</u> . <b>3. Regularidade Fiscal, social e trabalhista:</b> Conforme estabelecido nos <u>itens 16.6 e 16.7 do Termo de Referência</u> . <b>4. Qualificação técnica:</b> Conforme estabelecido no <u>item 16.4 do Termo de Referência</u> .		<b>Requisitos Específicos:</b>
<b>CONTRATAÇÃO EXCLUSIVA ME/EPP?</b>	<b>RESERVA COTA ME/EPP?</b>	<b>EXIGE AMOSTRA/DEMONSTRAÇÃO?</b>
Não	Não	Não
<b>CRITÉRIO DE JULGAMENTO</b>	<b>MODO DE DISPUTA</b>	<b>CONTRATAÇÃO OU AQUISIÇÃO</b>
Menor Preço por Lote	Aberto	Contratação
<b>TELEFONES PARA CONTATO</b>		<b>E-MAIL PARA CONTATO:</b>
Telefone: 69.3212-9243		<a href="mailto:cel@supel.ro.gov.br">cel@supel.ro.gov.br</a>
<b>OBSERVAÇÕES GERAIS:</b>		
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 <b>90000</b> antes do número do certame. (ex.: <b>90001/2024</b> )		

SUMÁRIO

- 1. DO PREÂMBULO;
- 2. DO OBJETO;
- 3. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO;
- 4. DAS CONDIÇÕES DE PARTICIPAÇÃO;
- 5. DO BENEFÍCIO ÀS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE;
- 6. DO REGISTRO DA PROPOSTA NO SISTEMA ELETRÔNICO;
- 7. DA FORMULAÇÃO DE LANCES, CONVOCAÇÃO ME/EPP E CRITÉRIO DE DESEMPATE;
- 8. A FASE DE NEGOCIAÇÃO E JULGAMENTO DA PROPOSTA DE PREÇOS;
- 9. DA FASE DE HABILITAÇÃO;
- 10. DO RECURSO;

11. DA HOMOLOGAÇÃO;
12. DA REVOGAÇÃO E DA ANULAÇÃO;
13. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES;
14. DA DOTAÇÃO ORÇAMENTÁRIA;
15. DAS DISPOSIÇÕES GERAIS;
16. DOS ANEXOS;

## 1. DO PREÂMBULO

**1.1. A SUPERINTENDÊNCIA ESTADUAL DE LICITAÇÕES**, por meio da **Portaria nº 75 de 13 de maio de 2025**, torna público que se encontra autorizada a realização da licitação na modalidade de **PREGÃO**, na forma **ELETRÔNICA**, sob o nº **90077/2025/SUPEL/RO**, do tipo **MENOR PREÇO POR LOTE ÚNICO**, 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 interessada a Secretaria de Estado do Desenvolvimento Ambiental - SEDAM.

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 contratação de empresa para fornecimento de **solução de proteção para estações de trabalho e servidores contra ataques cibernéticos**, visando atender as necessidades básicas da Secretaria de Estado do Desenvolvimento Ambiental – SEDAM, 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 4 e seus subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

**2.4. Da garantia do objeto:** Ficam aquelas estabelecidas no item 15 e seus subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

**2.5 Das condições contratuais/garantia do contratual:** Ficam aquelas estabelecidas nos itens 28 e 31 e seus subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

**2.6. Do reajuste e supressão contratual:** Ficam aquelas estabelecidas nos itens 29 e 30 e seus subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

**2.7. Da fiscalização e acompanhamento do recebimento/execução do objeto:** Ficam aquelas estabelecidas no item 19 e seus subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

**2.8. Da entrega/recebimento:** Ficam aquelas estabelecidas no item 13 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 18 e subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

**2.10. Da obrigação da contratada:** 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.

**2.11. Da obrigação da contratante:** 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.

**2.12. Dos critérios de sustentabilidade:** Ficam aquelas estabelecidas no item 25 e subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

**2.13. Dos requisitos da contratação:** Ficam aquelas estabelecidas no item 6 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, 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: [cel@supel.ro.gov.br](mailto:cel@supel.ro.gov.br);

3.1.2. Após o envio do e-mail, a licitante deverá certificar-se quanto à confirmação de recebimento pelo Núcleo de Atendimento desta Superintendência, para não tornar sem efeito, pelo telefone **(069) 3212-9243** ou ainda, concomitantemente, caso julgue necessário, protocolar o original presencialmente na SUPEL, 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 da Lei 14.133/2021.

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 (<https://www.gov.br/compras/pt-br>), por meio de Certificado Digital conferido pela Infraestrutura de Chaves Públicas Brasileira – ICP – Brasil.

4.2. Os licitantes deverão obedecer rigorosamente aos termos deste Edital e de seus anexos.

4.2.1. Ante eventual ausência de regramento específico em Edital, deverão ser observados



os inseridos no Termo de Referência, sempre pautando-se na legislação vigente.

4.3. 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, excluía 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.

4.4. 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 que se tornem desatualizados.

4.5. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

**4.6. Não poderão disputar esta licitação, direta ou indiretamente:**

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

4.6.2. 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:

4.6.2.1. 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;

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

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

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

4.6.5. Agente público de órgão ou entidade licitante ou contratante, conforme [§§ 1º e 2º do art. 9º da Lei nº 14.133, de 2021](#).

4.6.6. **Pessoas jurídicas reunidas em consórcio** observar o art. 15 da Lei n. 14.133, de 2021 e disposição constante no item 24.1 do Anexo I - Termo de Referência.

4.6.7. **Da subcontratação:** Ficam aquelas estabelecidas no item 21.1 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, em campo próprio, caso se enquadre, que cumpre os requisitos estabelecidos no [artigo 3º 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.

5.2.3. A empresa de pequeno porte que, no ano-calendário, exceder o limite de receita bruta anual, previsto no inciso II, do caput do artigo 3º da Lei Complementar n. 123/06, fica excluída, no mês subsequente à ocorrência do excesso, do tratamento jurídico diferenciado, bem como do regime de que trata o art. 12, para todos os efeitos legais, ressalvado o disposto nos §§9º-A, 10 e 12, da mesma LC 123/06.

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. DO REGISTRO DA PROPOSTA NO SISTEMA ELETRÔNICO**

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.

6.2. O licitante deverá registrar sua proposta, no sistema eletrônico, com os 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.

6.2.1. A licitante deverá preencher o campo "marca" apenas com a marca específica do produto que deseja ofertar, sob pena de ser desclassificada caso não esteja de acordo.

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 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.

6.7. Quando da inclusão do anexo da proposta no sistema eletrônico, as empresas deverão fornecer as informações necessárias para a identificação da proposta em conformidade com o item 23 do Anexo I deste Edital - Termo de Referência, que somente será pública após a fase de lances.

## **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 **UNITÁRIO** 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 de 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 inexecutável.

7.7. O procedimento seguirá de acordo com o modo de disputa **aberto**, conforme item 32.2 do Anexo I deste Edital - Termo de Referência,



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](#), nesta ordem:

a) disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

b) avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos na Lei nº 14.133, de 2021;

c) desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

d) desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

7.10. Persistindo o empate, será realizado sorteio em sessão pública entre as propostas empatadas.

7.11. Na hipótese do subitem 7.10, a sessão pública de sorteio será efetuada de forma presencial, podendo qualquer interessado participar, sendo transmitida em canal oficial da Superintendência Estadual de Compras e Licitações - SUPEL, sendo observado os procedimentos, a saber:

a) Informação no chat da sessão pública quanto: data, hora e local da sessão para o procedimento de desempate das propostas, a ser realizado no site [Sorteador.com.br](#)! (ou outro compatível);

b) Por ordem alfabética, será disponibilizado a indicação dos nomes das licitantes, que se encontram em situação de propostas empatadas, no site indicado na alínea "a" do subitem 7.11;

c) A primeira licitante sorteada, será a primeira classificada. A sequência classificatória das propostas empatadas seguirá em ordem sucessiva;

d) A sessão será oficialmente encerrada após a conclusão desses procedimentos, e o registro audiovisual da sessão permanecerá para visualização no canal oficial da Superintendência Estadual de Compras e Licitações - SUPEL.

e) Haverá transmissão ao vivo da sessão do sorteio nos canais oficiais SUPEL: <https://www.youtube.com/@supelro5251> e <https://www.instagram.com/supelrondonia/>

f) Haverá lavratura de ata de sorteio, com presença de testemunhas, que será incluída no processo administrativo;

7.12. 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.

7.13 Nos itens/lotos destinados à exclusiva participação de Microempresas e Empresas de Pequeno Porte e equiparadas será concedida prioridade de contratação de microempresas e empresas de pequeno porte sediadas local ou regionalmente, até o limite de 10% (dez por cento) do melhor preço válido, nos termos previstos no Decreto Estadual nº 21.675/2017:

a) aplica-se o disposto neste subitem nas situações em que as ofertas apresentadas pelas microempresas e empresas de pequeno porte sediadas local ou regionalmente sejam iguais ou até 10% (dez por cento) superior ao menor preço;

b) a microempresa ou a empresa de pequeno porte sediada local ou regionalmente melhor classificada poderá apresentar proposta de preço inferior àquela considerada vencedora da licitação, situação em que poderá ser adjudicado o objeto em seu favor;

c) na hipótese da não contratação da microempresa ou da empresa de pequeno porte sediada local ou regionalmente com base na alínea "b", serão convocadas as remanescentes que porventura se

enquadrem na situação da alínea "a", na ordem classificatória, para o exercício do mesmo direito;

d) no caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte sediadas local ou regionalmente, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta;

e) quando houver propostas beneficiadas com as margens de preferência para produto nacional em relação ao produto estrangeiro previstas no Decreto Estadual 21.675/2017, a prioridade de contratação prevista neste artigo será aplicada exclusivamente entre as propostas que fizerem jus às margens de preferência, de acordo com os Decretos de aplicação.

## **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. Sob análise do (a) Pregoeiro (a), poderá ser convocada 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.

8.3.1.1. Caberá ao licitante remeter no prazo estabelecido, exclusivamente via sistema Compras.gov, a proposta atualizada com o preço ou desconto, sob pena de desclassificação.

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 inexecutabilidade 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 nº 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. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no item XXX do Termo de Referência, sob pena de não aceitação da proposta.

8.8. A PROPOSTA DE PREÇOS, inserida no sistema de Compras.gov.br deverá estar de acordo com o [item 23 do Anexo I - termo de Referência](#).

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

apresentação.

8.9.1. A SUPEL solicitará às empresas, cujas propostas estiverem com prazo de vencimento inferior a **10 (dez) dias**, após declarada habilitada, para que façam a devida atualização com o intuito de dar celeridade ao processo de adjudicação e homologação pela Unidade Gestora.

8.9.2. As propostas com prazo de vencimento superior ao mencionado no item 8.9.1., serão enviadas imediatamente à Unidade Gestora sem a referida atualização temporal, para que se dê início ao procedimento homologatório.

8.9.2.1. Quando o processo for encaminhado para homologação juntamente com a proposta atualizada, cujo prazo de vencimento seja superior a 10 (dez) dias, ficará a cargo da SUPEL informar à Unidade o prazo em dias restante para o vencimento.

8.9.3. Decorrido o prazo de vencimento da proposta sem que a Unidade Gestora promova a homologação, a esta recai a responsabilidade de solicitar às licitantes a atualização.

8.9.4. O procedimento mencionado no item 8.9.1 será dispensado nos processos em que for certificada a necessidade de prioridade de tramitação, de modo que as propostas serão encaminhadas à Unidade Gestora para os atos de homologação, desde que dentro da validade, após finalizada a fase de habilitação.

8.10. Na ocasião da homologação, caso haja divergências entre o valor constante do documento da proposta, enviado pela licitante, e o valor final das negociações registradas no Termo de Julgamento, será considerado o registrado no para fins de homologação.

## **9. DA FASE DE HABILITAÇÃO**

9.1. Serão realizadas consultas, ao Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual - CAGEFIMP, instituído pela Lei Estadual 2.414, de 18 de fevereiro de 2011, ao Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS/CGU (Lei Federal 12.846/2013), Sistema de Cadastramento Unificado de Fornecedores - SICAF, Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça ([www.cnj.jus.br/improbidade\\_adm/consultar\\_requerido.php](http://www.cnj.jus.br/improbidade_adm/consultar_requerido.php)) e Lista de Inidôneos, mantida pelo Tribunal de Contas da União - TCU.

9.2. 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](#).

9.3. A DOCUMENTAÇÃO DE HABILITAÇÃO ANEXADA NO SISTEMA COMPRAS.GOV TERÁ EFEITO PARA TODOS OS ITENS, OS QUAIS A EMPRESA ENCONTRA-SE CLASSIFICADA.

9.4. 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.

9.5. 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.

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

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

9.8. O Pregoeiro, após 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 os documentos de habilitação.

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

9.9.1. 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

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

9.10. 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.

9.11. 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.

9.11.1. 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.

9.11.2. A prorrogação do prazo previsto no subitem 9.11.1 poderá ser concedida, a critério da Administração Pública, quando requerida pelo licitante, mediante apresentação de justificativa.

9.11.3. Ressalvado os documentos possíveis de verificação conforme item 9.4, os licitantes deverão encaminhar, nos termos deste Edital e anexos, a documentação relacionada nos itens a seguir, para fins de habilitação:

## **9.12. 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.

## **9.13. 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 nº 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.

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

#### **9.14. RELATIVOS À QUALIFICAÇÃO ECONÔMICA-FINANCEIRA**

9.14.1. Os critérios de qualificação econômico-financeira a serem atendidos pelo fornecedor serão aqueles estabelecidos no item 16.5 do Anexo I deste edital - Termo de Referência.

#### **9.15. RELATIVOS À QUALIFICAÇÃO TÉCNICA**

9.15.1. Os critérios de qualificação técnica a serem atendidos pelo fornecedor serão aqueles estabelecidos no item 16.4 do Anexo I – Termo de Referência deste Edital.

9.16. 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.

9.16.1. 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.

#### **9.17. DAS DECLARAÇÕES:**

9.17.1. As licitantes deverão dispor as seguintes declarações, exclusivamente em meio eletrônico, pela plataforma Compras.gov, não sendo necessária a juntada das mesmas com os demais documentos de habilitação/proposta:

a) Declaração de que atende aos requisitos de habilitação

b) Declaração, de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social.

c) Declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas previstos na CF/88, e demais legislações correlatas.

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

e) Declaração caso se enquadre, que cumpre os requisitos estabelecidos no artigo 3º da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49.

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.

g) Declaração do licitante de que, caso seja vencedor, contratará pessoas privadas de liberdade, em regime semiaberto ou egressos nos termos do Decreto nº 25.783, de 1º de fevereiro de 2021, que regulamenta a Lei Estadual nº 2.134, de 23 de julho de 2009, acompanhada de declaração emitida pela Gerência de Reinserção Social da Secretaria de Estado da Justiça - SEJUS, que dispõem acerca de pessoas aptas à execução de trabalho, no que couber.

h) Outras declarações eventualmente exigidas no Anexo I deste edital - Termo de Referência

9.18. As licitantes que deixarem de apresentar os documentos exigidos para a Habilitação ou os apresentar em desacordo com o estabelecido neste Edital, serão inabilitadas.

## **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 JULGAMENTO e 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, em cada fase.

10.1.1. A intenção de recorrer deverá ser registrada 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 terá efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

## **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 da unidade demandante 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 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 22 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 Secretaria de Estado do Desenvolvimento Ambiental, **Unidade Gestora SEDAM/RO**, conforme estabelecido no item 17 do Termo de Referência – Anexo I deste Edital.

### **15. DAS DISPOSIÇÕES GERAIS**

15.1. A qualquer momento, após a aceitação das propostas, poderão, os licitantes ser convocados a atualizar sua validade, no prazo de 2 (duas) horas, sob pena de desclassificação.

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

15.3. 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.

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

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

15.6. 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.

15.7. 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.

15.8. 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.

15.9. 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.

15.10. 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.

15.10.1. Fica o licitante incumbido de acompanhar todas as operações no sistema. Em caso de problemas técnicos/operacionais dentro da plataforma Compras.gov, deverá ser feita imediata manifestação pela empresa, direta e concomitantemente, à Superintendência Estadual de Compras e Licitações - SUPEL via telefone e/ou e-mail (ambos informados no resumo deste edital), sob pena de preclusão do direito de alegação em sede recursal.

15.11. 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/> e <https://www.gov.br/compras/pt-br>

15.12. Quando a desconexão do sistema eletrônico para o (a) Pregoeiro (a) persistir por tempo superior a 1 (uma) hora, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo (a) Pregoeiro (a) aos participantes, no sítio eletrônico utilizado para divulgação.

15.13. 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

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

**ANEXO I** - Termo de Referência (0059255807);

**ANEXO II** - Estudo Técnico Preliminar (0059485479);

**ANEXO III** - Mapa de de Risco (0055171825);

**ANEXO IV** - Modelo de Minuta de Contrato (0059625571);

**ANEXO V** - SAMS (0053337368);

**ANEXO VI** - Quadro Estimativo de Preços (0056463759).

Porto Velho/RO, data e hora do sistema.

**BRUNA GONÇALVES APOLINÁRIO**

Presidente da Comissão Especial de Licitações – COESP/SUPEL

Portaria nº 75 de 13 de maio de 2025

Mat. \*\*\*\*\*033

Elaborado por:

**Letícia Helen Almeida Ferreira**

Membro da Comissão Especial de Licitações – COESP/SUPEL

Portaria nº 75 de 13 de maio de 2025



Documento assinado eletronicamente por **Bruna Gonçalves Apolinário, Pregoeiro(a)**, em 15/05/2025, às 09:20, 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 **0060111104** e o código CRC **0A4792B5**.

**Referência:** Caso responda este Instrumento Convocatório, indicar expressamente o Processo nº 0028.020065/2024-49

SEI nº 0060111104



GOVERNO DO ESTADO DE RONDÔNIA  
Secretaria de Estado do Desenvolvimento Ambiental - SEDAM

TERMO DE REFERÊNCIA

1. IDENTIFICAÇÃO:

1.1. O presente Termo de Referência visa trazer a definição objetiva e elementos necessários para à aquisição **Contratação de empresa para fornecimento de solução de proteção para estações de trabalho e servidores contra ataques cibernéticos**, visando atender as necessidades básicas desta **Secretaria de Estado do Desenvolvimento Ambiental – SEDAM..**

2. DA INTRODUÇÃO LEGAL:

2.1. A contratação de pessoa jurídica para a prestação dos serviços deste objeto do presente Termo de Referência encontra amparo legal nos seguintes dispositivos:

2.2. Art. 6, inciso XXIII e XLI, da [Lei nº 14.133, de 01 de abril de 2021](#), conforme descrito abaixo:

- Art. 6º Para os fins desta Lei, consideram-se:
- XXII - obras, serviços e fornecimentos de grande vulto: aqueles cujo valor estimado supera R\$ 200.000.000,00 (duzentos milhões de reais);
- XLI - pregão: modalidade de licitação obrigatória para aquisição de bens e serviços comuns, cujo critério de julgamento poderá ser o de menor preço ou o de maior desconto;

2.3. Além disso, a presente contratação obedecerá aos ritos trazidos pelo art. 47, inciso XXI e art. 37 da Constituição Federal, bem como o disposto no Decreto Estadual nº 28.874 de 25 Janeiro de 2024 e Decreto 11.871 de 29 de Dezembro de 2023, que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.

2.4. Neste contexto, o respectivo Termo de Referência leva em consideração as regras e diretrizes para a aquisição no âmbito da Administração Pública do Poder Executivo Estadual, utilizando-se, normas e decisões pertinentes à nova Lei.

3. DA CARACTERIZAÇÃO DO OBJETO COMO COMUM:

3.1. O objeto desse Termo de Referência é comum, nos termos do art. 6º, inciso XIII da [Lei nº 14.133, de 01 de abril de 2021](#), visto que o referido objeto detém especificações técnicas conhecidas e utilizadas no mercado, sem variações que possam causar a necessidade de análises específicas e detalhada.

3.2. O presente objeto refuta qualquer descrição direcionada à marca, à modelo específico ou a qualquer característica suficiente para configurar restrição da competitividade licitatória, salvo nos casos em que for tecnicamente justificável, nos termos expressos do art. 41, inciso I, da [Lei nº 14.133, de 01 de abril de 2021](#).

4. CARACTERÍSTICAS DO OBJETO:

4.1. Especificações técnicas e quantitativas

LOTE	ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	CÓDIGO CATSER
LOTE ÚNICO	01	Solução de proteção avançada contra ataques cibernéticos para estações de trabalho (Extended detection and response - XDR)	Licenças	800	24333
	02	Solução de proteção avançada contra ataques cibernéticos para servidores (Extended detection and response - XDR)	Licenças	300	24333
	03	Serviços de suporte pro ativo, corretivo e para resposta a incidentes	Meses	60	5398
	04	Serviço de treinamento	UND	03	5398

5. DESCRIÇÃO DA SOLUÇÃO

5.1. A solução de segurança a ser contratada abrange proteção de Endpoint e proteção contra ataques avançados para usuário final, com todos os serviços necessários para uma implementação completa e eficaz. Essa solução deverá atender às necessidades específicas da Secretaria de Estado do Desenvolvimento Ambiental durante um período de 36 meses. Os componentes que compõem essa solução são os seguintes:

5.2. **SOLUÇÃO DE PROTEÇÃO AVANÇADA CONTRA ATAQUES CIBERNÉTICOS PARA ESTAÇÕES DE TRABALHO (EXTENDED DETECTION AND RESPONSE - XDR) (ITEM 1):**

5.2.1. Visa oferecer uma camada de defesa endpoints da rede, ajudando a prevenir, detectar e responder a ataques de malware, ransomware, vírus e outras ameaças. As proteções para endpoint geralmente incluem firewalls, antivírus, antimalware, detecção de intrusão, controle de aplicativos, gerenciamento de patches e outras ferramentas de segurança. Elas são essenciais para garantir a segurança dos dispositivos e dos dados armazenados neles, especialmente em ambientes corporativos, onde a proteção dos endpoints é crucial para a segurança global da rede.

5.3. **SOLUÇÃO DE PROTEÇÃO AVANÇADA CONTRA ATAQUES CIBERNÉTICOS PARA SERVIDORES (EXTENDED DETECTION AND RESPONSE - XDR) (ITEM 2):**

5.3.1. A proteção para servidores em um ambiente corporativo é de extrema importância porque os servidores são peças fundamentais da infraestrutura de tecnologia da informação de uma empresa. Eles armazenam e processam dados críticos e sensíveis, além de hospedar aplicativos e serviços essenciais para o funcionamento do negócio.

5.4. **SERVIÇO DE SUPORTE PRO ATIVO, CORRETIVO E PARA RESPOSTA A INCIDENTES (ITEM 3):**

5.4.1. O serviço abrange suporte proativo, corretivo e resposta a incidentes, visando prevenir problemas, corrigir falhas e reagir rapidamente a eventos adversos para manter a estabilidade e segurança dos sistemas.

5.5. **SERVIÇO DE TREINAMENTO (ITEM 5):**

5.5.1. Esse serviço visa fornecer treinamento e transferência de conhecimento para os clientes. Ele oferece capacitação especializada, permitindo que os usuários adquiram habilidades e compreensão sobre o uso eficaz das soluções ou tecnologias implementadas, capacitando-os a gerenciar, operar e manter os sistemas.

6. REQUISITOS DA CONTRATAÇÃO:

6.1. **Solução de proteção avançada contra ataques cibernéticos para estações de trabalho (Extended detection and response – XDR) (ITEM 01):**

- 6.1.1. A solução deverá ser entregue na modalidade como um serviço (em nuvem);
- 6.1.2. Possuir console Web para gerenciamento e administração da ferramenta;
- 6.1.3. A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações e Controle de dispositivos em um único agente.

6.2. **Módulo de Proteção Anti-Malware:**

- 6.2.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:
- 6.2.2. Windows 8.1 (x86/x64);

- 6.2.3. Windows 10 (x86/x64);
- 6.2.4. Windows 11 (x64).
- 6.2.5. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;
- 6.2.6. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;
- 6.2.7. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em: Processos em execução em memória principal (RAM);
- 6.2.8. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);
- 6.2.9. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, MIME/uu, CAB;
- 6.2.10. Arquivos recebidos por meio de programas de comunicação instantânea (MSN messenger, yahoo messenger, google talk, icq, dentre outros).
- 6.2.11. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript, VBScript/Activex;
- 6.2.12. Deve possuir detecção heurística de vírus desconhecidos;
- 6.2.13. Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada; Deve permitir diferentes configurações de detecção (varredura ou rastreamento):
- 6.2.14. Em tempo real de arquivos acessados pelo usuário;
- 6.2.15. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;
- 6.2.16. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;
- 6.2.17. Automáticos do sistema com as seguintes opções:
- 6.2.18. Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;
- 6.2.19. Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);
- 6.2.20. Frequência: horária, diária, semanal e mensal;
- 6.2.21. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;
- 6.2.22. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;
- 6.2.23. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;
- 6.2.24. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;
- 6.2.25. Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;
- 6.2.26. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;
- 6.2.27. Deve possuir capacidade de escaneamento de arquivos compactados e, em caso de identificação de um arquivo malicioso, apenas este deve ser removido, mantendo os demais intactos
- 6.2.28. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;
- 6.2.29. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;
- 6.2.30. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;
- 6.2.31. Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;
- 6.2.32. Deverá ter funcionalidade de Machine Learning em runtime para evitar possíveis métodos de obfuscação que o módulo de Machine Learning em pré-execução não consiga detectar;
- 6.2.33. Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;
- 6.2.34. Deve bloquear processos comuns associados a ransomware;
- 6.2.35. Em casos de ataques de ransomware, a solução deve ter a capacidade de interromper o processo de criptografia e restaurar os arquivos originais aos seus respectivos diretórios
- 6.2.36. Deve possuir funcionalidade de detecção de malwares conhecidos e desconhecidos por comportamento; Deve permitir a integração com solução de análise de artefatos suspeitos (sandbox) do próprio fabricante.
- 6.3. **Funcionalidade de Atualização:**
- 6.3.1. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;
- 6.3.2. Deve permitir atualização incremental da lista de definições de vírus;
- 6.3.3. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;
- 6.3.4. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;
- 6.3.5. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;
- 6.3.6. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;
- 6.3.7. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.
- 6.4. **Funcionalidade de Administração:**
- 6.4.1. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;
- 6.4.2. Deve possibilitar instalação "silenciosa";

- 6.4.3.

Deve permitir o bloqueio por nome de arquivo;
- 6.4.4.

Deve permitir o travamento de pastas e diretórios;
- 6.4.5.

Deve permitir o travamento de compartilhamentos;
- 6.4.6.

Deve permitir o rastreamento e bloqueio de infecções;
- 6.4.7.

Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;
- 6.4.8.

Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;
- 6.4.9.

Deve permitir a desinstalação através da console de gerenciamento da solução;
- 6.4.10.

Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;
- 6.4.11.

Deve permitir a deleção dos arquivos quarentenados;
- 6.4.12.

Deve permitir remoção automática de clientes inativos por determinado período;
- 6.4.13.

Deve permitir integração com serviço de autenticação como Active Directory para acesso a console de administração;
- 6.4.14.

Deve permitir criação de diversos perfis e usuários para acesso a console de administração;
- 6.4.15.

Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
- 6.4.16.

Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;
- 6.4.17.

Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;
- 6.4.18.

Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
- 6.4.19.

Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional;
- 6.4.20.

Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;
- 6.4.21.

Deve prover criptografia para as comunicações entre o servidor e os agentes de proteção; Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;
- 6.4.22.

Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;
- 6.4.23.

Deve permitir a criação de usuários locais de administração da console de anti-malware;
- 6.4.24.

Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;
- 6.4.25.

Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;
- 6.4.26.

Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;
- 6.4.27.

Deve permitir a gerência de domínios separados para usuários previamente definidos;
- 6.4.28.

Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;
- 6.4.29.

Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.
- 6.5.

**Funcionalidade de Controle de Dispositivos:**
- 6.5.1.

As configurações da funcionalidade de controle de dispositivos devem ser aplicadas por usuário;
- 6.5.2.

Deve permitir políticas e ações diferentes para dispositivos conectados à rede interna e aqueles utilizados na rede externa (conectado à Internet, por exemplo);
- 6.5.3.

Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;
- 6.5.4.

Deve possuir o controle de acesso a drives de mídias de armazenamento como CD-ROM, DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;
- 6.5.5.

Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;
- 6.5.6.

Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;
- 6.5.7.

Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa;
- 6.5.8.

Para ação de restrição como o bloqueio, a solução deve permitir adicionais dispositivos USB autorizados, bem como apontar executáveis específicos como exceção ao bloqueio;
- 6.5.9.

Deve ter a capacidade de bloquear a função de Autorun nos dispositivos;
- 6.5.10.

Deve permitir controle de permissão ou bloqueio para dispositivos que não armazenam dados tendo, pelo menos, os seguintes tipos de dispositivos: adaptadores bluetooth, dispositivos de imagem, modems, interfaces wireless externas, cartões PCMCIA, dispositivos infravermelhos e portas COM/LPT.
- 6.6.

**Módulo de Proteção Anti-Malware para estações MacOS:**
- 6.6.1.

O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:
- 6.6.2.

macOS 12 (Monterey);
- 6.6.3.

macOS 11 (Big Sur) macOS 10.15 (Catalina);
- 6.6.4.

macOS 10.14 (Mojave); macOS 10.13 (High Sierra);
- 6.6.5.

Suporte ao Apple Remote Desktop para instalação remota da solução;
- 6.6.6.

Gerenciamento integrado à console de gerência central da solução;
- 6.6.7.

Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;
- 6.6.8.

Permitir a verificação das ameaças da maneira manual e agendada;
- 6.6.9.

Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus; Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infeções a arquivos;
- 6.6.10.

Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;
- 6.6.11.

Deve possuir no mecanismo de autoproteção as seguintes proteções:

- 15/05/2025, 11:22SEI/RO - 0059255807 - Termo de Referência
- 6.6.12.

Proteção e verificação dos arquivos de assinatura;
- 6.6.13.

Proteção dos processos do agente de segurança;
- 6.6.14.

Proteção das chaves de registro do agente de segurança;
- 6.6.15.

Proteção do diretório de instalação do agente de segurança.
- 6.7.

**Funcionalidade de HIPS – Host IPS e Host Firewall:**
- 6.7.1.

Deve ser capaz de realizar a detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais:
- 6.7.2.

Windows 8.1 (x86/x64);
- 6.7.3.

Windows 10 (x86/x64);
- 6.7.4.

Windows 11 (x64).
- 6.7.5.

Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;
- 6.7.6.

As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;
- 6.7.7.

Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio);
- 6.7.8.

Deve permitir ativar e desativar o produto sem a necessidade de remoção;
- 6.7.9.

Deve permitir que o usuário altere as configurações de níveis de segurança e exceções;
- 6.7.10.

Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo;
- 6.7.11.

O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança; O modulo de HIPS deverá possuir regras pra proteger contra ameaças do tipo Ransomware;
- 6.7.12.

O modulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genericas protegendo contra ameaças conhecidas ou desconhecidas;
- 6.7.13.

O módulo de HIPS deverá permitir que o administrador monitore apenas ou realize o bloqueio das tentativas de exploração de vulnerabilidades;
- 6.7.14.

Deve suportar configuração de parâmetros de pacotes como quantidade máxima de conexões TCP e timeout para pacotes UDP;
- 6.7.15.

Deve ter a capacidade de proteção contra exploração de vulnerabilidades do sistema operacional e de aplicações terceiras instaladas na estação de trabalho;
- 6.7.16.

A lista de regras deve permitir que o administrador realize buscas e tenha rápida visibilidade do tipo da aplicação, em que modo a regra encontra-se (bloqueio ou monitoramento), CVE, CVSS score, quando aplicável.
- 6.8.

**Módulo para Controle De Aplicações:**
- 6.8.1.

Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:
- 6.8.2.

Windows 8.1 (x86/x64);
- 6.8.3.

Windows 10 (x64);
- 6.8.4.

Windows 11 (x64).
- 6.8.5.

As regras de controle de aplicação devem permitir as seguintes ações:
- 6.8.6.

Permissão de execução;
- 6.8.7.

Bloqueio de execução;
- 6.8.8.

Bloqueio de novas instalações.
- 6.8.9.

A regra de liberação para o controle de aplicação deverá permitir que o programa liberado efetue ou não a execução de outros processos,
- 6.8.10.

As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;
- 6.8.11.

As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:
- 6.8.12.

Assinatura SHA-1 e SHA-256 do executável;
- 6.8.13.

Atributos do certificado utilizado para assinatura digital do executável;
- 6.8.14.

Caminho lógico do executável;
- 6.8.15.

Base de assinaturas de cortiçados digitais válidos e seguros.
- 6.8.16.

As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;
- 6.8.17.

As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;
- 6.8.18.

O módulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionados para bloqueio e monitoramento tendo, pelo menos, as categorias de KeyLoggers, anonimizadores de proxy, P2P, crackers de senhas;
- 6.8.19.

Deve permitir a busca por aplicações ou fabricante destas;
- 6.8.20.

Deve possuir ferramenta para extrair o hash de um ou um grupo de executáveis, permitindo a importação destes hashes através de arquivo CSV.
- 6.9.

**Módulo de Detecção e Resposta:**
- 6.9.1.

A solução deve ser compatível com os sistemas operacionais Windows, Linux e MacOS;
- 6.9.2.

O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK®, identificando técnicas e táticas dos ataques;
- 6.9.3.

A solução deve possuir módulo de investigação e detecção integrados;
- 6.9.4.

Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;
- 6.9.5.

Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;
- 6.9.6.

Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;
- 6.9.7.

Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;
- 6.9.8.

Fornece a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;
- 6.9.9.

Capacidade de construir sequências de buscas poderosas para localizar os dados ou objetos em seu ambiente que você deseja examinar;
- 6.9.10.

Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo Kibana para identificar, categorizar e recuperar os resultados da pesquisa;
- 6.9.11.

Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;
- 6.9.12.

Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;



- 15/05/2025, 11:22SEI/RO - 0059255807 - Termo de Referência
- 6.9.13.

Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;
- 6.9.14.

Deve permitir que as detecções sejam correlacionadas com módulos de servidores, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;
- 6.9.15.

A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;
- 6.9.16.

Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;
- 6.9.17.

O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos; Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;
- 6.9.18.

A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;
- 6.9.19.

A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;
- 6.9.20.

Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;
- 6.9.21.

Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;
- 6.9.22.

Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade;
- 6.9.23.

Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;
- 6.9.24.

Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;
- 6.9.25.

Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;
- 6.9.26.

Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;
- 6.9.27.

Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;
- 6.9.28.

Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho;
- 6.9.29.

Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;
- 6.9.30.

Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;
- 6.9.31.

A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);
- 6.9.32.

Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas;
- 6.9.33.

Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;
- 6.9.34.

Deve permitir que o analista possa alterar o status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma;
- 6.9.35.

Deve permitir adicionar arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores; Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores; Deve permitir terminar processos ativos executados nas estações de trabalhos e servidores; Permitir coletar e fazer o download de um arquivo para investigação local detalhada;
- 6.9.36.

Isolar a estação de trabalho desconectando-a da rede e permitindo se comunicar exclusivamente com a
- 6.9.37.

console de gerenciamento do fabricante;
- 6.9.38.

Restaurar a conectividade da estação de trabalho com a rede;
- 6.9.39.

Iniciar uma sessão de shell remoto na estação de trabalho selecionada para execução de comandos remotos para investigação;
- 6.9.40.

Deve ser possível fazer o download do histórico da sessão após finalizar a sessão remota do shell na estação de trabalho para fins de auditoria.
- 6.10.

**SOLUÇÃO DE PROTEÇÃO AVANÇADA CONTRA ATAQUES CIBERNÉTICOS PARA SERVIDORES (EXTENDED DETECTION AND RESPONSE - XDR) (ITEM 2):**
- 6.11.

**SOLUÇÃO DE SEGURANÇA PARA CARGAS DE TRABALHO HÍBRIDAS COM DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO:**
- 6.12.

**Características Gerais Da Solução:**
- 6.12.1.

A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais:
- 6.12.2.

Windows Server 2000;
- 6.12.3.

Windows Server 2003 SP1 e 2003 R2 SP2; Windows Server 2008 e 2008 R2;
- 6.12.4.

Windows Server 2012 e 2012 R2;
- 6.12.5.

Windows Server 2016;
- 6.12.6.

Windows Server 2019;
- 6.12.7.

Windows Server 2022;
- 6.12.8.

Red Hat Enterprise 5, 6, 7 e 8;
- 6.12.9.

CentOS 5, 6, 7 e 8;
- 6.12.10.

AIX 6.1, 7.1 e 7.2;
- 6.12.11.

Oracle Linux 5, 6, 7 e 8;
- 6.12.12.

SUSE Linux Enterprise Server 10, 11, 12 e 15;
- 6.12.13.

Ubuntu 10, 12, 14, 16, 18 e 20;
- 6.12.14.

Debian 6, 7, 8, 9 e 10;
- 6.12.15.

Rocky Linux 8;
- 6.12.16.

AlmaLinux 8;
- 6.12.17.

Cloud Linux 5, 6, 7 e 8; Solaris 10 1/13 Sparc; Solaris 10 1/13 (x86/x64); Solaris 11.2/ 11.3 Sparc; Solaris 11.2/ 11.3 (x86/x64);
- 6.12.18.

Solaris 11.4 (x86, x64 ou SPARC) Amazon Linux e Amazon Linux 2 (x64).
- 6.12.19.

A solução deverá ser totalmente compatível e homologada com o ambiente Vmware;
- 6.12.20.

A console de gerenciamento deverá ser em nuvem, permitindo o gerenciamento das políticas de segurança através da Internet;
- 6.12.21.

A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Internet Explorer, Google Chrome e Firefox. Deve ainda suportar certificado digital para gerenciamento;
- 6.12.22.

A solução deverá permitir a integração com pelo menos as seguintes plataformas de nuvem: Vmware vCloud, MS Azure e AWS;

- 6.12.23. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;
- 6.12.24. A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;
- 6.12.25. A console de administração deverá permitir o envio de notificações via SMTP;
- 6.12.26. Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;
- 6.12.27. A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;
- 6.12.28. A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;
- 6.12.29. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;
- 6.12.30. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob- demanda, ou agendado com o envio automático do relatório via e-mail;
- 6.12.31. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;
- 6.12.32. A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;
- 6.12.33. A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS aplicadas e Firewall;
- 6.12.34. Em caso de solução e nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade; A solução de segurança ter a capacidade de identificar ataques entre containers;
- 6.12.35. Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";
- 6.12.36. Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar novas políticas de segurança;
- 6.12.37. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;
- 6.12.38. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;
- 6.12.39. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;
- 6.12.40. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;
- 6.12.41. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;
- 6.12.42. Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;
- 6.12.43. Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;
- 6.12.44. Para servidores Linux, a solução deverá possibilitar a atualização automática da versão quando o agente reiniciar;
- 6.12.45. Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;
- 6.12.46. Deve permitir a remoção automática de agentes inativos, definindo o período para, pelo menos 1 semana, 1 mês e 12 meses;
- 6.12.47. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;
- 6.12.48. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;
- 6.12.49. A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação; A solução deverá mostrar quais máquinas estão usando determinada política;
- 6.12.50. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;
- 6.12.51. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;
- 6.12.52. A solução deverá permitir a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;
- 6.12.53. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;
- 6.12.54. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;
- 6.12.55. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;
- 6.12.56. A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;
- 6.12.57. A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;
- 6.12.58. A solução deverá ter a capacidade de se integrar com o Amazon SNS e os principais softwares de SIEMs contemplando, no mínimo: Splunk, IBMQradar e HPArCSight de modo a permitir enviar os seus logs para essas soluções;
- 6.12.59. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;
- 6.12.60. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;
- 6.12.61. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;
- 6.12.62. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;
- 6.12.63. Após a atualização deve ser informado o que foi modificado ou adicionado;
- 6.12.64. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não as distribuir aos clientes;
- 6.12.65. A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras;
- 6.12.66. A solução deverá ter capacidade de gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;
- 6.12.67. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;
- 6.12.68. No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes;
- 6.12.69. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;
- 6.12.70. Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;

- 6.12.71. Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;
- 6.12.72. O fabricante deverá participar do programa “Microsoft Application Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;
- 6.12.73. A console de gerenciamento deve se integrar com o Vmware vCloud, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;
- 6.12.74. O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos; A solução deve possuir API documentada para integração na esteira de automação;
- 6.12.75. A documentação da API deve conter exemplos prontos para implementação de determinadas funcionalidades, como cookbooks;
- 6.12.76. Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;
- 6.12.77. A solução deve permitir desabilitar os módulos individualmente;
- 6.12.78. Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador.
- 6.13. **Antimalware:**
- 6.13.1. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;
- 6.13.2. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;
- 6.13.3. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;
- 6.13.4. Em plataforma Windows, a solução deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações;
- 6.13.5. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo;
- 6.13.6. Em servidores Windows, deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentenando arquivos identificados;
- 6.13.7. A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;
- 6.13.8. A solução deverá oferecer escanear processos em memória em busca de Malware;
- 6.13.9. O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;
- 6.13.10. O scan de arquivos comprimidos do tipo OLE deverá ser de no mínimo 20 camadas de compressão;
- 6.13.11. Para servidores Windows, a solução deverá permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline na console de gerenciamento;
- 6.13.12. A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;
- 6.13.13. Em servidores Windows, a solução deverá integrar-se com interface AMSI (Antimalware Scan Interface);
- 6.13.14. A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado; Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware; Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;
- 6.13.15. Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no servidor;
- 6.13.16. A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs; Em servidores Windows, deve possuir capacidade de detectar ameaças por comportamento;
- 6.13.17. Deverá ter a possibilidade de escanear drivers de rede mapeados nos servidores.
- 6.14. **Proteção Contra URLs Maliciosas:**
- 6.14.1. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;
- 6.14.2. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;
- 6.14.3. A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas tendo, pelo menos, os níveis Alto, médio e baixo;
- 6.14.4. Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;
- 6.14.5. Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;
- 6.14.6. Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;
- 6.14.7. A solução deve permitir que o administrador reclassifique uma URL através do site do fabricante para evitar falsos positivos;
- 6.14.8. A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.
- 6.14.9. Firewall.
- 6.14.10. Operar como firewall de host, através da instalação de agente nos servidores protegidos;
- 6.14.11. Precisa ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;
- 6.14.12. Precisa ter a capacidade de controlar conexões TCP baseado nas Flags TCP; Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;
- 6.14.13. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYN SYN Scan, TCP Xmas Scan e Computer OS Fingerprint por até 30 minutos;
- 6.14.14. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;
- 6.14.15. Precisa ter a capacidade de definição de regras para contextos específicos;
- 6.14.16. Para facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de ips, lista de MACs, lista de portas;
- 6.14.17. Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);
- 6.14.18. Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana; O firewall deverá ser stateful bidirecional;
- 6.14.19. O firewall deverá permitir liberar ou apenas logar eventos;
- 6.14.20. O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;
- 6.14.21. As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny;

- 6.14.22. A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;
- 6.14.23. As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;
- 6.14.24. Deverá realizar pseudo stateful em tráfego UDP; Deverá logar a atividade stateful;
- 6.14.25. Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador;
- 6.14.26. Deverá permitir limitar o número de meias conexões vindas de um computador; Deverá prevenir ack storm;
- 6.14.27. Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;
- 6.14.28. Deverá identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um período de tempo configurado pelo administrador;
- 6.14.29. Deverá permitir criar lista de exceções para identificar os Ips autorizados a realizar varreduras de portas ou da rede;
- 6.14.30. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.
- 6.15. **Proteção De Vulnerabilidades de SO e Aplicações:**
- 6.15.1. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;
- 6.15.2. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;
- 6.15.3. A solução deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;
- 6.15.4. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;
- 6.15.5. Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;
- 6.15.6. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;
- 6.15.7. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;
- 6.15.8. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;
- 6.15.9. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para
- 6.15.10. fins de investigação do incidente;
- 6.15.11. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;
- 6.15.12. Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;
- 6.15.13. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);
- 6.15.14. Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana; Deverá ser capaz de inspecionar tráfego criptografado de entrada;
- 6.15.15. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL injection, Crosssite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;
- 6.15.16. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;
- 6.15.17. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;
- 6.15.18. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;
- 6.15.19. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;
- 6.15.20. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;
- 6.15.21. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;
- 6.15.22. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;
- 6.15.23. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs; As regras de IPS poderão ter sua capacidade de LOG desabilitado;
- 6.15.24. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta; As regras devem ser atualizadas automaticamente pelo fabricante;
- 6.15.25. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.
- 6.16. **Monitoramento De Integridade:**
- 6.16.1. A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;
- 6.16.2. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;
- 6.16.3. Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux; Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional; Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;
- 6.16.4. Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;
- 6.16.5. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;
- 6.16.6. O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;
- 6.16.7. Deverá alertar toda vez que uma modificação ocorrer em tempo real para ambiente Windows e pseudo real-time para ambiente Linux;
- 6.16.8. Deverá logar e colocar em relatório todas as modificações que ocorram;
- 6.16.9. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;
- 6.16.10. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;
- 6.16.11. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;
- 6.16.12. Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente.

- 6.17.

**Inspeção De Logs:**
- 6.17.1.

A solução deverá permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX;
- 6.17.2.

Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;
- 6.17.3.

Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;
- 6.17.4.

Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;
- 6.17.5.

Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;
- 6.17.6.

Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;
- 6.17.7.

Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;
- 6.17.8.

Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;
- 6.17.9.

Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;
- 6.17.10.

Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram; As regras poderão ser modificadas por severidade de ocorrência de eventos;
- 6.17.11.

As regras devem se atualizar automaticamente pelo fabricante;
- 6.17.12.

Permitir modificação pelo administrador em regras para adequação ao ambiente.

- 6.18.

**Controle De Aplicações:**
- 6.18.1.

A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;
- 6.18.2.

O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;
- 6.18.3.

O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina; A console deverá exibir eventos de no mínimo 30 dias;
- 6.18.4.

A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período que deve ser no máximo 10 horas;
- 6.18.5.

A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente.

- 6.19.

**Detecção e Resposta:**
- 6.19.1.

A solução deve ser compatível com Linux e Windows Server 2008 R2 e superiores; A solução deve possuir módulo de investigação, detecção integrados.
- 6.19.2.

Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;
- 6.19.3.

A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;
- 6.19.4.

Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;
- 6.19.5.

O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos; Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;
- 6.19.6.

A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;
- 6.19.7.

A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados na console, ainda que estas não sejam detectadas como maliciosas;
- 6.19.8.

A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;
- 6.19.9.

Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;
- 6.19.10.

Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;
- 6.19.11.

Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;
- 6.19.12.

Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;
- 6.19.13.

Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;
- 6.19.14.

Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;
- 6.19.15.

A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);
- Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.
- 6.20.

**SERVIÇO DE SUPORTE PRO ATIVO, CORRETIVO E PARA RESPOSTA A INCIDENTES (ITEM 3):**

6.20.1.

O serviço de suporte proativo, corretivo e para resposta a incidentes compreende um conjunto abrangente de atividades destinadas a assegurar o pleno funcionamento e a continuidade operacional de sistemas, soluções ou serviços. Este serviço é estrategicamente desenhado para atender às demandas dinâmicas do ambiente tecnológico, oferecendo suporte preventivo, corretivo e uma resposta ágil a incidentes de segurança.

6.20.2.

Todo o Serviço de Suporte deverá ser prestado por profissional certificado pelo Fabricante da Solução, em nível compatível com a prestação do serviço. Deverá ser apresentado comprovação da certificação dos profissionais responsáveis no ato da assinatura do contrato.

6.20.3.

Deverá disponibilizar um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução ofertada;

6.20.4.

deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução.

6.21.

**Suporte Proativo:**

6.21.1.

O suporte proativo deverá antecipar potenciais problemas, identificando e resolvendo questões antes mesmo que impactem o desempenho e a segurança do ambiente;

6.21.2.

A contratada deverá notificar a contratante sobre atualizações de segurança, patches e correções assim que estiverem disponíveis, caso autorizado aplicar as atualizações de segurança e evolutiva dos produtos;

6.21.3.

Deverá realizar análises preditivas, buscando otimizar a performance e prevenir falhas nos produtos, além de detectar padrões que possam indicar uma possível violação de segurança, proporcionando um ambiente mais estável e seguro;

6.21.4.

Deverá realizar avaliações regulares de riscos para identificar possíveis vulnerabilidades e pontos fracos nos sistemas e, implementar medidas corretivas com base nos resultados das avaliações de riscos;
- https://sei.sistemas.ro.gov.br/sei/controlador.php?acao=documento\_visualizar&acao\_origem=arvore\_visualizar&id\_documento=61262456&infra\_sistema=100000100&infra\_unidade\_atual=110000209&infra\_hash=4...

9/27

- 6.21.5. Realizar auditorias regulares para garantir que as melhores práticas e os controles de segurança estejam operacionais e, utilizar resultados de auditorias para implementar melhorias contínuas;
- 6.21.6. A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução do problema.
- 6.22. **Suporte Corretivo:**
- 6.22.1. Este componente concentra-se na solução de problemas ou incidentes. O suporte corretivo atua de forma ágil para restabelecer a funcionalidade normal do sistema, minimizando impactos negativos e mantendo a continuidade operacional;
- 6.22.2. Serviço Especializado de Suportes corretivo para xx(xxxx) meses. Serviço de Suporte especializado para ajustes, correções e configurações da solução a ser fornecida. Neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução;
- 6.22.3. A contratada deverá:

a) Implementar um sistema de abertura de chamados, para registrar, rastrear e priorizar incidentes e requisições de suporte;

b) Atribuir números de caso exclusivos para facilitar a comunicação e o acompanhamento;

c) Garantir disponibilidade 24/7 para responder a incidentes críticos.
- 6.22.4. Deverá apresentar relatório contendo as ações adotadas para a solução do problema.
- 6.23. **Resposta a Incidentes:**
- 6.23.1. O serviço de resposta a incidentes deverá lidar com eventos imprevistos, como violações de segurança, falhas críticas ou interrupções inesperadas. deverá ser realizada por profissionais especializados e certificados pelo fabricante;
- 6.23.2. Deverá realizar investigações para determinar a natureza, origem e impacto de incidentes de segurança;
- 6.23.3. Desenvolver planos de mitigação e estratégia de recuperação para minimizar o impacto de incidentes;
- 6.23.4. Elaborar relatórios detalhados sobre os incidentes, incluindo ações tomadas e recomendações de melhorias.
- 6.24. **SERVIÇO DE IMPLANTAÇÃO:**
- 6.24.1. Nesta etapa, compreende-se a instalação e configuração da solução contratada, contados a partir da emissão da Ordem de Serviço (OS);
- 6.24.2. O serviço de implantação abrange integralmente as fases essenciais para a integração, instalação e configuração da solução contratada, alinhando-se precisamente com as especificações técnicas e requisitos predefinidos. Esta abordagem abarca desde o planejamento inicial até a conclusão efetiva, assegurando uma transição suave dos processos existentes para a nova solução;
- 6.24.3. O Plano de Implantação assume a forma de um documento fundamental que consolida a estratégia para instalação, configuração e entrega da solução contratada. Sua importância reside em orientar e alinhar as atividades, garantindo eficiência e uma implementação adequada da solução conforme os requisitos estabelecidos;
- 6.24.4. O documento deverá conter no mínimo os requisitos de ambiente tecnológicos necessários para a instalação das licenças, cronograma e detalhamento das atividades a serem realizadas, topologia do ambiente pós instalação da solução, matriz de responsabilidade, plano de comunicação;
- 6.24.5. Durante esta etapa, a equipe da Contratada deverá estar presente nos horários de instalação definidos pelo Contratante. As atividades de instalação e configuração poderão ser realizadas, conforme necessário, em horário comercial, período noturno ou final de semana;
- 6.24.6. O Contratante disponibilizará a infraestrutura de hardware e software necessária e já existente em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução durante esta etapa.
- 6.25. **Serviço de capacitação e repasse de conhecimento (Item 12):**
- 6.25.1. Repasse de conhecimento, na forma de treinamento para técnicos, de forma virtual, para 1 (uma) turma, com carga horária mínima de 40 (quarenta) horas, abrangendo todos os softwares integrantes da suíte de solução de segurança;
- 6.25.2. O conteúdo programático abordará tanto aspectos teóricos quanto práticos, contemplando de maneira abrangente todos os módulos relevantes da solução de segurança;
- 6.25.3. O treinamento pode ser segmentado de acordo com o produto a ser instalado no ambiente tecnológico, contemplando, no mínimo, os seguintes módulos:
- 6.25.4. Instalação do módulo de gerenciamento central;
- 6.25.5. Instalação do software de Endpoint Protection em estações de trabalho e servidores;
- 6.25.6. Descrição e configuração de todas as funcionalidades contratadas da solução;
- 6.25.7. Melhores práticas utilizadas no mercado para otimização dos softwares e suas funcionalidades.
- 6.25.8. A carga horária mínima estabelecida será de 40 (quarenta) horas, divididas em expedientes de 4 horas por dia, no horário comercial. A contratada é responsável por fornecer apostilas em formato digital que contemplem o conteúdo referente ao produto, oferecendo suporte ao aprendizado prático e teórico dos participantes;
- 6.25.9. Este treinamento visa capacitar adequadamente os usuários finais, garantindo que compreendam e aproveitem plenamente as funcionalidades da solução de segurança. O enfoque prático e teórico, aliado às melhores práticas do mercado, promove uma formação abrangente e eficaz.
- 6.26. **SERVIÇO DE TREINAMENTO (ITEM 4):**
- 6.26.1. Repasse de conhecimento, na forma de treinamento para técnicos, de forma virtual, para 1 (uma) turma, com carga horária mínima de 40 (quarenta) horas, abrangendo todos os softwares integrantes da suíte de solução de segurança;
- 6.26.2. O conteúdo programático abordará tanto aspectos teóricos quanto práticos, contemplando de maneira abrangente todos os módulos relevantes da solução de segurança;
- 6.26.3. O treinamento pode ser segmentado de acordo com o produto a ser instalado no ambiente tecnológico, contemplando, no mínimo, os seguintes módulos:
- 6.26.4. Instalação do módulo de gerenciamento central;
- 6.26.5. Instalação do software de Endpoint Protection em estações de trabalho e servidores;
- 6.26.6. Descrição e configuração de todas as funcionalidades contratadas da solução;
- 6.26.7. Melhores práticas utilizadas no mercado para otimização dos softwares e suas funcionalidades.
- 6.26.8. A carga horária mínima estabelecida será de 40 (quarenta) horas, divididas em expedientes de 4 horas por dia, no horário comercial. A contratada é responsável por fornecer apostilas em formato digital que contemplem o conteúdo referente ao produto, oferecendo suporte ao aprendizado prático e teórico dos participantes;
- 6.26.9. Este treinamento visa capacitar adequadamente os usuários finais, garantindo que compreendam e aproveitem plenamente as funcionalidades da solução de segurança. O enfoque prático e teórico, aliado às melhores práticas do mercado, promove uma formação abrangente e eficaz.
- 6.27. **DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC:**
- 6.28. **Requisitos de Capacitação**
- 6.28.1. A empresa CONTRATADA deverá realizar o repasse de conhecimento aos funcionários da CONTRATANTE que atuarão, diretamente, com a solução de segurança adquirida, contemplando instalação, parametrização, monitoramento, melhores práticas e atuação de incidentes com carga horária mínima de 40 (quarenta)



horas ministrado por profissional certificado pelo fabricante.

6.28.2. O treinamento será demandado à CONTRATADA pela CONTRATANTE após a efetiva implementação e estruturação da solução de segurança em seu parque tecnológico, quando acordarão cronograma para realização do treinamento.

6.28.3. O treinamento deverá ser realizado na modalidade presencial nas dependências da CONTRATANTE a participantes da equipe técnica a serem definidos pela CONTRATANTE.

6.28.4. Os horários do curso deverão seguir a conveniência do CONTRATANTE, podendo sua realização ocorrer apenas em um dos períodos do dia (manhã ou tarde).

6.28.5. Deverá ser fornecido material didático completo e com conteúdo oficial do fabricante em língua portuguesa. Caso seja utilizado material elaborado exclusivamente pelo fabricante e fique demonstrado que este não é oferecido em língua portuguesa, será aceito o fornecimento em língua inglesa.

6.28.6. O treinamento deve conter parte teórica e prática, incluindo tópicos sobre a instalação, uso, configuração, resolução de problemas da solução, análise de relatórios, respostas a incidentes e outros.

6.28.7. As datas do treinamento devem ser previamente combinadas com o CONTRATANTE.

6.28.8. Todos os custos relativos à realização do treinamento são de exclusiva responsabilidade da CONTRATADA.

6.29. **REQUISITOS E FUNCIONALIDADES TÉCNICOS DA SOLUÇÃO:**

6.29.1. A especificação técnica mínima e obrigatória da solução encontra-se detalhada no Anexo I deste estudo.

6.30. **Requisitos de manutenção e garantia:**

6.30.1. A empresa contratada é responsável por fornecer suporte técnico e garantia de atualização da solução pelo período de 36 meses, a contar da data de emissão do Termo de Recebimento. É importante ressaltar que essa garantia não se limita ao término da vigência contratual.

6.30.2. A garantia deve incluir obrigatoriamente:

- a) Atualização das versões dos softwares fornecidos, caso sejam disponibilizadas novas versões.
- b) Atualização dos softwares fornecidos caso haja lançamento de novos softwares que substituam os fornecidos ou se ficar evidente a descontinuidade dos softwares fornecidos, mesmo que não se trate de substituição direta.
- c) Correções dos softwares fornecidos, incluindo a aplicação de patches para corrigir eventuais falhas (bugs) de software que possam prejudicar o ambiente de produção ou vulnerabilidades que comprometam a segurança da solução.

6.30.3. A garantia deverá ser prestada durante todo o período de contrato e aditivos relacionados à atualização das licenças e proteção.

6.30.4. Durante o período de garantia, a empresa contratada compromete-se a substituir, em até 15 dias úteis, os equipamentos que apresentarem, em um período de 60 dias, duas ocorrências de defeitos por inoperância do produto ou 3 ocorrências de deficiência operacional do produto.

6.30.5. As ferramentas e equipamentos necessários à manutenção serão de responsabilidade da contratada.

6.31. **Suporte Técnico:**

6.31.1. Deverá ser oferecido suporte técnico da Contratada, com a possibilidade de abertura de chamados, das 7h00 às 20h00, em dias úteis, para a resolução de problemas. É importante destacar que os serviços de suporte técnico devem contemplar as manutenções corretivas e evolutivas para a solução contratada e não podem acarretar custos adicionais ao CONTRATANTE, além do que foi previamente acordado.

6.31.2. A empresa contratada deve encaminhar o chamado para o suporte do fabricante sempre que necessário, seja devido à criticidade, impacto ou urgência do problema, ou caso seja necessário o envolvimento direto do fabricante no processo de correção. É imprescindível que seja fornecido acesso ao site do fabricante para acompanhamento dos chamados, acesso à base de conhecimento e aos fóruns relacionados à solução.

6.31.3. Os serviços de suporte técnico abrangem:

- a) Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução.
- b) Elaboração de relatórios, estudos e diagnósticos sobre o ambiente.
- c) Transferência de conhecimento aos técnicos da Contratante referente aos problemas vivenciados e às soluções aplicadas, na forma a ser determinada pelas partes.
- d) Realização de instalação, atualização e configuração de novas versões dos produtos após a disponibilização das atualizações tecnológicas pelo fabricante.

6.31.4. O suporte técnico deve contemplar o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso do software ou para correção de problemas, em especial na configuração de parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução.

6.31.5. O suporte técnico deve contemplar, quando for o caso, atendimento a eventual problema de instalação ou configuração de softwares básicos e de infraestrutura de TIC (sistemas operacionais, servidores de banco de dados, servidores de aplicação, etc.) necessários ao funcionamento da solução.

6.31.6. Deve contemplar também a atualização de versões do software aplicativo, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela fabricante, num empacotamento estável do sistema. O serviço de atualização de versão tem por finalidade assegurar a devida atualização da solução durante o período de vigência da garantia. Refere-se ao fornecimento de novas versões e releases da solução lançados no período. A cada nova liberação de versão e release, serão disponibilizados em formato digital manuais e demais documentos técnicos, bem como nota informativa das funcionalidades implementadas. Em caso de lançamento de patch de correção, a CONTRATADA deverá comunicar o fato ao CONTRATANTE e indicar a forma de obtenção e os defeitos que serão corrigidos pelo patch. Em ambos os casos, a comunicação deve ser feita no prazo de até 30 dias, a contar do lançamento de nova versão ou solução de correção.

6.31.7. A CONTRATADA será responsável pelos serviços de implantação das novas versões e releases dos produtos por ela fornecidos como partes do objeto, bem como pela aplicação dos patches de correção e pacotes de serviço (service packs) relativos a esses produtos. Para a implantação das novas versões/releases, bem como para a aplicação dos patches, deverá ser aberto chamado de suporte técnico com nível de severidade adequado e a prestação dos serviços deve ser agendada com os responsáveis pela solução na CONTRATANTE;

6.31.8. Deverá ser prestado suporte técnico remoto com atendimento mediante registro de chamados em página de website, em sistema fornecido pela CONTRATADA e/ou pelo fabricante; e também através de contato telefônico. Esse serviço destina-se a esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução CONTRATADA;

6.31.9. As peças substitutas deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento e devem integrar a garantia da solução;

6.31.10. A CONTRATADA auxiliará o CONTRATANTE na reinstalação das ferramentas, caso seja necessário, ao longo do tempo de garantia da ferramenta;

6.31.11. A CONTRATADA deverá disponibilizar os seguintes canais de acesso ao suporte técnico:

- I - Portal Web;
- II - E-mail;
- III - Central 0800; e/ou
- IV - Telefone fixo.

6.31.12. O atendimento deve ser contínuo, 24 horas por dia, 7 dias por semana, durante todo o ano, incluindo feriados, em língua portuguesa. O início do atendimento e o prazo de solução devem ser determinados de acordo com o nível de severidade exigido para o caso, conforme os índices de criticidade abaixo:

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço	Glosa (por evento) para eventual descumprimento
Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto nas operações críticas de negócio.  Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção. Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 2 horas deve ter um técnico do fornecedor on-site.	Em até 8 horas	10%
		Em até 4 horas deve ter um técnico do fornecedor on-site.	Entrega da Solução pelo fabricante em até 6 dias.	
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Em até 4 horas deve ter um técnico do fornecedor on-site.	Em até 4 horas deve ter um técnico do fornecedor on-site.	7,50%
		Em até 2 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou retorno de chamada. Gerente técnico do fabricante deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.	Em até 16 horas	
			Entrega da Solução pelo fabricante em até 10 dias.	
Severidade 3	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	Um técnico do fornecedor on-site ou atendimento remoto.	Em até 24 horas.	5%
		Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato.	Entrega da Solução pelo fabricante em até 15 dias ou na próxima atualização do Software.	

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço	Glosa (por evento) para eventual descumprimento
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. Exemplos: O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 12 horas um técnico do fornecedor entra em contato.	2%

6.31.13. Para cada chamado de suporte categorizado como grau de severidade 1, o recurso previsto na tabela acima deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante. É importante destacar que todos os prazos para atendimento da garantia começarão a ser contados a partir da abertura do chamado, independentemente de ter sido feito via telefone, e-mail, site da contratada ou do fabricante. Além disso, o período de suporte deve estar diretamente atrelado ao período de garantia da solução.

6.31.14. Dentro do prazo máximo de atendimento, cabe ao fornecedor dar início, junto ao contratante, às providências que serão adotadas para a solução do chamado. Considera-se plenamente solucionado o problema quando os sistemas/serviços forem restabelecidos sem restrições, ou seja, quando não se tratar de uma solução paliativa.

6.31.15. Para os chamados de severidades 1 e 2, os serviços de atendimento de garantia não podem ser interrompidos até o completo restabelecimento de todas as funções do sistema paralisado, mesmo que isso exija períodos noturnos e dias não úteis (sábados, domingos e feriados). Além disso, os chamados de garantia de severidades 1 e 2 devem contar com suporte in loco da contratada para agilizar o restabelecimento do serviço.

6.31.16. O fornecedor emitirá um relatório, sempre que solicitado pelo contratante, em formato eletrônico, preferencialmente em arquivo texto, contendo informações analíticas e sintéticas dos chamados da garantia abertos e fechados no período. Esse relatório deve incluir:

- I - Quantidade de ocorrências (chamados) registradas no período.
- II - Número do chamado registrado e nível de severidade, incluindo reaberturas. Data e hora de abertura.
- III - Data e hora de início e conclusão do atendimento.
- IV - Identificação do técnico do contratante que registrou o chamado.
- V - Identificação do técnico do contratante que atendeu o chamado da garantia. Descrição do problema.
- VI - Descrição da solução.
- VII - Informações sobre eventuais escalonamentos.
- VIII - Resumo da lista de chamados concluídos fora do prazo de solução estabelecido.
- IX - Total de chamados no mês e o total acumulado até a apresentação do relatório.

6.31.17. Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante.

6.31.18. Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante.

6.31.19. Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução.

6.31.20. Para esses problemas, o fornecedor deverá, nos prazos estabelecidos nos níveis de criticidade, restabelecer o ambiente, através de uma solução de contorno e informar ao contratante, em um prazo máximo de 24 (vinte e quatro) horas, quando a solução definitiva será disponibilizada para o contratante.

6.31.21. Esta solução definitiva de que trata o subitem anterior deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias úteis, no caso da necessidade de criação de um patch/fix.

6.32. **Requisitos Sociais, Ambientais e Culturais:**

6.32.1. A Contratada deve aderir aos padrões estabelecidos pelo Modelo de Acessibilidade em Governo Eletrônico (e-MAG), conforme a Portaria Normativa SLTI nº 03, de 7 de maio de 2007. Essa aderência é necessária quando houver a necessidade de tornar o aplicativo acessível para solicitações de suporte técnico, visando garantir a inclusão e acessibilidade para todos os usuários.

6.32.2. Os serviços prestados pela Contratada devem sempre considerar o uso racional de recursos e equipamentos, com o objetivo de evitar o desperdício de insumos e materiais, bem como a geração excessiva de resíduos. Essa prática está alinhada com as diretrizes de responsabilidade ambiental adotadas pela Contratante.

6.32.3. A Contratada é responsável por fornecer orientações aos seus funcionários sobre a importância da racionalização de recursos no desempenho de suas atribuições, assim como sobre as diretrizes de responsabilidade ambiental adotadas pela Contratante. Essas orientações devem destacar a importância de reduzir o consumo de recursos, reutilizar materiais sempre que possível e realizar descarte adequado dos resíduos.

6.32.4. Além disso, a Contratada deve autorizar a participação de seus funcionários em eventos de capacitação e sensibilização promovidos pela Contratante, quando necessário. Esses eventos têm como objetivo fornecer conhecimentos e práticas relacionadas à racionalização de recursos e responsabilidade ambiental, visando aprimorar a conscientização e o desempenho sustentável da equipe da Contratada.

6.33. **Requisitos Temporais:**

6.33.1. As diretrizes relacionadas aos requisitos a seguir deverão ser considerados no processo de atendimento, entrega e instalação de equipamentos e serviços:

6.34. **Prazo de início de atendimento para suporte técnico e manutenção pela garantia:**

6.34.1. O início do atendimento deve seguir o que está especificado no acordo de nível de serviço presente no Termo de Referência.

6.35. **Requisitos de Segurança e Privacidade**

6.35.1. A CONTRATADA deve seguir os regulamentos, normas e instruções de segurança da informação e comunicações adotados pela CONTRATANTE. Isso inclui a Política de Segurança da Informação e Comunicações e suas Normas Complementares durante a execução dos serviços nas instalações da Secretaria.

6.36. **Devolução de informações confidenciais:**

- 6.36.1. Toda informação confidencial gerada e/ou manipulada em decorrência do contrato, seja ela armazenada em meio físico, magnético ou eletrônico, deve ser devolvida nas seguintes situações:

a) término ou rompimento do contrato; ou

b) solicitação da CONTRATANTE. A formalização entre as partes é necessária nesses casos.
- 6.37. **Utilização de ferramentas de proteção e segurança de informações:**
- 6.37.1. É imprescindível o uso de ferramentas de proteção e segurança de informações para evitar acesso não autorizado aos sistemas e softwares. Isso se aplica tanto aos sistemas sob responsabilidade direta da CONTRATADA quanto aos disponibilizados à CONTRATANTE, mesmo que por meio de link.
- 6.38. **Realização de alterações para sanar problemas de segurança ou vulnerabilidade:**
- 6.38.1. Quando formalmente solicitado pela CONTRATANTE, a CONTRATADA deve priorizar e realizar alterações para solucionar possíveis problemas de segurança ou vulnerabilidade nos sistemas ou softwares utilizados para a execução do serviço contratado.
- 6.39. **Comunicação de atualizações ou mudanças na configuração dos serviços:**
- 6.39.1. A CONTRATADA deve informar formalmente e de forma tempestiva ao CONTRATANTE sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados.
- 6.40. **Prestação de esclarecimentos e informações:**
- 6.40.1. É responsabilidade da CONTRATADA prestar os esclarecimentos necessários à CONTRATANTE, bem como fornecer informações sobre a natureza e o andamento dos serviços executados ou em execução.
- 6.41. **Garantia da integridade e disponibilidade dos documentos e informações:**
- 6.41.1. A empresa CONTRATADA deve garantir a integridade e disponibilidade dos documentos e informações que estão sob sua guarda em função do contrato. Caso ocorram perdas ou danos, a CONTRATADA será responsabilizada.
- 6.42. **Confidencialidade das informações:**
- 6.42.1. A CONTRATADA não pode divulgar, mesmo que em caráter estatístico, quaisquer informações originadas na CONTRATANTE sem prévia autorização. Controle de acesso e identificação dos profissionais:
- 6.42.2. O acesso às instalações da CONTRATADA onde os serviços serão realizados deve ser controlado e permitido apenas para pessoas autorizadas. Os profissionais da CONTRATADA devem estar devidamente identificados por crachás durante o trabalho. Qualquer profissional considerado inconveniente à boa ordem ou que viole as normas disciplinares da CONTRATANTE deve ser substituído imediatamente.
- 6.43. **Conhecimento e observância das normas disciplinares da CONTRATANTE:**
- 6.43.1. A CONTRATADA deve garantir que seus profissionais tenham conhecimento das normas disciplinares do CONTRATANTE e exijam sua fiel observância, especialmente em relação à utilização e segurança das instalações.
- 6.43.2. A CONTRATADA deve manter sigilo absoluto sobre todas as informações provenientes dos serviços realizados, documentos elaborados e informações obtidas dentro do ambiente da CONTRATANTE.
- 6.44. **Requisitos Legais:**
- 6.44.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021 (Lei de Licitações e Contratos Administrativos), à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

7. DO TRATAMENTO DOS DADOS

- 7.1. O cadastramento dos itens deve estar devidamente alinhado com a Lei nº 13.709/2018, Lei Geral de Proteção de Dados - LGPD, visando maior segurança jurídica ao estado no contrato a ser firmado;
- 7.2. A contratada deve seguir as normas relativas ao tratamento de dados pessoais, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD) e no que couber, as orientações contidas nas normas ABNT NBR ISO/IEC 29151:2020 (estabelece objetivos de controle para atender aos requisitos identificados por uma avaliação de risco e impacto relacionada à proteção de dados pessoais) e ABNT NBR ISO/IEC 27701:2019 (especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação).
- 7.3. A CONTRATADA não pode divulgar, mesmo que em caráter estatístico, quaisquer informações originadas na CONTRATANTE sem prévia autorização.
- 7.4. A CONTRATADA deve seguir os regulamentos, normas e instruções de segurança da informação e comunicações adotados pela CONTRATANTE. Isso inclui a Política de Segurança da Informação e Comunicações e suas Normas Complementares durante a execução dos serviços nas instalações da Secretaria.
- 7.5. A empresa CONTRATADA deve assegurar a disponibilidade, integridade, confidencialidade e sigilo dos documentos e informações relacionados ao contrato e aos serviços prestados. Qualquer pessoa que cause perdas e danos à CONTRATANTE ou a terceiros poderá ser responsabilizada legalmente.

8. DO ESTUDO TÉCNICO PRELIMINAR: (0059485479)

- 8.1. Levando-se em consideração que o estudo técnico preliminar é o documento que descreve as análises realizadas em relação às condições da contratação em termos de necessidades, requisitos, alternativas, escolhas, resultados pretendidos e demais características, que demonstra a viabilidade técnica e econômica da contratação.
- 8.2. Informamos que consta nos autos Estudo Técnico Preliminar 23 (0059485479) e Documento de Oficialização de Demanda 13 (0052860440).
- 8.3. **Resultados pretendidos:**
- 8.3.1. Com o objetivo da implantação de novas políticas de segurança, projeta-se um cenário primordial para controle e proteção contra ameaças básicas e avançadas no âmbito desta Secretaria de Estado do Desenvolvimento Ambiental - SEDAM, adotando padrões e diretrizes para melhor eficiência .
- 8.3.2. O monitoramento contínuo dos endpoints da SEDAM em busca de atividades suspeitas, garante uma segurança proativa e eficaz, permitindo a identificação e mitigação de ameaças antes que elas possam causar danos significativos à organização.
- 8.3.3. Detecção avançada de ameaças que outros sistemas de segurança podem não conseguir detectar. Por meio da análise comportamental dos endpoints, a solução pode identificar padrões suspeitos e agir de forma rápida e efetiva para lidar com os incidentes de segurança, reduzindo os danos potenciais à organização.
- 8.3.4. Resposta automatizada a incidentes, adotando medidas como bloquear o acesso ao endpoint infectado, isolá-lo da rede ou executar ações de limpeza para remover o malware. Essa resposta automatizada agiliza o tempo de resposta aos incidentes, minimizando o impacto na organização.
- 8.3.5. Análise forense aprofundada dos endpoints comprometidos. A solução é capaz de capturar registros de eventos, memória e arquivos, o que facilita a identificação da origem da ameaça e a implementação de medidas preventivas para evitar futuros incidentes no ambiente da organização.
- 8.3.6. Ao automatizar a detecção e resposta a ameaças comuns, a solução de antivírus corporativa contribui para o aumento da eficiência operacional da equipe de segurança. Isso permite que os profissionais se dediquem a tarefas mais críticas e estratégicas, reduzindo a carga de trabalho e otimizando o uso dos recursos disponíveis.

RESULTADOS A SEREM ALCANÇADOS	
01	Capacidade de detecção e resposta de ameaças em tempo real



RESULTADOS A SEREM ALCANÇADOS	
02	Proteção contra ameaças avançadas
03	Analises avançadas de malware
04	Visibilidade gráfica detalhada do ambiente
05	Maior taxa de acertividade de detecções
06	Inteligência de ameaças
07	Implantação de atualizações automáticas e automatizadas
08	Controle avançado do inventário de endpoints
09	Capacidade de resposta a incidentes
10	Redução do risco de incidentes

9. MANIFESTAÇÃO DA EQUIPE TÉCNICA QUANTO A JUSTIFICATIVA/COMPROVAÇÃO DO QUANTITATIVO PRETENDIDO

- 9.1. O quantitativo pretendido do presente termo de referência deu-se em consonância às averiguações, realizadas no Estudo Técnico Preliminar 23 (0059485479).
- 9.2. Justifica-se a aquisição, para atendimento a todo parque de computadores desta SEDAM, contemplados também os 14 (quatorze) escritórios regionais do estado e servidores virtuais de infraestrutura que hospedam serviços e sistemas.
- 9.3. Faz-se necessário a aquisição de 800 licenças para estações de trabalho e 300 licenças para servidores considerando o crescimento da Secretaria ao longo dos anos. Além disso, a prestação de serviços especializados para resposta a incidentes e monitoramento ativo, além de trazer treinamento para a compreensão completa da ferramenta, permitindo a configuração, análise e autonomia por parte da Secretaria.

10. GRUPO (LOTE)

- 10.1. O art. 40 § 3º, incisos I e II da Lei nº 14.133, de 01 de abril de 2021, traz a seguinte redação:

Art. 40. O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:

§ 3º O parcelamento não será adotado quando:

I - a economia de escala, a redução de custos de gestão de contratos ou a maior vantagem na contratação recomendar a compra do item do mesmo fornecedor;

II - o objeto a ser contratado configurar sistema único e integrado e houver a possibilidade de risco ao conjunto do objeto pretendido;

- 10.2. Há o agrupamento em lote em virtude de alguns objetos não poderem ser divididos. O não agrupamento causaria prejuízo e riscos para o conjunto, conforme Súmula 247 – TCU/2007 e artigo de lei supracitado.
- 10.3. É de suma importância para a Administração Pública que a contratação ocorra por lotes, visando à obtenção de menor preço na etapa dos lances, em atendimento ao Princípio da Economicidade (pois o parcelamento pode causar perda da economia de escala), para se evitar o grande dispêndio de atividades, tais como o controle, acompanhamento, fiscalização do contrato e execução financeira, que poderá ocasionar prejuízo ao erário público, bem como para resguardar a qualidade do produto ofertado e ainda a contratação por um único lote ampliará a concorrência.
- 10.4. Vale salientar, que o presente certame ao ser agrupado por lote, se torna economicamente e tecnicamente viável, onde esta divisão não trará elevação de custos e não afetará a integridade do objeto.
- 10.5. É de asseverar que a licitação divida em lotes por gênero, demonstra-se ser economicamente viável a aquisição, haja vista alguns itens serem de gêneros diferentes, onde haveria dificuldades para licitar, visto que é possível que uma única empresa não seria capaz de ofertar todos os itens.
- 10.6. Em que pese as razões expendidas, é imprescindível Súmula n.º 08 do TCE/RO 16 de setembro de 2014 DOE nº 753 p. 5:

"A Administração Pública em geral deverá restringir a utilização do critério de julgamento menor preço por lote, reservando-a àquelas situações em que a fragmentação em itens acarretar a perda do conjunto; perda da economia de escala; redundar em prejuízo à celeridade da licitação; ocasionar a excessiva pulverização de contratos ou resultar em contratos de pequena expressão econômica, observadas as seguintes condições cumulativas:

a) apresentar justificativa que demonstre a motivação para a utilização do critério de julgamento menor preço por lote;

b) prever quantidade restrita de itens por lote;

c) proceder ao agrupamento por lote de itens que guardem homogeneidade entre si, isto é, considerando-se a natureza e características dos itens, possam ser fornecidos por um mesmo fornecedor, concretizando, assim, os princípios da competitividade e igualdade;

d) estabelecer no instrumento convocatório a definição das unidades e das quantidades a serem adquiridas em função do consumo e utilização prováveis, cuja estimativa será obtida, sempre que possível, mediante adequadas técnicas quantitativas de estimação;

e) proceder à rigorosa, ampla e irrestrita pesquisa de preços de mercado vigente na data da licitação;

f) prever no edital a desclassificação da proposta se contemplar valor unitário (item) e/ou global (lote) acima do valor de mercado;

g) contemplar no critério de julgamento previsto no edital além dos valores unitários dos itens, a estimativa de quantidade a ser adquirida por item no prazo de validade do registro;

h) considerar no julgamento da proposta o resultado mais vantajoso à Administração Pública ao se efetuar a comparação entre “a soma dos preços por item no lote” e a “somatória dos preços dos itens do lote, multiplicado pela estimativa de consumo”; e

i) fazer menção expressa no Edital de que compete ao pregoeiro diligenciar, se, no curso da licitação, depreender indício de que o levantamento prévio de preços padece de fragilidade, a exemplo da disparidade entre o preço inicialmente previsto e o preço ofertado pelos participantes."

- 10.7. Além disso, constata-se também Acórdão 1650/2020 Plenário, conforme descrito abaixo:

Licitação. Registro de preços. Lote (Licitação). Adjudicação. Preço global. Preço unitário.

Nas licitações para registro de preços, a modelagem de aquisição por preço global de grupo de itens é medida excepcional que precisa ser devidamente justificada, a ser utilizada apenas nos casos em que a Administração pretende contratar a totalidade dos itens do grupo, respeitadas as proporções de quantitativos definidos no certame. Apesar de essa modelagem ser, em regra, incompatível com a aquisição futura de itens isoladamente, admite-se tal hipótese quando o preço unitário ofertado pelo vencedor do grupo for o menor lance válido na disputa relativa ao item.

- 10.8. Desse modo, demonstra-se ser conveniente e oportuno que não haja o parcelamento do objeto, haja vista que caso a licitação seja por item, poderá a empresa vencedora de um dos itens por circunstância gerais não entregar, prejudicando num todo, pois cada item preenche o outro, sendo desse modo imprescindível que a contratação ocorra em lotes.
- 10.9. Considerando os princípios da economicidade, legalidade, impessoalidade, celeridade, igualdade, vinculação ao instrumento convocatório e julgamento objetivo, deve-se observar a não ocorrência de fracasso da contratação, e incorrer no planejamento anual desta Secretaria.
- 10.10. A contratação por lotes se fundamenta no fato de que os itens formam um conjunto, e diante da não realização do certame por grupo de itens, se sagrarem-se vencedoras empresas diversas, poderíamos incorrer no problema de que esta única empresa não poderia disponibilizar todos os materiais pertinentes, por tratarem-se de gêneros diferentes.
- 10.11. Podemos verificar que a licitação em lotes é perfeitamente possível, visto que, a junção dos itens específicos em lotes, dá-se em virtude por tratar-se de um conjunto de materiais que servirão a um mesmo fim específico, e para o mesmo local.

10.12. Visto ainda que, se adquiridos em lote, em virtude de sua quantidade, conforme evidenciado acima quanto ao mecanismo de "economia de escala", poderá ser adquirido a preços mais baixos pela administração, evidenciando assim o atendimento aos princípios da economicidade e eficiência.

11. **DA CONTRATAÇÃO DE PESSOA FÍSICA E SOCIEDADE COOPERATIVA:**

11.1. Em atenção ao art. 34, inciso XIV do Decreto Estadual nº 28.874/2024 e art. 16 da [Lei nº 14.133, de 01 de abril de 2021](#), justifica-se a exclusão de participação de pessoas físicas e de sociedades em forma de cooperativa no presente processo, considerando que a Administração Pública tem a obrigação de garantir a segurança e a qualidade dos itens que contrata ou adquire.

11.2. Em razão disso, é importante que os contratados tenham a capacidade técnica e a estrutura necessária para prestar o serviço de forma adequada.

11.3. Desta forma, as pessoas físicas e sociedades em forma de cooperativa, podem não possuir a mesma capacidade técnica e estrutura que empresas especializadas.

11.4. Por isso, a participação de pessoas físicas e sociedades em forma de cooperativa na aquisição pretendida pode colocar em risco a segurança e a qualidade dos serviços a serem prestados.

12. **DA JUSTIFICATIVA**

12.1. A prática em adotar uma postura no âmbito cibernético é cada vez mais necessário quando falamos em segurança de endpoints, uma vez que estes dispositivos (estações de trabalho e servidores virtuais) são o ponto de entrada para atividades maliciosas de pessoas e grupos criminosos que praticam tais atividades.

12.2. Considera-se de grande importância, a identificação e a mitigação de tal atividade e/ou comportamento fora do comum executado em um endpoint, através de técnicas e procedimentos que possam identificar e categorizar o tipo de ameaça detectada, trazendo uma visão geral dos riscos e ameaças presentes no ambiente computacional desta Sedam.

12.3. Por diversos momentos, a ferramenta de antivírus usada atualmente a mais de 3 anos "Kasperky Endpoint Security", mostrou-se ineficaz em detecções e problemática para na usabilidade e implementação nesta Sedam, tendo um alto consumo de recursos de hardware, regras que não aplicam de forma eficaz em ambientes distintos (interno e externo), problemas de atualizações para estações de trabalho e servidores de administração, pouca ou nenhuma visibilidade do atual ambiente de ameaças, falha na contenção de infecções, falha em processar arquivos infectados, causando problemas para o usuário final que apenas usa de sua estação de trabalho para executar suas atividades diárias, causando-lhe morosidade, lentidão devido ao processamento do atual antivírus.

12.4. Nos dias atuais, o conceito de antivírus mudou de Endpoint detection and response (EDR) para Extended detection and response (XDR), o que representa uma evolução de tecnologia, não sendo somente um antivírus comum que aguarda o vírus comprometer o equipamento para depois ele comparar se aquele arquivo malicioso já foi detectado e possui uma vacina conhecida, possuindo agora com o conceito de XDR, detecções comportamentais, inteligência artificial, detecções baseadas em heurística, tempo real, Ameaças Persistentes Avançadas (APT), Phishing, análise avançada de malwares, dentre outras, trazendo uma visão muito mais assertiva e de fácil tomada de decisão para o administrador.

12.5. **RELATÓRIO DE VULNERABILIDADES - 6 DE JUNHO DE 2024 11:04:05**

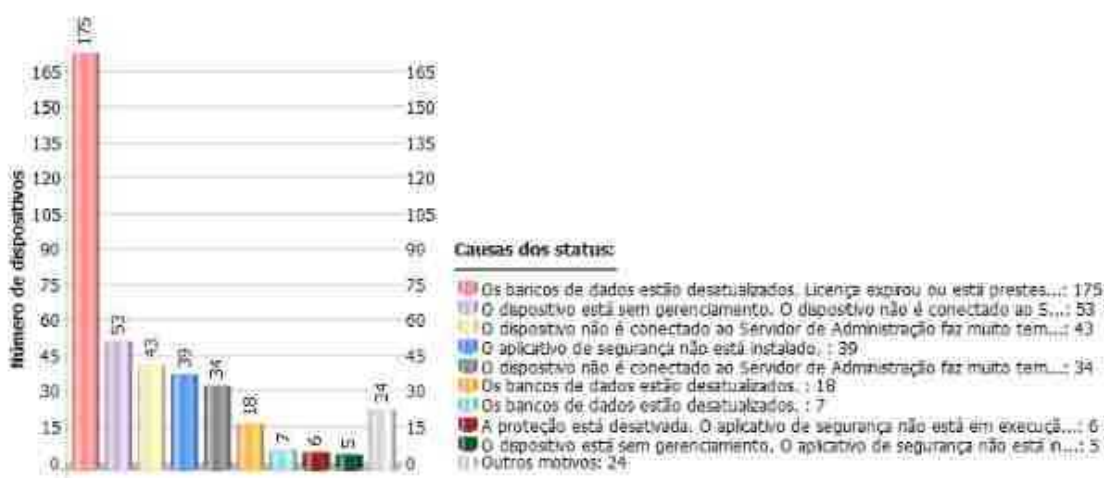


12.6.

12.7. O relatório acima, obtido pelo antivírus Kaspersky, utilizado atualmente nesta Sedam, aponta de 393 dispositivos apresentam vulnerabilidades críticas, mas o mesmo não detalha facilmente o motivo e nem alerta o administrador das possíveis vulnerabilidades em que os dispositivos são afetados.

12.8. Isso mostra a falta de visibilidade e detalhamento de ameaças provido pelo antivírus já depreciado pelo mercado de segurança de endpoints.

12.9. **RELATÓRIO DO STATUS DE PROTEÇÃO - 6 DE JUNHO DE 2024 10:58:50**



12.10.

12.11. Já o outro relatório acima, indica por quais motivos (de forma superficial), os status dos endpoints, sendo em grande maioria, a falta de atualização do banco de dados de antivírus, motivo esse, causado pela expiração da licença, impactando em um parque de computadores e servidores totalmente desprotegido, correndo grandes riscos de parada devido a ameaça de incidente.

12.12. A segurança da rede da Secretaria de Estado do Desenvolvimento Ambiental - SEDAM, depende da utilização de recursos de segurança cibernética, que incluem várias camadas de proteção para monitorar o comportamento dos usuários, estações de trabalho e servidores, com o objetivo de proteger o ambiente da Secretaria contra ameaças básicas e avançadas.

12.13. É fundamental tratar a informação como um recurso estratégico e econômico, devido à crescente valorização dos dados pessoais e da informação como ativos de gestão do Estado. O uso inadequado desses recursos oferece um alto risco de impactos negativos e pode resultar em consequências indesejadas, como prejuízo financeiro, problemas operacionais, danos à imagem do órgão ou governo, vazamento de informações e dados pessoais, e até mesmo sequestro de dados.

12.14. A SEDAM possui um parque computacional para atendimento aos usuários, com mais de 500 usuários ativos na rede, mais de 60 servidores virtuais dentre outros recursos, de acordo com o levantamento realizado no ambiente de infraestrutura de TI. A aferição do comportamento das estações de usuários e servidores virtuais, tem como objetivo detectar, bloquear, investigar e responder a incidentes de segurança da informação que possam ocorrer na rede da Secretaria.

12.15. É essencial garantir a proteção e a integridade dos dados e sistemas da SEDAM, bem como a segurança dos usuários e da informação compartilhada. Portanto, é necessário implementar medidas de monitoramento contínuo, análise de logs, detecção de anomalias e resposta rápida a incidentes, a fim de mitigar riscos e garantir um ambiente seguro e confiável para as operações da Secretaria.



12.16. Diante desse cenário, é fundamental investir em estratégias robustas de segurança da informação, incluindo a implementação de sistemas de detecção e prevenção de ameaças, atualizações regulares de software e hardware, treinamento e conscientização dos usuários, além de políticas de segurança claras e bem definidas. Além disso, é importante contar com equipes especializadas em segurança cibernética, capazes de identificar e responder rapidamente aos incidentes, minimizando danos e prejuízos.

12.17. A proteção dos dados pessoais e a segurança das informações são responsabilidades compartilhadas, exigindo a colaboração de todos os usuários e organizações. É essencial promover uma cultura de segurança, estimulando a adoção de boas práticas e a conscientização sobre os riscos existentes. Somente assim poderemos enfrentar os desafios cada vez mais frequentes e sofisticados no mundo da segurança cibernética e garantir a integridade e confidencialidade dos dados de forma eficaz.

12.18. Portanto, é crucial fornecer à SEDAM recursos de segurança atualizados, capazes de monitorar e responder a infecções causadas por software malicioso desenvolvido por indivíduos com más intenções. Esses recursos abrangem desde a exposição simples de informações obtidas até a exigência de pagamento de resgate para a liberação de dados sequestrados, como ocorre nos ataques de ransomware. Além disso, é essencial que esses recursos garantam a detecção proativa de ameaças, a implementação de medidas preventivas, a resposta rápida a incidentes e a recuperação eficiente dos sistemas afetados.

12.19. Dessa forma, a contratação de recursos adicionais para cumprir com a LGPD é uma medida indispensável para garantir a proteção e preservar a privacidade dos usuários da SEDAM. Ao implementar as medidas de proteção adequadas, a secretaria estará em conformidade com a legislação vigente, assegurando a confidencialidade, integridade e disponibilidade dos dados pessoais sob sua responsabilidade.

#### 12.20. **NECESSIDADE DO NEGÓCIO:**

12.21. A contratação em questão tem como objetivo atender às necessidades de segurança da SEDAM, garantindo o cumprimento das diretrizes da Lei Geral de Proteção de Dados Pessoais (LGPD), implantação futura do Plano Diretor de Tecnologia da Informação PDTI e da Política de Segurança da Informação (PSI) dentre outras legislações relacionadas à segurança cibernética.

12.22. O objetivo em questão visa minimizar a vulnerabilidade dos sistemas corporativos, redes, estações de trabalho, caixas postais, implementando metodologias de segurança de antivírus corporativo, prevenindo possíveis ataques internos e externos de vírus, spams e spywares e outras ameaças virtuais ao ambiente tecnológico da Secretaria.

12.23. Além disso, a contratação visa estabelecer práticas de segurança cibernética sólidas, alinhadas com as melhores práticas e padrões do setor. Esse enfoque na segurança cibernética é essencial para mitigar riscos e proteger a integridade dos dados da Secretaria, sendo fundamental para garantir um ambiente seguro e confiável para a manipulação e proteção dos dados pessoais, cumprindo as exigências legais e fortalecendo a postura de segurança da secretaria.

### 13. **DA ENTREGA E DOS CRITÉRIOS DE ACEITAÇÃO DO OBJETO**

#### 13.1. **Local de Entrega:**

13.1.1. Havendo a necessidade de entrega de equipamento para compor a solução, a entrega do mesmo deverá ocorrer a contar do recebimento da Nota de Empenho, nas dependências da Gerência de Patrimônio e Almoxarifado - GPA, sito à Estrada do Santo Antônio, nº 5323, bairro triangulo, CEP 76805-696, Porto Velho – RO, no horário das 07:30 às 13:30 horas, sempre através de documento hábil que comprove as quantidades recebidas, indicando o nome e matrícula do responsável pelo recebimento.

13.1.2. A data prevista da entrega deverá ser informada com antecedência mínima de 48 (quarenta e oito) horas através do telefone (3216-1072 – GPA).

13.1.3. Na entrega dos produtos/serviços deverão fazer-se acompanhar, além da nota fiscal/fatura, e o certificado de garantia.

#### 13.2. **Prazo/Cronograma de Entrega:**

13.2.1. A Contratação será realizada mediante solicitação da SEDAM, conforme a necessidade/demanda.

13.2.2. A entrega deverá ocorrer no prazo de até 20 (vinte) dias corridos , após o recebimento da nota de empenho e ordem de fornecimento.

13.2.3. Findo o prazo previsto no item anterior, a contratada terá um prazo adicional de até 10 (dez) dias de tolerância, para entrega dos materiais, a critério do ordenador de despesas, desde que, comunique o fato a contratante com antecedência mínima de 48 (quarenta e oito) horas do término do prazo, acompanhado de justificativa que comprove o impedimento para o cumprimento da obrigação, no qual esta Secretaria por sua vez, decidirá a possibilidade de prorrogação do prazo, ou determinará a cominação das multas cabíveis, que ocorrerá a partir da efetiva notificação.

#### 13.3. **Do recebimento:**

13.4. O recebimento, conforme o art. 140 da [Lei nº 14.133, de 01 de abril de 2021](#), se dará na forma abaixo:

#### 13.5. **Do recebimento provisório:**

13.5.1. Serão os objetos deste Termo de Referência recebidos **PROVISORIAMENTE, pelo seu responsável por seu acompanhamento e fiscalização**, para efeito da verificação da conformidade dos materiais/serviços fornecidos, em relação à qualidade e quantidades conforme especificações exigidas, o prazo máximo de 10 (dez) dias úteis contados da data de sua efetiva entrega.

13.5.2. O fiscal do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico, no qual elaborará o laudo de averiguação.

13.5.3. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

13.5.4. Independente de aceitação, a **CONTRATADA** garantirá a qualidade e segurança dos objetos contra defeitos de fabricação, pelo prazo mínimo de 12 (doze) meses, bem como oferecer durante todo o prazo de garantia, efetuando a substituição do produto no prazo de 10 (dez) dias corridos, evitando assim a descontinuidade dos serviços desta Secretaria.

#### 13.6. **Do recebimento definitivo:**

13.6.1. Serão os objetos deste Termo de Referência recebidos **DEFINITIVAMENTE**, por servidor ou comissão designada pela autoridade competente, após a comprovação da qualidade e quantidades entregues, conforme especificações exigidas, no prazo máximo de 10 (dez) dias da emissão do **TERMO DE RECEBIMENTO PROVISÓRIO**;

13.7. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da lei nº 14.133 de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertinente à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

13.8. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

#### 13.9. **Das condições gerais de recebimento de bens:**

13.9.1. Todos os bens deverão ser entregues em perfeito estado de conservação e utilização.

13.9.2. **O recebimento provisório ou definitivo**, não exclui a responsabilidade civil, pela qualidade, correção solidez, e segurança do objeto contratual, nem ético profissional, pela perfeita execução do contrato;

13.9.3. Não serão recebidos ainda que provisoriamente serviços que:

a) Sejam entregues para recebimento com as especificações diferentes das contidas neste Termo de Referência;

13.9.4. Os bens/serviços deverão obedecer as especificações do objeto, bem como todas as outras condições previstas neste Termo de Referência.

13.9.5. O prazo de entrega somente poderá ser prorrogado mediante o cumprimento, pela **CONTRATADA**, dos seguintes requisitos cumulativos:

a) solicitação de prorrogação protocolada dentro do prazo de entrega;

b) comprovação documental da ocorrência de motivo imprevisível (caso fortuito, força maior ou fato do príncipe), ocorrido depois da apresentação de sua proposta, que tenha correlação direta de causa e efeito sobre a necessidade do atraso.

13.10. Não se admitirá prorrogação se:

- a) o atraso ocorrer por culpa da **CONTRATADA**;
- b) se não cumprir os requisitos da entrega/execução do objeto; ou
- c) houver interesse público devidamente justificado nos autos que demonstre ser a escolha mais vantajosa para a administração.

13.11. As faturas de bens ou serviços serão recebidos e analisados pela comissão nomeada através da portaria vigente na data de elaboração deste Termo de Referência, na sede desta SEDAM, sito à Av. Farquar, nº 2986, Bairro Pedrinhas, Edifício Rio Cautário, Curvo 2, 2º andar, CEP 76.801-361 – Porto Velho – RO, telefone nº (69)98482-8704, no horário das 07:30 às 13:30 horas de segunda à sexta.

13.11.1. Os bens/serviços deverão obedecer as especificações do objeto, bem como todas as outras condições previstas neste Termo de Referência.

13.11.2. A execução do contrato deverá ser acompanhada e fiscalizada por 1 (um) fiscal de contrato, ou membros de comissão de fiscalização, representantes da Administração especialmente designados conforme requisitos estabelecidos no art. 7º da [Lei nº 14.133, de 01 de abril de 2021](#), ou pelos respectivos substitutos, permitida a contratação de terceiros para assisti-los e subsidiá-los com informações pertinentes a essa atribuição.

14. **ESTIMATIVA DA DESPESA:**

14.1. Informamos que diante da especificidade da referida contratação, a estimativa da presente contratação será definida pela Superintendência Estadual de Licitações, por meio da montagem de Quadro estimativo de licitações.

15. **DO PRAZO E CONDIÇÕES DE GARANTIA**

15.1. A garantia dos referidos serviços concernentes ao objeto deste Termo de Referência serão regidos conforme os dispositivos da Lei 8.078/90 (Código de Defesa do Consumidor - CDC), bem como o disposto na [Lei nº 14.133, de 01 de abril de 2021](#).

15.2. Os serviços deverão fazer-se acompanhar da nota fiscal discriminativa para efetivação de sua entrega, bem como o termo de garantia contra defeito de fabricação.

15.3. A garantia deverá ser fornecida com prazo mínimo de 36 (trinta e seis) meses, contadas a partir da emissão do Termo de Recebimento Definitivo emitido por esta Secretaria, nos moldes descritos no item 13.6.

15.4. A garantia deverá atender a todos os componentes físicos e lógicos que fazem parte do objeto do presente instrumento;

15.5. Em caso de garantia superior ao previsto no subitem 15.3 não poderá esta impor nenhum custo adicional a contratante.

15.6. O pedido de substituição ou reparo do objeto, durante o período de garantia, poderá ser formalizado por telefone, e-mail, ofício ou outro meio hábil de comunicação disponibilizado pela CONTRATADA.

16. **DA HABILITAÇÃO**

16.1. Será exigida a habilitação: jurídica, técnica, fiscal, social/trabalhista e econômico-financeira, conforme disposto nos **arts. 62 ao 70 da Lei nº 14.133 de 01 de abril de 2021**, bem como obediência ao **Decreto Estadual nº 28.874 de 25 Janeiro de 2024**.

16.2. Concluído a fase de aceitação ocorrerá a fase de habilitação da(s) licitante vencedora(s);

16.3. **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 microempresa ou empresa de pequeno porte:** certidão expedida pela Junta Comercial ou pelo Registro Civil das Pessoas Jurídicas, conforme o caso, que comprove a condição de microempresa ou empresa de pequeno porte, segundo determinado pelo Departamento de Registro Empresarial e Integração - DREI, podendo ser substituída por outro documento que comprove o atual enquadramento na condição de microempresa e empresa de pequeno porte, tendo em vista a desburocratização e simplificação da função administrativa do Estado;
- e) **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;
- f) **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](#);
- g) **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 nº 11.802, de 28/11/2023.
- h) **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.
- i) **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.

16.3.1. Os documentos supramencionados deverão estar acompanhados da última alteração ou da consolidação respectiva.

16.3.2. Procuração por instrumento público, comprovando a delegação de poderes para assinatura e rubrica dos documentos integrantes da habilitação e propostas, quando estas não forem assinadas por diretor(es), com poderes estatutários para firmar compromisso;

16.3.3. A documentação de habilitação da licitante poderá ser substituída pelo Sistema de Cadastramento de Fornecedores (SICAF) ou pelo Certificado de Registro Cadastral, expedido pela Superintendência Estadual de Compras e Licitações – SUPEL/RO, nos documentos por eles abrangidos.

16.4. **Qualificação Técnica**

16.4.1. No que tange a qualificação técnica, será exigido atestados da empresa licitante, em conformidade com o art. 67 da Lei Federal 14.133 de 01 de abril de 2021:

Art. 67. A documentação relativa à qualificação técnico-profissional e técnico-operacional será restrita a:

[...]

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

§ 1º A exigência de atestados será restrita às parcelas de maior relevância ou valor significativo do objeto da licitação, assim consideradas as que tenham valor individual **igual ou superior a 4% (quatro por cento) do valor total estimado da contratação (grifo nosso)**

§ 2º Observado o disposto no **caput** e no § 1º deste artigo, será admitida a exigência de atestados com **quantidades mínimas de até 50% (cinquenta por cento)** das parcelas de que trata o referido parágrafo, vedadas limitações de tempo e de locais específicos relativas aos atestados. **(grifo nosso)**

[...]

§ 5º Em se tratando de serviços contínuos, o edital poderá exigir certidão ou atestado que demonstre que o licitante tenha executado serviços similares ao objeto da licitação, em períodos sucessivos ou não, por um prazo mínimo, que não poderá ser superior a 3 (três) anos. (grifo nosso)

16.4.2. Em atenção ao estabelecido na sobredita norma, para a presente aquisição dever-se-á apresentar atestados compatível em quantidade o(s) e características, em sua individualidade ou soma que contemple a entrega de serviços condizentes com o percentual de 10% (dez por cento) desta licitação, apenas para os itens 01 e 02, sendo estes de maior relevância.

16.4.2.1. Entende-se por pertinente e compatível em **características - o bem com características semelhantes ao** objeto do presente termo de referência, a fim de demonstrar atuação na atividade no ramo de negócio.

16.4.2.2. Entende-se por pertinente e compatível em **quantidade - fornecimento de bem no montante mínimo exigido para item ou lote**, com quantidade expressa em unidade ou valor convergente ao do presente termo de referência, com o fito de atestar que suporta a demanda a que será submetido.

16.4.3. O atestado deverá indicar dados da entidade emissora (razão social, CNPJ, endereço, telefone, fax, data de emissão) e dos signatários do documento (nome, função, telefone, etc.), além da descrição do objeto e quantidade expressa em valor, este último quando possível.

16.4.4. O atestado e/ou declaração emitido por pessoa de direito público deverá constar órgão, cargo e matrícula do emitente.

#### 16.5. **Qualificação Econômico Financeira:**

a) **Balanco Patrimonial**, ou o Balanco de Abertura dos 02 (dois) dois últimos anos, ou do último exercício caso a licitante tenha sido constituída em menos de um ano, devidamente autenticado ou registrado na Junta Comercial do Estado, para que o(a) Pregoeiro(a) possa aferir se esta possui Patrimônio Líquido (licitantes constituídas há mais de um ano) ou Capital Social (licitantes constituídas há menos de um ano), de 10% (dez por cento) do valor estimado do item/ lote que o licitante estiver participando, conforme art. 69, § 4º da Lei 14.133/2021.

a.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;

a.2) Caso seja constatada a insuficiência de patrimônio líquido ou capital social para a integralidade dos itens/lotos 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;

a.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).

a.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)

a.5) As regras descritas nos itens acima, deverão ser observadas em caso de ulterior classificação de licitante que já se consagrou classificado em outro item(ns)/lote(s).

b) **Certidão Negativa de feitos sobre falência** – [Lei nº 11.101, de 09 de fevereiro de 2005](#) - expedida pelo distribuidor da sede do licitante, expedida nos últimos **90 (noventa)** dias caso não conste o prazo de validade;

b.1) Na hipótese de apresentação de Certidão Positiva de recuperação judicial, o (a) Pregoeiro verificará se a interessada teve seu plano de recuperação judicial homologado pelo juízo, conforme determina o art. 58 da [Lei nº 11.101, de 2005](#).

b.2) Caso a empresa interessada não obteve acolhimento judicial do seu plano de recuperação judicial, a interessada será inabilitada, uma vez que não há demonstração de viabilidade econômica.

#### 16.6. **Regularidade Fiscal**

16.6.1. A regularidade fiscal será baseada conforme dispõe o art. 63, inciso III da [Lei nº 14.133, de 01 de abril de 2021](#).

a) **Prova de regularidade fiscal perante a Fazenda Nacional**, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta [nº 1.751, de 02/10/2014](#), do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional;

b) **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;

c) **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;

d) **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

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

#### 16.7. **Regularização Trabalhista**

a) **Certidão de Regularidade perante a Justiça do Trabalho - CNDT** ([Lei nº 12.440, de 07 de julho de 2011](#), Art. 642-A), admitida comprovação também por meio de “certidão positiva, com efeito, de negativa” diante da existência de débito confesso, parcelado e em fase de adimplemento.

#### 16.8. **Das declarações:**

a) Declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, conforme inciso IV do § 1º do art. 63 da Lei 14.133/21.

b) Apresentar declaração, sob as penas da lei e em cumprimento ao art. 68 inciso VI da Lei nº 14.133/21, que não utiliza em trabalho noturno, perigoso ou insalubre mão-de-obra de menores de 18 (dezoito) e de qualquer trabalho a menores de 16 (dezesseis) anos, salvo na condição de aprendiz, a partir de 14 (quatorze) anos, nos termos do art. 7º, Inciso XXXIII, [Constituição Federal](#), redação dada pela [Emenda Constitucional nº 20, de 15 de dezembro de 1998](#).

16.8.1. A apresentação de certidões positivas com efeito de negativa, serão aceitas nas mesmas condições, quanto a sua validade e efeitos, tendo em vista a sua emissão diante da exigência de débito confesso, parcelamento e em fase de adimplemento.

#### 16.9. **Justificativa para exigência da qualificação econômico financeira e atestado de capacidade técnica:**

16.9.1. A exigência de apresentação de qualificação econômico financeira atende aos preceitos trazidos pela [Lei nº 14.133, de 01 de abril de 2021](#), em seu art. 69, § 4º da referida lei, visto que a documentação **DEVERÁ** ser exigida em aquisições e contratações que ultrapassem 1/4 (um quarto) do limite para dispensa de licitação para compras em geral, conforme exposto abaixo:

Art. 69. A habilitação econômico-financeira visa a demonstrar a aptidão econômica do licitante para cumprir as obrigações decorrentes do futuro contrato, devendo ser comprovada de forma objetiva, por coeficientes e índices econômicos previstos no edital, devidamente justificados no processo licitatório, e será restrita à apresentação da seguinte documentação:

I - balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais;

Art. 70. A documentação referida neste Capítulo poderá ser:

III - dispensada, total ou parcialmente, nas contratações para entrega imediata, nas contratações em valores inferiores a 1/4 (um quarto) do limite para dispensa de licitação para compras em geral e nas contratações de produto para pesquisa e desenvolvimento até o valor de R\$ 300.000,00 (trezentos mil reais).



- 16.9.2. Logo, considerando o valor estimado para a presente licitação, não há possibilidade de dispensa do referido documento.
- 16.9.3. No que tange a solicitação de apresentação de atestado de capacidade técnica, informamos que para a presente licitação serão fornecidos solução de proteção para estações de trabalho de servidores contra ataques cibernéticos, A prática em adotar uma postura no âmbito cibernético é cada vez mais necessário quando falamos em segurança de endpoints, uma vez que estes dispositivos (estações de trabalho e servidores virtuais) são o ponto de entrada para atividades maliciosas de pessoas e grupos criminosos que praticam tais atividades.
- 16.9.4. **Qualidade e Confiabilidade:** O atestado comprova que o fornecedor já forneceu licenças similares para outros clientes.
- 16.9.5. **Experiência no Mercado:** Exige-se o documento para verificar se o fornecedor possui histórico de entrega e atendimento às especificações técnicas.
- 16.9.6. Dessa forma, a exigência do atestado de capacidade técnica contribui para a seleção de fornecedores qualificados e garante maior eficiência e qualidade na prestação de serviços.

17. **DO SISTEMA ORÇAMENTÁRIO**

- 17.1. As despesas decorrentes para a contratação de empresa especializada no serviço, objeto do presente instrumento, correrão por conta dos recursos consignados no orçamento da Secretaria de Estado do Desenvolvimento Ambiental - SEDAM, conforme a seguinte dotação orçamentária.
- 17.2. **Unidade Gestora:** 18001 - SEDAM; **Fontes:** 1.708.0.00001 e/ou 2.708.0.00001 - Transferência da União Referente à Compensação Financeira de Recursos Minerais; **P/A:** 2580 - PROMOVER A INOVAÇÃO NA GESTÃO, GOVERNANÇA E SOLUÇÕES TECNOLÓGICAS; **Elemento de Despesa:** 33.90.40 - Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica.

18. **CONDIÇÕES DE PAGAMENTO**

**Fundamentação Legal:** [Lei nº 14.133, de 01 de abril de 2021](#) e **Decreto Estadual nº 28.874/2024**.

- 18.1. O pagamento das notas fiscais seguirá os moldes definidos pela [Lei nº 14.133, de 01 de abril de 2021](#), descritos no art. 18, inciso III e art. 25 da referida lei.
- 18.2. O pagamento será efetuado mediante Nota Fiscal de Bens/Serviços certificada pela Comissão de Recebimento de Bens e Serviços e de acordo com o art. 117 da [Lei nº 14.133, de 01 de abril de 2021](#), que deverão ser apresentadas juntamente com a entrega dos serviços, devendo conter no corpo da referida Nota Fiscal/Fatura, a descrição do objeto, o número do contrato e o número da Conta Bancária da futura **CONTRATADA**, para efetivação do pagamento, o qual deverá ser realizado no prazo de até 15 (quinze) dias após a emissão de Termo de Recebimento Definitivo.
- 18.3. Na hipótese da apresentação de mais de uma nota fiscal/fatura, e, se alguma delas apresentarem erros ou dúvidas quanto à exatidão ou documentação, a **CONTRATANTE** poderá pagar apenas àquela que se encontra correta, no prazo fixado para pagamento, ressalvado o direito da **CONTRATADA** de reapresentar, para cobrança àquelas inexatas devidamente corrigidas, com as justificativas necessárias (nestes casos também a **CONTRATANTE** terá o prazo de até 15 (quinze) dias, a partir do recebimento, para efetuar uma análise e o pagamento, conforme art. 190 do Decreto Estadual nº 28.874/2024.
- 18.4. Nota(s) Fiscal (is)/Fatura (s) deverá (ao) vir acompanhada (s) das seguintes comprovações:

a) da regularidade fiscal, mediante as Fazendas Federal, Estadual e Municipal

b) do cumprimento das obrigações trabalhistas;

c) do relatório das manutenções realizadas, contemplando a descrição dos serviços, dos itens substituídos.

d) O cumprimento das obrigações trabalhistas, previdenciárias e as relativas ao FGTS.
- 18.5. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pela Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

$I=(TX/100)$

$365$

$EM = I \times N \times VP$ , onde:

$I = \text{Índice de atualização financeira};$

$TX = \text{Percentual da taxa de juros de mora anual};$

$EM = \text{Encargos moratórios};$

$N = \text{Número de dias entre a data prevista para o pagamento e a do efetivo pagamento};$

$VP = \text{Valor da parcela em atraso}.$

- 18.6. Ocorrendo erro no documento da cobrança, este será devolvido e o pagamento será sustado para que a **CONTRATADA** tome as medidas necessárias, passando o prazo para o pagamento a ser contado a partir de data da reapresentação do mesmo.
- 18.7. Caso se constate erro ou irregularidade na Nota Fiscal, a **ADMINISTRAÇÃO**, a seu critério, poderá devolvê-la, para as devidas correções, ou aceitá-las, com a glosa da parte que considerar indevida.
- 18.8. Na hipótese de devolução, a Nota Fiscal será considerada como não apresentada, para fins de atendimento das condições contratuais.
- 18.9. A administração não pagará, sem que tenha autorização prévia e formalmente, 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.
- 18.10. Os eventuais encargos financeiro, processuais e outros, decorrentes da inobservância, pela empresa de prazo de pagamento, serão de sua exclusiva responsabilidade.
- 18.11. A **ADMINISTRAÇÃO** efetuará retenção, na fonte, dos tributos e contribuições sobre todos os pagamentos à **CONTRATADA**, conforme Instrução Normativa nº 34/2023/SEFIN-COTES.
19. **DO ACOMPANHAMENTO E FISCALIZAÇÃO**
- 19.1. A execução do Contrato, nos termos da [Lei nº 14.133, de 01 de abril de 2021](#), em seu art. 117, será acompanhada e fiscalizada por servidores da Gerência de Patrimônio e Almoxarifado - GPA e Gerência de Contratos - GCON, que serão oportunamente designados pela Coordenadoria de Patrimônio Administração e Finanças e/ou Diretoria Executiva e/ou Gabinete.
- 19.2. A responsável pela fiscalização e acompanhamento do processo será **Victor da Silva Tavares, Matrícula: \*\*\*.\*\*\*.597, E-mail: victortavares@sedam.ro.gov.br**.
- 19.3. Será anotado em registro próprio todas as ocorrências relacionadas com o recebimento dos objetos, determinando o que for necessário à regularização das faltas ou defeitos observados, e atestará as notas fiscais/faturas apresentadas, para fins de pagamento, conforme traz o art. 117, § 1º da [Lei nº 14.133, de 01 de abril de 2021](#).
- 19.3.1. Conforme traz o art. 20 do Decreto Estadual nº 28.874/2024, as atribuições do **Gestor do Contrato**, serão:

- Art .20. 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;
- [...]

19.4. No que tange as atribuições vinculadas ao **Fiscal do Contrato**, estão especificadas:

- Art. 22. A função de fiscal de contrato deve ser atribuída a servidor com experiência e conhecimento na área relativa ao objeto contratado, designado para auxiliar o gestor do contrato quanto à fiscalização dos aspectos administrativos e técnicos do contrato, cabendo-lhe, dentre outras atribuições inerentes à função:
- I - conhecer o termo de contrato e todos os seus Anexos, especialmente o Projeto Básico ou o Termo de Referência, certificando-se de que a contratada está cumprindo todas as obrigações assumidas;
  - II - confrontar os preços e quantidades constantes da nota fiscal com os estabelecidos no contrato;
  - III - no caso específico de obras e prestação de serviços de engenharia, cumpre ainda aos fiscais:
    - a) fazer constar todas as ocorrências no Diário de Obras, com vistas a compor o processo documental, de modo a contribuir para dirimir dúvidas e embasar informações acerca de eventuais reivindicações futuras, tomando as providências que estejam sob sua alçada e dando ciência ao gestor quando excederem as suas competências;
    - b) zelar pela fiel execução da obra, sobretudo no que concerne à qualidade dos materiais utilizados e dos serviços prestados, bem como quanto aos aspectos ambientais;
    - c) atestar o funcionamento de equipamentos e registrar a conformidade em documento;
    - d) acompanhar e analisar os testes, ensaios, exames e provas necessários ao controle de qualidade dos materiais, serviços e equipamentos a serem aplicados na execução do objeto contratado, quando houver;
    - e) informar ao gestor ocorrências que possam gerar dificuldades à conclusão da obra ou em relação a terceiros; e
    - f) proceder, conforme cronograma físico-financeiro, às medições dos serviços executados, conforme disposto em contrato.

19.5. A fiscalização da execução dos serviços abrange, ainda, as seguintes rotinas:

- a) Observar o fiel adimplemento das disposições contratuais;
- b) Solicitar a imediata substituição de funcionário da **CONTRATADA** que embaraçar ou dificultar o seu atendimento e a sua fiscalização, a seu exclusivo critério;
- c) Rejeitar, no todo ou em parte, os serviços fornecidos em desacordo com as especificações deste Termo de Referência;
- d) Suspender a execução do fornecimento contratados, sem prejuízo das penalidades a que se sujeita a **CONTRATADA**, garantido o contraditório e a ampla defesa.

19.6. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da **CONTRATADA**, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da **CONTRATANTE** ou de seus agentes e prepostos, de conformidade com o art. 120 da [Lei nº 14.133, de 01 de abril de 2021](#).

20. **DOS DEVERES E OBRIGAÇÕES**

20.1. **Da Contratante**

- a) Acompanhar e fiscalizar a execução do contrato, nos termos da [Lei nº 14.133, de 01 de abril de 2021](#) e Decreto Estadual nº 28.874/2024;
- b) Promover o acompanhamento e o recebimento do objeto, verificando se está em conformidade com o que foi solicitado nas especificações/quantitativos contidos neste Termo.
- c) Permitir o livre acesso dos empregados da **CONTRATADA** às dependências do contratante para tratar de assuntos pertinentes aos serviços contratados;
- d) Rejeitar, no todo ou em parte, os serviços e/ou objetos realizados em desacordo com o contrato;
- e) Proceder ao pagamento do contrato, na forma e no prazo pactuado;
- f) Comunicar prontamente à **CONTRATADA**, qualquer anormalidade no objeto do instrumento contratual ou equivalente, podendo recusar o recebimento, caso não esteja de acordo com as especificações e condições estabelecidas no Termo de Referência;
- g) Notificar previamente à **CONTRATADA**, quando da aplicação de sanções administrativa;
- h) Efetuar o pagamento à **CONTRATADA**, de acordo com o estabelecido neste Termo de Referência.
- i) Designar servidor habilitado responsável por acompanhar a realização dos serviços.
- j) Fiel observância ao que tange às prerrogativas da Administração Pública em relação ao Regime Jurídico dos contratos administrativos, consoante ao disposto na [Lei nº 14.133, de 01 de abril de 2021](#).

20.2. **Da Contratada/Fornecedor**

20.2.1. Além daquelas determinadas por leis, decretos, regulamentos e demais dispositivos legais que regem os procedimentos licitatórios e os princípios da administração pública, nas obrigações da **CONTRATADA**, além das previstas no presente Termo de Referência, também se incluem os dispositivos a seguir:

- a) Assinar o contrato ou retirar a nota de empenho quando convocada a fazê-lo, no prazo máximo de 10 (dez) dias.
- b) Comunicar a **CONTRATANTE**, verbalmente no prazo de 12 (doze) horas e, por escrito, no prazo de 48 (quarenta e oito) horas, quaisquer alterações ou acontecimento que impeçam mesmo temporariamente, de cumprir seus deveres e responsabilidades relativos à execução da Nota de Empenho, total ou parcialmente, por motivo de caso fortuito ou força maior;
- c) Cumprir fielmente o prazo estabelecido no presente Termo de Referência para o fornecimento do objeto constante do mesmo;
- d) Responsabilizar-se, integralmente, pela entrega dos serviços, não podendo repassar nenhum dos itens do presente a terceiros;
- e) Responsabilizarem-se, integralmente, por todos os tributos, taxas e contribuições (inclusive para-fiscais), que direta ou indiretamente, incidam ou vierem a incidir sobre a presente contratação;
- f) Responsabilizar-se pelos atrasos e/ou prejuízos decorrentes de paralisação parcial ou total da entrega dos materiais/bens;
- g) Permitir e oferecer condições para a mais ampla e completa fiscalização durante a vigência do Contrato;
- h) Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no TR, informando à Secretaria qualquer adversidade, nos termos do Art. 92, inciso XVI da [Lei nº 14.133, de 01 de abril de 2021](#);
- i) Responsabilizar-se totalmente e as suas expensas com (impostos, taxas e pessoal) pelo transporte/frete dos bens/materiais até o destino final, bem como, quando apresentar defeitos de qualquer natureza, correrá por conta e risco da **CONTRATADA**;
- j) Prestar todos os esclarecimentos que lhe forem solicitados no concernente ao objeto do presente Termo de Referência, inclusive documentação e atos praticados até o recebimento definitivo e cujas reclamações formalmente realizadas obriga-se a atender prontamente;
- k) Responder, integralmente, por perdas e danos que vier a causar à **CONTRATANTE** ou a terceiros, em razão de ação ou omissão dolosa ou culpa, sua ou dos seus prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita;

- l) Responsabilizar-se pelos encargos trabalhistas, previdenciários e comerciais, bem como pelos custos de frete e de tributos, resultantes da execução do contrato;
- m) Prover todos os meios necessários à garantia da plena operacionalidade do fornecimento, inclusive considerados os casos de greve ou paralisação de qualquer natureza;
- n) Apresentar Nota Fiscal onde constem detalhadamente indicações de marca, fabricante, modelo, tipo, procedência e prazo de garantia;
- o) Garantir a titularidade e/ou permissão de uso de todo e qualquer direito de propriedade industrial envolvido nos bens, assumindo a responsabilidade por eventuais ações e/ou reclamações, de modo a assegurar à SEDAM a plena utilização dos bens adquiridos, ou a respectiva indenização;
- p) Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, [Lei nº 8.078, de 11 de setembro de 1990 \(Código de Defesa do Consumidor\)](#);
- q) Prestar todo o suporte solicitado, sem ônus para a **CONTRATANTE**, seja via telefone, seja através de correio eletrônico, seja, ainda, presencialmente.
- r) Responsabilizar-se quanto a reparação, correção, remoção, reconstrução ou substituição, no total ou em parte, o objeto em comento caso seja verificado vícios, defeitos ou incorreções resultantes da execução ou do material empregado, conforme determina o art. 119 da [Lei nº 14.133, de 01 de abril de 2021](#);
- s) pelo adequado tratamento de dados pessoais, seguindo instruções fornecidas pelo Contratante e observando suas próprias instruções e normas sobre a matéria;
- t) pelo registro das operações de tratamento de dados pessoais;
- u) pela guarda de sigilo dos dados pessoais tratados ou por informações de cunho restrito ou confidencial que tenha acesso em decorrência da execução do contrato;
- v) pela formulação de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao objeto do contrato;
- w) pela adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;
- x) por notificar/informar imediatamente à Contratante os casos de incidentes de segurança da informação que envolvam o objeto de contrato;
- y) pelo descarte seguro dos dados pessoais tratados após o término de seu tratamento;
- z) pelo não compartilhamento dos dados pessoais com outras organizações ou pessoas sem autorização da Contratante e nem tratá-los de forma incompatível com as finalidades do contrato;
- aa) por seguir as normas relativas ao tratamento de dados pessoais, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD), regulamentações expedidas pela Autoridade nacional de Proteção de Dados Pessoais (ANPD) e pelo Comitê Gestor de Privacidade e proteção de Dados Pessoais do Estado de Rondônia (CGPD); e
- ab) por seguir, no que couber, as orientações contidas nas normas ABNT NBR ISO/IEC 29151:2020 (estabelece objetivos de controle para atender aos requisitos identificados por uma avaliação de risco e impacto relacionada à proteção de dados pessoais) e ABNT NBR ISO/IEC 27701:2019 (especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação).

## 21. DA SUBCONTRATAÇÃO, CESSÃO E/OU TRANSFERÊNCIA

21.1. É vedada a subcontratação, cessão e/ou transferência total ou parcial do objeto deste termo de referência, conforme art. 122, §2º da [Lei nº 14.133, de 01 de abril de 2021](#).

## 22. DAS SANÇÕES

**Fundamentação Legal:** [Lei nº 14.133, de 01 de abril de 2021](#) e Decreto Estadual nº 28.874/2024.

22.1. Sem prejuízo das sanções cominadas no art. 156, I, III e IV, da [Lei nº 14.133, de 01 de abril de 2021](#), pela inexecução total ou parcial do contrato, a Administração poderá, garantida a prévia e ampla defesa, aplicar à **CONTRATADA** multa de até 10% (dez por cento) sobre a parcela inadimplida.

22.2. 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 total adjudicado*.

22.3. A interessada, adjudicatária ou **CONTRATADA** que, convocada dentro do prazo de validade de sua proposta, não celebrar o instrumento contratual, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a proposta, falhar ou fraudar na execução do instrumento contratual, comportar-se de modo inidôneo ou cometer fraude fiscal, garantida a prévia e ampla defesa, ficará impedida de licitar e contratar com a União, Estados Distrito Federal e Municípios, e será descredenciado no Cadastro de Fornecedores dos Órgãos da Administração Pública e Estadual, pelo prazo de até 03 (três) anos, sem prejuízo das multas previstas no Termo de Referência e das demais cominações legais, devendo ser incluída a penalidade no SICAFI e no CAGEFIMP - Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual;

22.4. 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) dias úteis, contados de sua intimação, para efetuar o pagamento da multa. Após esse prazo, não sendo efetuado o pagamento seus dados serão encaminhados ao órgão competente para que seja inscrita na dívida ativa, podendo, ainda a administração proceder à cobrança judicial da multa.

22.5. As multas previstas não eximem a adjudicatória ou **CONTRATADA** da reparação dos eventuais danos, perdas ou prejuízos que seu ato punível venha causar a Administração.

22.6. De acordo com a gravidade do descumprimento, poderá ainda a interessada 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 Administração pelos prejuízos resultantes e depois de decorrido o prazo da sanção aplicada com base na legislação vigente.

22.7. 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 significativo.

22.8. São exemplos de infrações administrativas, nos termos da [Lei nº 14.133, de 01 de abril de 2021](#), em seu art. 155, além do art. 156 conforme disposto abaixo:

Art. 155. O licitante ou o contratado será responsabilizado administrativamente pelas seguintes infrações:

I - dar causa à inexecução parcial do contrato;

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

III - dar causa à inexecução total do contrato;

IV - deixar de entregar a documentação exigida para o certame;

V - não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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



- VII - ensinar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;
- VIII - apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;
- IX - fraudar a licitação ou praticar ato fraudulento na execução do contrato;
- X - comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- XI - praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
- XII - praticar ato lesivo previsto no [art. 5º da Lei nº 12.846, de 1º de agosto de 2013](#).

Art. 156. Serão aplicadas ao responsável pelas infrações administrativas previstas nesta Lei as seguintes sanções:

- I - advertência;
- II - multa;
- III - impedimento de licitar e contratar;
- IV - declaração de inidoneidade para licitar ou contratar.

22.9. No caso de atraso injustificado na execução do contrato, a CONTRATADA estará sujeita à multa de mora, no valor de 0,4% do valor inicial contratado por dia, estando sujeita ainda as outras penalidades previstas neste Termo de Referência e/ou no Contrato, nos termos do art. 162 da [Lei nº 14.133, de 01 de abril de 2021](#), conforme citado abaixo:

Art. 162. O atraso injustificado na execução do contrato sujeitará o contratado a multa de mora, na forma prevista em edital ou em contrato.  
Parágrafo único. A aplicação de multa de mora não impedirá que a Administração a converta em compensatória e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções previstas nesta Lei.

22.10. 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.

22.11. Para efeito de aplicação de multas, às infrações são atribuídos graus, com percentuais de multa 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*
01	Permitir situação que crie a possibilidade ou cause dano físico, lesão corporal ou consequências letais; por ocorrência.	06	4,0% por dia
02	Usar indevidamente informações sigilosas a que teve acesso; por ocorrência	06	4,0% por dia
03	Suspender, interromper ou recusar-se, salvo por motivo de força maior ou caso fortuito, a entrega dos produtos e nas condições estabelecidas, por dia e por unidade de atendimento;	05	3,2% por dia
04	Destruir ou danificar documentos por culpa ou dolo de seus agentes; por ocorrência.	05	3,2% por dia
05	Recusar-se a executar serviço determinado pela FISCALIZAÇÃO, sem motivo justificado; por ocorrência;	04	1,6 % por dia
06	Manter funcionário sem qualificação para a execução dos serviços; por empregado e por dia.	03	0,8 % por dia
07	Executar serviço incompleto, paliativo substitutivo como por caráter permanente, ou deixar de providenciar recomposição complementar; por ocorrência.	02	0,4 % por dia
08	Fornecer informação pérfida de serviço ou substituição de material; por ocorrência.	02	0,4 % por dia
ITEM	Para os itens a seguir, deixar de:	GRAU	MULTA*
01	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
02	Refazer serviço não aceito pela FISCALIZAÇÃO, nos prazos estabelecidos no contrato ou determinado pela FISCALIZAÇÃO; por unidade de tempo definida para determinar o atraso.	03	0,8% por dia
03	Cumprir prazo previamente estabelecido com a FISCALIZAÇÃO para fornecimento de materiais ou execução de serviços; por unidade de tempo definida para determinar o atraso.	03	0,8 % por dia
04	Iniciar execução de serviço nos prazos estabelecidos pela FISCALIZAÇÃO, observados os limites mínimos estabelecidos por este Contrato; por serviço, por ocorrência.	02	0,4% por dia
05	Disponibilizar equipamentos, insumos e materiais necessários à realização dos serviços do escopo do contrato; por ocorrência.	02	0,4% por dia
06	Efetuar a entrega dos produtos nos prazos estabelecidos, observadas as condições estabelecidas por este Contrato, por ocorrência.	02	0,4% por dia
07	Ressarcir o órgão por eventuais danos causados por sua culpa, ou de seus prepostos.	02	0,4% por dia
08	Manter a documentação de habilitação atualizada; por item, por ocorrência.	01	0,2% por dia

*\* incidente sobre a parte inadimplida do contrato"*

22.12. As sanções aqui previstas poderão ser aplicadas concomitantemente, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 15 (quinze) dias úteis.

22.13. Após 30 (trinta) dias da falta de execução do objeto, será considerada inexecução total do contrato, o que ensejará a rescisão contratual.

22.14. As sanções de natureza pecuniária serão diretamente descontadas de créditos que eventualmente detenha a **CONTRATADA** ou efetuada a sua cobrança na forma prevista em lei.

22.15. As sanções previstas não poderão ser relevadas, salvo ficar comprovada a ocorrência de situações que se enquadrem no conceito jurídico de força maior ou casos fortuitos, devidos e formalmente justificados e comprovados, e sempre a critério da autoridade competente, conforme prejuízo auferido.

22.16. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

22.17. Também ficam sujeitas às penalidades de suspensão de licitar e impedimento de contratar com o órgão licitante e de declaração de inidoneidade, previstas no subitem anterior, as empresas ou profissionais que, em razão do contrato decorrente desta licitação:

- a) Tenham sofrido condenações definitivas por praticarem, por meio dolosos, fraude fiscal no recolhimento de tributos;
- b) Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;
- c) Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

22.18. Atender no que pede a Instrução Normativa nº 1/2021/SUPEL/ASJUR, que regula o rito processual administrativo.

**23. DA PROPOSTA DE PREÇOS**

23.1. **A Proposta de Preços** a ser elaborada deverá estar em estrita conformidade com a relação do objeto constante no Termo de Referência e será solicitado à licitante provisoriamente colocada em primeiro lugar a apresentação de folder/prospecto/catálogo do produto ofertado para comprovação das especificações técnicas do objeto, conforme expresso no art. 41, inciso II da [Lei nº 14.133, de 01 de abril de 2021](#). A ausência do fornecimento do folder/prospecto/catálogo do produto ofertado, por si só, não será motivo para desclassificar a proposta da empresa.

23.2. 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;

23.3. 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;

23.4. 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.

23.5. Prazo de validade, não inferior a de 90 (noventa) dias, contados a partir da data da entrega das propostas, conforme disposto no Art. 90, § 3º [Lei nº 14.133, de 01 de abril de 2021](#).

23.6. 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;

23.7. No que tange à apresentação de amostras, informamos que não será necessária à apresentação de amostras devido a natureza do serviço.

**24. DA PARTICIPAÇÃO DE EMPRESAS REUNIDAS SOB A FORMA DE CONSÓRCIO**

24.1. Não poderão participar da presente licitação as empresas interessadas que se apresente em consórcio, qualquer que seja sua forma de constituição.

24.2. A vedação à participação de empresas constituídas sob a forma de consórcio se justifica na medida em que nas contratações de serviços e nas aquisições de pequeno vulto não se torna interessante a participação de grandes empresas, sendo comum a competição entre interessadas de pequeno e médio porte, às quais, em sua maioria, apresentam o mínimo exigido no tocante à qualificação técnica e econômico-financeira, condições suficientes para a execução de contratos dessa natureza.

24.3. Tendo em vista que é prerrogativa do Poder Público, na condição de contratante, permitir a participação, ou não, de empresas constituídas sob a forma de consórcio, com as devidas justificativas, conforme se depreende da literalidade do texto do art. 15, da [Lei nº 14.133, de 01 de abril de 2021](#), e, ainda, do entendimento contido no Acórdão TCU nº 1316/2010, que atribui à Administração a prerrogativa de autorizar a admissão de consórcios em licitações por ela promovidas, pelos motivos já expostos, conclui-se que a vedação da participação de empresas constituídas em consórcio, neste certame, é o que melhor atende o interesse público, por prestigiar os princípios da competitividade, economicidade e moralidade.

**25. DAS EXIGÊNCIAS DE CRITÉRIOS DE SUSTENTABILIDADE**

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

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

25.3. 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;

25.4. A **CONTRATADA** deverá cumprir as orientações dispostas aos critérios de Sustentabilidade Ambiental, no que couber, conforme art. 144 da [Lei nº 14.133, de 01 de abril de 2021](#).

25.5. A **CONTRATADA** deverá preencher modelo de declaração de sustentabilidade ambiental presente no **ANEXO III** deste Termo de Referência.

**26. DO ACRESCIMO E SUPRESSÃO**

26.1. Os acréscimos ou supressões não poderão exceder a 25% do valor inicial atualizado do contrato, conforme estabelece o art. 125 da [Lei nº 14.133, de 01 de abril de 2021](#).

26.3. O contratado fica obrigado a aceitar, nas mesmas condições contratuais, as supressões resultantes de acordo celebrado entre os contratantes.

**27. JUSTIFICATIVA DA NÃO APLICABILIDADE DA RESERVA DE COTA 25% ME E EPP - [LEI COMPLEMENTAR Nº 123, DE 14 DE DEZEMBRO DE 2006](#)**

27.1. Não se aplica ao presente caso, haja vista a especificidade dos equipamentos que são oferecidos e fabricados por empresas de grande porte e até mesmo multinacionais. Nesse sentido, o enquadramento da presente reserva poderá ocasionar prejuízos a licitação, bem como a setorial solicitante do equipamento.

27.2. O art. 49 da Lei Complementar nº 123/06 proíbe a aplicação do disposto nos seus artigos 47 e 48 quando o tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte não for vantajoso para a Administração ou representar prejuízo ao conjunto ou complexo do objeto a ser contratado.

27.3. A Súmula 247, do Tribunal de Contas da União, afasta a obrigatoriedade do parcelamento, fator que se traduz na ampliação do número de competidores –, em hipóteses que representem prejuízo para o conjunto ou complexo do objeto, conforme citado abaixo:

É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo *objeto* seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou *perda* de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do *objeto*, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade.

27.4. A Lei Complementar nº 123/06, tem por incompatível com o interesse público, a exclusividade de participação de entidades de menor porte, em licitação cujo valor estimado não supere R\$ 80.000,00 (oitenta mil reais), sempre que a Administração verifique o risco de prejuízo para o conjunto ou complexo do objeto a ser contratado.

27.5. Ademais, a referida lei afasta a exclusividade para o efeito de subcontratação e de reserva de cota de até vinte e cinco por cento do objeto, quando o tratamento privilegiado mostrar-se desvantajoso para a Administração.

27.6. De acordo com o [art. 10, inciso II, do Decreto federal nº 8.538/2015](#), considera-se desvantajosa a contratação quando resultar em preço superior ao valor estabelecido como referência.

27.7. Desta feita neste certame não serão concedidos os benefícios de até 25% (vinte e cinco por cento) para o objeto desta contratação, para pequenas empresas, conforme [Lei Complementar nº 123/2006](#), quanto a previsão legal de cota para empresas ME/EPP, constantes deste Termo de Referência (TR).

27.8. A não aplicação visa garantir maior competitividade entre os grandes fornecedores.

**28. DO INSTRUMENTO CONTRATUAL**

**Fundamentação Legal:** [Lei nº 14.133, de 01 de abril de 2021](#) e [Decreto Estadual nº 28.874/2024](#).

28.1. Após a homologação da licitação, o adjudicatário terá o prazo de 10 dias úteis, contados a partir de sua convocação, para assinar o Termo de Contrato, conforme art. 105 a 114, da [Lei nº 14.133, de 01 de abril de 2021](#).

28.2. Prazo de vigência do contrato será de até 12 (doze) meses contados da data de assinatura do contrato, podendo ser prorrogado na forma da [Lei nº 14.133, de 01 de abril de 2021](#).

28.3. Em caso de descumprimento de quaisquer das condições estabelecidas no presente instrumento, à rescisão do contrato, seja administrativa ou amigável, será efetuada de acordo com as disposições da [Lei nº 14.133, de 01 de abril de 2021](#) e demais ordenamentos jurídicos, pertinentes ao caso.

28.4. A empresa **CONTRATADA**, deverá apresentar como **condição para assinatura do contrato** a declaração, sob as pena da lei e em cumprimento ao artigo [12º da Constituição do Estado de Rondônia](#), que não possui nenhum vínculo com a administração pública:

Art. 112. Nenhum servidor poderá ser diretor ou integrar conselho de empresa fornecedora do Estado, ou que realize qualquer modalidade de contrato com o Estado, sob pena de demissão do serviço público, salvo quando o contrato obedecer a cláusulas uniformes.

29. DA RESCISÃO CONTRATUAL

Fundamentação Legal: [Lei nº 14.133, de 01 de abril de 2021](#) e [Decreto Estadual nº 28.874/2024](#).

29.1. A rescisão contratual consensual será efetuada na seara administrativa, em conformidade com as disposições do Art. 137 e seguintes da [Lei nº 14.133, de 01 de abril de 2021](#) e legislação pertinente.

29.2. A rescisão do instrumento contratual, poderá ocorrer nos casos descritos no art. 137 da [Lei nº 14.133, de 01 de abril de 2021](#), conforme citado abaixo:

Art. 137. Constituirão motivos para extinção do contrato, a qual deverá ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa, as seguintes situações:

I - não cumprimento ou cumprimento irregular de normas editais ou de cláusulas contratuais, de especificações, de projetos ou de prazos;

II - desatendimento das determinações regulares emitidas pela autoridade designada para acompanhar e fiscalizar sua execução ou por autoridade superior;

III - alteração social ou modificação da finalidade ou da estrutura da empresa que restrinja sua capacidade de concluir o contrato;

IV - decretação de falência ou de insolvência civil, dissolução da sociedade ou falecimento do contratado;

V - caso fortuito ou força maior, regularmente comprovados, impeditivos da execução do contrato;

VI - atraso na obtenção da licença ambiental, ou impossibilidade de obtê-la, ou alteração substancial do anteprojeto que dela resultar, ainda que obtida no prazo previsto;

VII - atraso na liberação das áreas sujeitas a desapropriação, a desocupação ou a servidão administrativa, ou impossibilidade de liberação dessas áreas;

VIII - razões de interesse público, justificadas pela autoridade máxima do órgão ou da entidade contratante;

IX - não cumprimento das obrigações relativas à reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz.

29.3. A Administração, a qualquer tempo, poderá promover a extinção antecipada do Termo Contratual, nas formas descritas abaixo:

- a) Pela Administração Pública, determinada por ato unilateral e escrito;
- b) Consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas;
- c) Judicial, determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

29.4. O instrumento contratual também poderá ser rescindido pela Contratada, conforme dispõe o art. 137, § 2º da [Lei nº 14.133, de 01 de abril de 2021](#):

§ 2º O contratado terá direito à extinção do contrato nas seguintes hipóteses:

I - supressão, por parte da Administração, de obras, serviços ou compras que acarrete modificação do valor inicial do contrato além do limite permitido no [art. 125 desta Lei](#);

II - suspensão de execução do contrato, por ordem escrita da Administração, por prazo superior a 3 (três) meses;

III - repetidas suspensões que totalizem 90 (noventa) dias úteis, independentemente do pagamento obrigatório de indenização pelas sucessivas e contratualmente imprevistas desmobilizações e mobilizações e outras previstas;

IV - atraso superior a 2 (dois) meses, contado da emissão da nota fiscal, dos pagamentos ou de parcelas de pagamentos devidos pela Administração por despesas de obras, serviços ou fornecimentos;

V - não liberação pela Administração, nos prazos contratuais, de área, local ou objeto, para execução de obra, serviço ou fornecimento, e de fontes de materiais naturais especificadas no projeto, inclusive devido a atraso ou descumprimento das obrigações atribuídas pelo contrato à Administração relacionadas a desapropriação, a desocupação de áreas públicas ou a licenciamento ambiental.

§ 3º As hipóteses de extinção a que se referem os incisos II, III e IV do § 2º deste artigo observarão as seguintes disposições:

30. DO REAJUSTE E REEQUILÍBRIO CONTRATUAL

Fundamentação Legal: [Lei nº 14.133, de 01 de abril de 2021](#) e [Decreto Estadual nº 28.874/2024](#).

30.1. O reajuste de preços poderá ser utilizado na presente contratação, desde que seja observado o interregno mínimo de 01 (um) sendo a data-base vinculada à data do orçamento estimado para contratação.

30.2. O contrato será reajustado ou corrigido monetariamente tendo como base os requisitos trazidos no art. 25 da [Lei nº 14.133, de 01 de abril de 2021](#), §§ 7º e 8º, conforme citado abaixo:

§ 7º Independentemente do prazo de duração do contrato, será obrigatória a previsão no edital de índice de reajustamento de preço, com data-base vinculada à data do orçamento estimado e com a possibilidade de ser estabelecido mais de um índice específico ou setorial, em conformidade com a realidade de mercado dos respectivos insumos.

§ 8º Nas licitações de serviços contínuos, observado o interregno mínimo de 1 (um) ano, o critério de reajustamento será por:

I - reajustamento em sentido estrito, quando não houver regime de dedicação exclusiva de mão de obra ou predominância de mão de obra, mediante previsão de índices específicos ou setoriais;

II - repactuação, quando houver regime de dedicação exclusiva de mão de obra ou predominância de mão de obra, mediante demonstração analítica da variação dos custos.

Conforme arts. 152 e 155 do Decreto Estadual nº 28.874/2024, o pedido de reajuste , repactuação e revisão deverá ser instruído com os seguintes documentos:

Art. 152.Os pedidos de reajustamento em sentido estrito, repactuação e revisão, além da documentação específica relativa ao requerimento elencada nos artigos seguintes, deverão ser instruídos com:

I - requerimento expresso do contratado, contados da publicação do índice ajustado contratualmente, no caso de reajuste em sentido estrito, ou da entrada em vigor do acordo, convenção ou dissídio coletivo, no caso de repactuação;

II - análise técnica acerca da correção do requerimento do contratado, inclusive quanto aos cálculos, a ser realizada pela Pasta responsável pelo contrato;

III - documentação comprobatória da disponibilidade de recursos orçamentários previstos para fazer frente à despesa a ser assumida, como pedido de reserva ou documento equivalente, além da declaração da compatibilidade da despesa com a legislação orçamentária;

IV - autorização expressa por parte da autoridade máxima da Pasta.

Art. 155.O pedido de reajuste do contrato deverá ser devidamente fundamentado e instruído, além daqueles constante no art. 152, com os seguintes documentos:

I - planilha de custos demonstrando a equação inicial do contrato, quando esta já não constar do processo licitatório; e

II - planilha de custos demonstrando a equação atual do contrato, a qual deverá demonstrar a variação do preço, levando em consideração o índice de reajuste pré-fixado no instrumento convocatório e no contrato.

30.3. Considerando que o reajuste de preços pode ser efetuado mediante a aplicação de índice – reajuste indexação – ou por meio de demonstração analítica de variação dos custos índices aplicar-se-á aos cálculos o índice **IGP-M (Índice Geral dos Preços – Mercado)** ou **IPC-A (Índice Nacional de Preços ao Consumidor – Amplo)**, sendo o critério de aplicação, aquele que de forma mais vantajosa se adequar às especificidades do objeto.

30.4. Os reajustes serão precedidos obrigatoriamente de solicitação da CONTRATADA, acompanhada de memória do cálculo, conforme for a variação de custos objeto do reajuste;

30.5. É vedada a inclusão, por ocasião do reajuste de itens não previstos na proposta inicial, exceto quando se tornarem obrigatórios por força de instrumento legal.

30.6. O pedido de reajuste e reequilíbrio contratual será analisado por esta Secretaria em até 60 (sessenta) dias.

30.7. A análise quanto ao reajuste ou repactuação ficará suspensa em caso de pendência de atos ou apresentação de documentação por parte da CONTRATADA.

31. GARANTIA CONTRATUAL



Informamos pelo presente instrumento, que em detrimento do objeto, não será exigida apresentação de Garantia Contratual por parte desta Secretaria.

Fundamentação Legal: [Lei nº 14.133, de 01 de abril de 2021](#) e [Decreto Estadual nº 28.874/2024](#).

31.1. O adjudicatário, no prazo de 5 (cinco dias) após a assinatura do Termo de Contrato, prestará garantia no valor correspondente a 2% (dois por cento) do valor do Contrato, que será liberada de acordo com as condições previstas neste Termo de Referência, conforme disposto no art. 96 [Lei nº 14.133, de 01 de abril de 2021](#), desde que cumpridas as obrigações contratuais, optando por uma das seguintes modalidades:

- a) caução em dinheiro ou títulos da dívida pública;
- b) seguro – garantia;
- c) fiança bancária; ou
- d) Título de capitalização custeado por pagamento único.

31.2. A garantia contratual não poderá ultrapassar a 5% do valor inicial do contrato, envolvendo alta complexidade técnica e riscos financeiros consideráveis, demonstrados nos autos do processo, hipótese em que o limite pode chegar até 10%.

31.3. A garantia prestada pela Contratada será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração, e, quando em dinheiro, atualizada monetariamente, deduzidos eventuais valores devido à Contratante.

32. **DA SELEÇÃO, TIPO, MODALIDADE DE LICITAÇÃO E CRITÉRIO DE JULGAMENTO**

32.1. A **seleção**, contratação e as fases da licitação obedecerão aos ditames da [Lei nº 14.133, de 01 de abril de 2021](#).

32.2. Concernente à seleção de empresa para realização da contratação/fornecimento, objeto do presente instrumento, será escolhida levando-se em conta a modalidade de licitação, **disputa de modo aberto**, por meio de Pregão Eletrônico, que será oportunamente definida pela Superintendência de Licitações do Estado de Rondônia - SUPEL.

32.3. O **critério de julgamento** adotado será o de **MENOR PREÇO POR LOTE**, observadas as exigências contidas neste Termo de Referência e seus anexos quanto às especificações do objeto.

33. **DAS DISPOSIÇÕES FINAIS**

33.1. As omissões, dúvidas e casos não previstos neste instrumento, serão resolvidos e decididos aplicando-se as regras da [Lei nº 14.133, de 01 de abril de 2021](#) e suas alterações, bem como demais ordenamentos jurídicos correlatos, levando-se sempre em consideração os princípios que regem a Administração Pública.

34. **DO FORO**

34.1. 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”, [Constituição Federal](#).

34.2. A Administração utilizar-se-á da aplicação de juízo arbitral para dirimir conflitos relativos a direitos patrimoniais disponíveis, conforme disposto na Lei Estadual 407 e Lei n. 9.307, de 1996, alterada pela Lei Federal n. 13.129, de 2015.

35. **ANEXOS**

ANEXO I- Estudo Técnico Preliminar 23 ([0059485479](#));

Anexo II- Minuta de Contrato [0059625571](#);

ANEXO III

MODELO DE DECLARAÇÃO DE SUSTENTABILIDADE AMBIENTAL

PREGÃO ELETRÔNICO Nº \_\_\_\_/2025

PROPONENTE: \_\_\_\_\_ ENDEREÇO: \_\_\_\_\_

\_\_\_\_\_ CNPJ: \_\_\_\_\_ FONE/FAX: \_\_\_\_\_

\_\_\_\_\_

Declaro, sob as penas da [Lei nº 6.938, de 31 de agosto de 1981](#), na qualidade de proponente do procedimento licitatório, sob a modalidade Pregão Eletrônico nº \_\_\_\_/2025, instaurado pelo Processo de nº [0028.020065/2024-49](#), que atendemos aos critérios de qualidade ambiental e sustentabilidade socioambiental, respeitando as normas de proteção do meio ambiente.

Estou ciente da obrigatoriedade da apresentação das declarações e certidões pertinentes dos órgãos competentes quando solicitadas como requisito para habilitação e da obrigatoriedade do cumprimento integral ao que estabelece o art. 6º e seus incisos, da [Instrução Normativa nº 01, de 19 de janeiro de 2010, do Ministério do Planejamento, Orçamento e Gestão – MPOG](#) e [Decreto nº 7.746, de 05 de junho de 2012](#), que estabelece critérios, práticas e diretrizes para a promoção do desenvolvimento nacional sustentável.

Estou ciente da obrigatoriedade da apresentação do registro no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais caso minha empresa exerça uma das atividades constantes no Anexo II da [Instrução Normativa nº 31, de 03 de dezembro de 2009, do IBAMA](#).

Por ser a expressão da verdade, firmamos a presente.

\_\_\_\_\_ de \_\_\_\_\_ de 2025.

Nome:

RG/CPF:

Cargo:

ELABORAÇÃO:  
ANDREZA DOS SANTOS BARBOSA  
Assessor III

REVISÃO:

[https://sei.sistemas.ro.gov.br/sei/controlador.php?acao=documento\\_visualizar&acao\\_origem=arvore\\_visualizar&id\\_documento=61262456&infra\\_sistema=100000100&infra\\_unidade\\_atual=110000209&infra\\_hash=...](https://sei.sistemas.ro.gov.br/sei/controlador.php?acao=documento_visualizar&acao_origem=arvore_visualizar&id_documento=61262456&infra_sistema=100000100&infra_unidade_atual=110000209&infra_hash=...)

26/27

SARA MIDIÃ GOMES PASCOAL  
Gerente Administrativa GAD/COPAF/SEDAM

ESPECIFICAÇÃO E REVISÃO TÉCNICA:  
RENATA DOS SANTOS LUZ COUTINHO  
Coordenadora de Tecnologia da Informação

De acordo e autorizado nos termos da lei:  
MARCO ANTÔNIO RIBEIRO DE MENEZES LAGOS  
Secretário de Estado do Desenvolvimento Ambiental



Documento assinado eletronicamente por **Andreza dos Santos Barbosa, Assessor(a)**, em 07/05/2025, às 12:17, 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 **Sara Midia Gomes Pascoal, Gerente**, em 07/05/2025, às 12:17, 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 **RENATA DOS SANTOS LUZ, Coordenador(a)**, em 08/05/2025, às 12:47, 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 **MARCO ANTÔNIO RIBEIRO DE MENEZES LAGOS, Secretário(a)**, em 09/05/2025, às 13:37, 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 **0059255807** e o código CRC **7FDFFD46**.



GOVERNO DO ESTADO DE RONDÔNIA  
Secretaria de Estado do Desenvolvimento Ambiental - SEDAM

ESTUDO TÉCNICO PRELIMINAR

Objeto: Registro de preço para futura e eventual contratação de empresa para fornecimento de solução de proteção para estações de trabalho e servidores contra ataques cibernéticos.

1. INTRODUÇÃO:
<p>O Estudo Técnico Preliminar, em obediência ao Inciso I, Art. 18 da Lei Federal nº 14.133 de 01/04/2021, tem por objetivo planejar, descrever e analisar a necessidade, interesse público, evidenciar o problema a ser resolvido e sua melhor solução demonstrando a viabilidade técnica e econômica para contratação, fornecendo subsídios para elaboração do Projeto Básico e/ou Termo de Referência caso se conclua pela sua viabilidade.</p> <p>Este documento integra a fase de planejamento das contratações públicas, constituindo importante mecanismo de controle da eficiência e economicidade na gestão dos recursos públicos, a partir da identificação das necessidades do ente, análise da viabilidade e razoabilidade da contratação, apontamento das possíveis soluções, análise de impacto ambiental, descrição fiel dos produtos, informações orçamentarias, dentre outros.</p> <p>Assim o estudo tem como objetivo analisar a viabilidade para a Contratação de empresa especializada em <b>fornecimento de solução de proteção para estações de trabalho e servidores contra ataques cibernéticos</b>, para atender as demandas da Secretaria de Estado do Desenvolvimento Ambiental.</p>

2. DESCRIÇÃO DO OBJETO:			
ITEM	DESCRIÇÃO	ESPECIFICAÇÕES TÉCNICAS	CÓDIGO CATMAT OU CATSER
01	Solução de proteção avançada contra ataques cibernéticos para estações de trabalho (Extended detection and response - XDR)	<p><b>1. Solução de proteção avançada contra ataques cibernéticos para estações de trabalho (Extended detection and response – XDR) (ITEM 01)</b></p> <p>1.1. Características gerais</p> <p>1.1.1. A solução deverá ser entregue na modalidade como um serviço (em nuvem);</p> <p>1.1.2. Possuir console Web para gerenciamento e administração da ferramenta;</p> <p>1.1.3. A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações e Controle de dispositivos em um único agente.</p> <p><b>1.2. Módulo de Proteção Anti-Malware</b></p> <p>1.2.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:</p> <p>1.2.1.1. Windows 8.1 (x86/x64);</p> <p>1.2.1.2. Windows 10 (x86/x64);</p> <p>1.2.1.3. Windows 11 (x64).</p> <p>1.2.2. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;</p> <p>1.2.3. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;</p> <p>1.2.4. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em: Processos em execução em memória principal (RAM);</p> <p>1.2.5. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);</p> <p>1.2.6. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, MIME/uu, CAB;</p> <p>1.2.7. Arquivos recebidos por meio de programas de comunicação instantânea (MSN messenger, yahoo messenger, google talk, icq, dentre outros).</p> <p>1.2.8. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript, VBScript/Activex;</p> <p>1.2.9. Deve possuir detecção heurística de vírus desconhecidos;</p> <p>1.2.10. Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada; Deve permitir diferentes configurações de detecção (varredura ou rastreamento):</p> <p>1.2.11. Em tempo real de arquivos acessados pelo usuário;</p> <p>1.2.12. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;</p> <p>1.2.13. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;</p> <p>1.2.14. Automáticos do sistema com as seguintes opções:</p> <p>1.2.15. Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;</p> <p>1.2.16. Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);</p> <p>1.2.17. Frequência: horária, diária, semanal e mensal;</p> <p>1.2.18. Exclussões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;</p> <p>1.2.19. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;</p> <p>1.2.20. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;</p> <p>1.2.21. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL’s maliciosas, de modo a prover, rápida detecção de novas ameaças;</p> <p>1.2.22. Deve ser capaz de aferir a reputação das URL’s acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;</p> <p>1.2.23. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;</p> <p>1.2.24. Deve possuir capacidade de escaneamento de arquivos compactados e, em caso de identificação de um arquivo malicioso, apenas este deve ser removido, mantendo os demais intactos</p> <p>1.2.25. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;</p> <p>1.2.26. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;</p> <p>1.2.27. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;</p> <p>1.2.28. Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;</p> <p>1.2.29. Deverá ter funcionalidade de Machine Learning em runtime para evitar possíveis métodos de obfuscação que o módulo de Machine Learning em pré-execução não consiga detectar;</p> <p>1.2.30. Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;</p> <p>1.2.31. Deve bloquear processos comuns associados a ransomware;</p> <p>1.2.32. Em casos de ataques de ransomware, a solução deve ter a capacidade de interromper o processo de criptografia e restaurar os arquivos originais aos seus respectivos diretórios</p> <p>1.2.33. Deve possuir funcionalidade de detecção de malwares conhecidos e desconhecidos por comportamento; Deve permitir a integração com solução de análise de artefatos suspeitos (sandbox) do próprio fabricante.</p> <p><b>1.3. Funcionalidade de Atualização</b></p> <p>1.3.1. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo</p>	24333



administrador da solução;  
1.3.2. Deve permitir atualização incremental da lista de definições de vírus;  
1.3.3. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;  
1.3.4. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;  
1.3.5. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;  
1.3.6. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;  
1.3.7. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

1.4. Funcionalidade de Administração

1.4.1. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;  
1.4.2. Deve possibilitar instalação "silenciosa";  
1.4.3. Deve permitir o bloqueio por nome de arquivo;  
1.4.4. Deve permitir o travamento de pastas e diretórios;  
1.4.5. Deve permitir o travamento de compartilhamentos;  
1.4.6. Deve permitir o rastreamento e bloqueio de infecções;  
1.4.7. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;  
1.4.8. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;  
1.4.9. Deve permitir a desinstalação através da console de gerenciamento da solução;  
1.4.10. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;  
1.4.11. Deve permitir a deleção dos arquivos quarentenados;  
1.4.12. Deve permitir remoção automática de clientes inativos por determinado período;  
1.4.13. Deve permitir integração com serviço de autenticação como Active Directory para acesso a console de administração;  
1.4.14. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;  
1.4.15. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;  
1.4.16. Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;  
1.4.17. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;  
1.4.18. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;  
1.4.19. Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional;  
1.4.20. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;  
1.4.21. Deve prover criptografia para as comunicações entre o servidor e os agentes de proteção; Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;  
1.4.22. Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;  
1.4.23. Deve permitir a criação de usuários locais de administração da console de anti-malware;  
1.4.24. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;  
1.4.25. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;  
1.4.26. Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;  
1.4.27. Deve permitir a gerência de domínios separados para usuários previamente definidos;  
1.4.28. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;  
1.4.29. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

1.5. Funcionalidade de Controle de Dispositivos

1.5.1. As configurações da funcionalidade de controle de dispositivos devem ser aplicadas por usuário;  
1.5.2. Deve permitir políticas e ações diferentes para dispositivos conectados à rede interna e aqueles utilizados na rede externa (conectado à Internet, por exemplo);  
1.5.3. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;  
1.5.4. Deve possuir o controle de acesso a drives de mídias de armazenamento como CD-ROM, DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;  
1.5.5. Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;  
1.5.6. Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;  
1.5.7. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa;  
1.5.8. Para ação de restrição como o bloqueio, a solução deve permitir adicionais dispositivos USB autorizados, bem como apontar executáveis específicos como exceção ao bloqueio;  
1.5.9. Deve ter a capacidade de bloquear a função de Autorun nos dispositivos;  
1.5.10. Deve permitir controle de permissão ou bloqueio para dispositivos que não armazenam dados tendo, pelo menos, os seguintes tipos de dispositivos: adaptadores bluetooth, dispositivos de imagem, modems, interfaces wireless externas, cartões PCMCIA, dispositivos infravermelhos e portas COM/LPT.

1.6. Módulo de Proteção Anti-Malware para estações MacOS

1.6.1. O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:  
1.6.1.1. macOS 12 (Monterey);  
1.6.1.2. macOS 11 (Big Sur) macOS 10.15 (Catalina);  
1.6.1.3. macOS 10.14 (Mojave); macOS 10.13 (High Sierra);  
1.6.2. Suporte ao Apple Remote Desktop para instalação remota da solução;  
1.6.3. Gerenciamento integrado à console de gerência central da solução;  
1.6.4. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;  
1.6.5. Permitir a verificação das ameaças da maneira manual e agendada;  
1.6.6. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus; Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infeções a arquivos;  
1.6.7. Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;  
1.6.8. Deve possuir no mecanismo de autoproteção as seguintes proteções:  
1.6.8.1. Proteção e verificação dos arquivos de assinatura;  
1.6.8.2. Proteção dos processos do agente de segurança;  
1.6.8.3. Proteção das chaves de registro do agente de segurança;  
1.6.8.4. Proteção do diretório de instalação do agente de segurança.

1.7. Funcionalidade de HIPS – Host IPS e Host Firewall

1.8. Deve ser capaz de realizar a detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais:  
1.8.1.1. Windows 8.1 (x86/x64);

1.8.1.2. Windows 10 (x86/x64);  
1.8.1.3. Windows 11 (x64).  
1.9. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;  
1.10. As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;  
1.11. Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio);  
1.12. Deve permitir ativar e desativar o produto sem a necessidade de remoção;  
1.13. Deve permitir que o usuário altere as configurações de níveis de segurança e exceções;  
1.14. Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo;  
1.15. O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança; O modulo de HIPS deverá possuir regras pra proteger contra ameaças do tipo Ransomware;  
1.16. O modulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genericas protegendo contra ameaças conhecidas ou desconhecidas;  
1.17. O módulo de HIPS deverá permitir que o administrador monitore apenas ou realize o bloqueio das tentativas de exploração de vulnerabilidades;  
1.18. Deve suportar configuração de parâmetros de pacotes como quantidade máxima de conexões TCP e timeout para pacotes UDP;  
1.19. Deve ter a capacidade de proteção contra exploração de vulnerabilidades do sistema operacional e de aplicações terceiras instaladas na estação de trabalho;  
1.20. A lista de regras deve permitir que o administrador realize buscas e tenha rápida visibilidade do tipo da aplicação, em que modo a regra encontra-se (bloqueio ou monitoramento), CVE, CVSS score, quando aplicável.

1.21. **Módulo para Controle De Aplicações**

1.21.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:  
1.21.1.1. Windows 8.1 (x86/x64);  
1.21.1.2. Windows 10 (x64);  
1.21.1.3. Windows 11 (x64).  
1.21.2. As regras de controle de aplicação devem permitir as seguintes ações:  
1.21.2.1. Permissão de execução;  
1.21.2.2. Bloqueio de execução;  
1.21.2.3. Bloqueio de novas instalações.  
1.21.3. A regra de liberação para o controle de aplicação deverá permitir que o programa liberado efetue ou não a execução de outros processos,  
1.21.4. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;  
1.21.5. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:  
1.21.5.1. Assinatura SHA-1 e SHA-256 do executável;  
1.21.5.2. Atributos do certificado utilizado para assinatura digital do executável;  
1.21.5.3. Caminho lógico do executável;  
1.21.5.4. Base de assinaturas de cortiçados digitais válidos e seguros.  
1.21.6. As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;  
1.21.7. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;  
1.21.8. O módulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionados para bloqueio e monitoramento tendo, pelo menos, as categorias de KeyLoggers, anonimizadores de proxy, P2P, crackers de senhas;  
1.21.9. Deve permitir a busca por aplicações ou fabricante destas;  
1.21.10. Deve possuir ferramenta para extrair o hash de um ou um grupo de executáveis, permitindo a importação destes hashes através de arquivo CSV.

1.22. **Módulo de Detecção e Resposta**

1.22.1. A solução deve ser compatível com os sistemas operacionais Windows, Linux e MacOS;  
1.22.2. O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK®, identificando técnicas e táticas dos ataques;  
1.22.3. A solução deve possuir módulo de investigação e detecção integrados;  
1.22.4. Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;  
1.22.5. Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;  
1.22.6. Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;  
1.22.7. Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;  
1.22.8. Fornece a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;  
1.22.9. Capacidade de construir sequências de buscas poderosas para localizar os dados ou objetos em seu ambiente que você deseja examinar;  
1.22.10. Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo Kibana para identificar, categorizar e recuperar os resultados da pesquisa;  
1.22.11. Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;  
1.22.12. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;  
1.22.13. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;  
1.22.14. Deve permitir que as detecções sejam correlacionadas com módulos de servidores, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;  
1.22.15. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;  
1.22.16. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;  
1.22.17. O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos; Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;  
1.22.18. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;  
1.22.19. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;  
1.22.20. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;  
1.22.21. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;  
1.22.22. Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade;  
1.22.23. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;  
1.22.24. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;  
1.22.25. Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;  
1.22.26. Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;  
1.22.27. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;  
1.22.28. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho;  
1.22.29. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;  
1.22.30. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;  
1.22.31. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);  
1.22.32. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas;  
1.22.33. Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;  
1.22.34. Deve permitir que o analista possa alterar o status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma;  
1.22.35. Deve permitir adicionar arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores; Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores; Deve permitir terminar processos ativos executados nas estações de trabalhos e servidores; Permitir coletar e fazer o download de um arquivo para investigação local detalhada;

		<p>1.22.36. Isolar a estação de trabalho desconectando-a da rede e permitindo se comunicar exclusivamente com a</p> <p>1.22.37. console de gerenciamento do fabricante;</p> <p>1.22.38. Restaurar a conectividade da estação de trabalho com a rede;</p> <p>1.22.39. Iniciar uma sessão de shell remoto na estação de trabalho selecionada para execução de comandos remotos para investigação;</p> <p>1.22.40. Deve ser possível fazer o download do histórico da sessão após finalizar a sessão remota do shell na estação de trabalho para fins de auditoria.</p>	
02	Solução de proteção avançada contra ataques cibernéticos para servidores (Extended detection and response - XDR)	<p><b>2. SOLUÇÃO DE PROTEÇÃO AVANÇADA CONTRA ATAQUES CIBERNÉTICOS PARA SERVIDORES (EXTENDED DETECTION AND RESPONSE - XDR) (ITEM 2)</b></p> <p><b>2.1. SOLUÇÃO DE SEGURANÇA PARA CARGAS DE TRABALHO HÍBRIDAS COM DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO</b></p> <p><b>2.2. Características Gerais Da Solução</b></p> <p>2.2.1. A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais;</p> <p>2.2.2. Windows Server 2000;</p> <p>2.2.3. Windows Server 2003 SP1 e 2003 R2 SP2; Windows Server 2008 e 2008 R2;</p> <p>2.2.4. Windows Server 2012 e 2012 R2;</p> <p>2.2.5. Windows Server 2016;</p> <p>2.2.6. Windows Server 2019;</p> <p>2.2.7. Windows Server 2022;</p> <p>2.2.8. Red Hat Enterprise 5, 6, 7 e 8;</p> <p>2.2.9. CentOS 5, 6, 7 e 8;</p> <p>2.2.10. AIX 6.1, 7.1 e 7.2;</p> <p>2.2.11. Oracle Linux 5, 6, 7 e 8;</p> <p>2.2.12. SUSE Linux Enterprise Server 10, 11, 12 e 15;</p> <p>2.2.13. Ubuntu 10, 12, 14, 16, 18 e 20;</p> <p>2.2.14. Debian 6, 7, 8, 9 e 10;</p> <p>2.2.15. Rocky Linux 8;</p> <p>2.2.16. AlmaLinux 8;</p> <p>2.2.17. Cloud Linux 5, 6, 7 e 8; Solaris 10 1/13 Sparc; Solaris 10 1/13 (x86/x64); Solaris 11.2/ 11.3 Sparc; Solaris 11.2/ 11.3 (x86/x64);</p> <p>2.2.18. Solaris 11.4 (x86, x64 ou SPARC) Amazon Linux e Amazon Linux 2 (x64).</p> <p>2.2.19. A solução deverá ser totalmente compatível e homologada com o ambiente Vmware;</p> <p>2.2.20. A console de gerenciamento deverá ser em nuvem, permitindo o gerenciamento das políticas de segurança através da Internet;</p> <p>2.2.21. A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Internet Explorer, Google Chrome e Firefox. Deve ainda suportar certificado digital para gerenciamento;</p> <p>2.2.22. A solução deverá permitir a integração com pelo menos as seguintes plataformas de nuvem: Vmware vCloud, MS Azure e AWS;</p> <p>2.2.23. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;</p> <p>2.2.24. A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;</p> <p>2.2.25. A console de administração deverá permitir o envio de notificações via SMTP;</p> <p>2.2.26. Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;</p> <p>2.2.27. A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;</p> <p>2.2.28. A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;</p> <p>2.2.29. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;</p> <p>2.2.30. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob-demanda, ou agendado com o envio automático do relatório via e-mail;</p> <p>2.2.31. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;</p> <p>2.2.32. A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;</p> <p>2.2.33. A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS aplicadas e Firewall;</p> <p>2.2.34. Em caso de solução e nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade; A solução de segurança ter a capacidade de identificar ataques entre containeres;</p> <p>2.2.35. Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";</p> <p>2.2.36. Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar novas políticas de segurança;</p> <p>2.2.37. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;</p> <p>2.2.38. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;</p> <p>2.2.39. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;</p> <p>2.2.40. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;</p> <p>2.2.41. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;</p> <p>2.2.42. Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;</p> <p>2.2.43. Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;</p> <p>2.2.44. Para servidores Linux, a solução deverá possibilitar a atualização automática da versão quando o agente reiniciar;</p> <p>2.2.45. Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;</p> <p>2.2.46. Deve permitir a remoção automática de agentes inativos, definindo o período para, pelo menos 1 semana, 1 mês e 12 meses;</p> <p>2.2.47. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;</p> <p>2.2.48. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;</p> <p>2.2.49. A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação; A solução deverá mostrar quais máquinas estão usando determinada política;</p> <p>2.2.50. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;</p> <p>2.2.51. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;</p> <p>2.2.52. A solução deverá permitir a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;</p> <p>2.2.53. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;</p> <p>2.2.54. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;</p> <p>2.2.55. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;</p> <p>2.2.56. A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;</p> <p>2.2.57. A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;</p> <p>2.2.58. A solução deverá ter a capacidade de se integrar com o Amazon SNS e os principais softwares de SIEMs contemplando, no mínimo: Splunk, IBMQradar e HPArCSight de modo a permitir enviar os seus logs para essas soluções;</p> <p>2.2.59. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;</p> <p>2.2.60. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;</p> <p>2.2.61. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;</p>	24333

2.2.62. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;

2.2.63. Após a atualização deve ser informado o que foi modificado ou adicionado;

2.2.64. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não as distribuir aos clientes;

2.2.65. A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras;

2.2.66. A solução deverá ter capacidade de gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;

2.2.67. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;

2.2.68. No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes;

2.2.69. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;

2.2.70. Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;

2.2.71. Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;

2.2.72. O fabricante deverá participar do programa “Microsoft Application Protection Program” para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;

2.2.73. A console de gerenciamento deve se integrar com o Vmware vCloud, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;

2.2.74. O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos; A solução deve possuir API documentada para integração na esteira de automação;

2.2.75. A documentação da API deve conter exemplos prontos para implementação de determinadas funcionalidades, como cookbooks;

2.2.76. Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;

2.2.77. A solução deve permitir desabilitar os módulos individualmente;

2.2.78. Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador.

2.3. Antimalware

2.3.1. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

2.3.2. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;

2.3.3. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

2.3.4. Em plataforma Windows, a solução deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações;

2.3.5. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo;

2.3.6. Em servidores Windows, deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentenando arquivos identificados;

2.3.7. A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;

2.3.8. A solução deverá oferecer escanear processos em memória em busca de Malware;

2.3.9. O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;

2.3.10. O scan de arquivos comprimidos do tipo OLE deverá ser de no mínimo 20 camadas de compressão;

2.3.11. Para servidores Windows, a solução deverá permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline na console de gerenciamento;

2.3.12. A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;

2.3.13. Em servidores Windows, a solução deverá integrar-se com interface AMSI (Antimalware Scan Interface);

2.3.14. A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado; Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware; Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;

2.3.15. Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no servidor;

2.3.16. A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs; Em servidores Windows, deve possuir capacidade de detectar ameaças por comportamento;

2.3.17. Deverá ter a possibilidade de escanear drivers de rede mapeados nos servidores.

2.4. Proteção Contra URLs Maliciosas

2.4.1. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;

2.4.2. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;

2.4.3. A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas tendo, pelo menos, os níveis Alto, médio e baixo;

2.4.4. Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;

2.4.5. Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;

2.4.6. Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;

2.4.7. A solução deve permitir que o administrador reclassifique uma URL através do site do fabricante para evitar falsos positivos;

2.4.8. A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.

2.5. Firewall

2.5.1. Operar como firewall de host, através da instalação de agente nos servidores protegidos;

2.5.2. Precisa ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;

2.5.3. Precisa ter a capacidade de controlar conexões TCP baseado nas Flags TCP; Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;

2.5.4. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYN SYN Scan, TCP Xmas Scan e Computer OS Fingerprint por até 30 minutos;

2.5.5. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;

2.5.6. Precisa ter a capacidade de definição de regras para contextos específicos;

2.5.7. Para facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de ips, lista de MACs, lista de portas;

2.5.8. Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);

2.5.9. Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana; O firewall deverá ser stateful bidirecional;

2.5.10. O firewall deverá permitir liberar ou apenas logar eventos;

2.5.11. O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;

2.5.12. As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny;

2.5.13. A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;

2.5.14. As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;

2.5.15. Deverá realizar pseudo stateful em tráfego UDP; Deverá logar a atividade stateful;

2.5.16. Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador;

2.5.17. Deverá permitir limitar o número de meias conexões vindas de um computador; Deverá prevenir ack storm;

2.5.18. Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;

2.5.19. Deverá identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um período de tempo configurado pelo administrador;

2.5.20. Deverá permitir criar lista de exceções para identificar os Ips autorizados a realizar varreduras de portas ou da

rede;  
2.5.21. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

2.6. **Proteção De Vulnerabilidades de SO e Aplicações**

- 2.6.1. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;
- 2.6.2. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;
- 2.6.3. A solução deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;
- 2.6.4. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;
- 2.6.5. Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;
- 2.6.6. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;
- 2.6.7. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;
- 2.6.8. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;
- 2.6.9. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para
- 2.6.10. fins de investigação do incidente;
- 2.6.11. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;
- 2.6.12. Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;
- 2.6.13. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);
- 2.6.14. Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana; Deverá ser capaz de inspecionar tráfego criptografado de entrada;
- 2.6.15. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL injection, Crosssite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;
- 2.6.16. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;
- 2.6.17. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;
- 2.6.18. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;
- 2.6.19. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;
- 2.6.20. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;
- 2.6.21. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;
- 2.6.22. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;
- 2.6.23. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs; As regras de IPS poderão ter sua capacidade de LOG desabilitado;
- 2.6.24. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta; As regras devem ser atualizadas automaticamente pelo fabricante;
- 2.6.25. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

2.7. **Monitoramento De Integridade**

- 2.7.1. A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;
- 2.7.2. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;
- 2.7.3. Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux; Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional; Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;
- 2.7.4. Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;
- 2.7.5. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;
- 2.7.6. O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;
- 2.7.7. Deverá alertar toda vez que uma modificação ocorrer em tempo real para ambiente Windows e pseudo real-time para ambiente Linux;
- 2.7.8. Deverá logar e colocar em relatório todas as modificações que ocorram;
- 2.7.9. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;
- 2.7.10. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;
- 2.7.11. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;
- 2.7.12. Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente.

2.8. **Inspeção De Logs**

- 2.8.1. A solução deverá permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX;
- 2.8.2. Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;
- 2.8.3. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;
- 2.8.4. Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;
- 2.8.5. Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;
- 2.8.6. Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;
- 2.8.7. Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;
- 2.8.8. Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;
- 2.8.9. Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;
- 2.8.10. Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram; As regras poderão ser modificadas por severidade de ocorrência de eventos;
- 2.8.11. As regras devem se atualizar automaticamente pelo fabricante;
- 2.8.12. Permitir modificação pelo administrador em regras para adequação ao ambiente.

2.9. **Controle De Aplicações**

- 2.9.1. A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;
- 2.9.2. O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;
- 2.9.3. O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina; A console deverá exibir eventos de no mínimo 30 dias;
- 2.9.4. A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período que deve ser no máximo 10 horas;
- 2.9.5. A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente.



		<p><b>2.10. Detecção e Resposta</b></p> <p>2.10.1. A solução deve ser compatível com Linux e Windows Server 2008 R2 e superiores; A solução deve possuir módulo de investigação, detecção integrados;</p> <p>2.10.2. Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;</p> <p>2.10.3. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;</p> <p>2.10.4. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;</p> <p>2.10.5. O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos; Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;</p> <p>2.10.6. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;</p> <p>2.10.7. A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados na console, ainda que estas não sejam detectadas como maliciosas;</p> <p>2.10.8. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;</p> <p>2.10.9. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;</p> <p>2.10.10. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;</p> <p>2.10.11. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;</p> <p>2.10.12. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;</p> <p>2.10.13. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;</p> <p>2.10.14. Deverá informar com qual técnica e tática do MITRE ATT&amp;CK framework o ataque está relacionado, além de possuir link direto para o site da organização;</p> <p>2.10.15. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);</p> <p>Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.</p>	
03	Serviços de suporte pro ativo, corretivo e para resposta a incidentes	<p><b>3. SERVIÇO DE SUPORTE PRO ATIVO, CORRETIVO E PARA RESPOSTA A INCIDENTES (ITEM 3)</b></p> <p>3.1. O serviço de suporte proativo, corretivo e para resposta a incidentes compreende um conjunto abrangente de atividades destinadas a assegurar o pleno funcionamento e a continuidade operacional de sistemas, soluções ou serviços. Este serviço é estrategicamente desenhado para atender às demandas dinâmicas do ambiente tecnológico, oferecendo suporte preventivo, corretivo e uma resposta ágil a incidentes de segurança.</p> <p>3.2. Todo o Serviço de Suporte deverá ser prestado por profissional certificado pelo Fabricante da Solução, em nível compatível com a prestação do serviço. Deverá ser apresentado comprovação da certificação dos profissionais responsáveis no ato da assinatura do contrato.</p> <p>3.3. Deverá disponibilizar um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução ofertada;</p> <p>3.4. deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução.</p> <p><b>3.5. Suporte Proativo:</b></p> <p>3.5.1. O suporte proativo deverá antecipar potenciais problemas, identificando e resolvendo questões antes mesmo que impactem o desempenho e a segurança do ambiente;</p> <p>3.5.2. A contratada deverá notificar a contratante sobre atualizações de segurança, patches e correções assim que estiverem disponíveis, caso autorizado aplicar as atualizações de segurança e evolutiva dos produtos;</p> <p>3.5.3. Deverá realizar análises preditivas, buscando otimizar a performance e prevenir falhas nos produtos, além de detectar padrões que possam indicar uma possível violação de segurança, proporcionando um ambiente mais estável e seguro;</p> <p>3.5.4. Deverá realizar avaliações regulares de riscos para identificar possíveis vulnerabilidades e pontos fracos nos sistemas e, implementar medidas corretivas com base nos resultados das avaliações de riscos;</p> <p>3.5.5. Realizar auditorias regulares para garantir que as melhores práticas e os controles de segurança estejam operacionais e, utilizar resultados de auditorias para implementar melhorias contínuas;</p> <p>3.5.6. A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução do problema.</p> <p><b>3.6. Suporte Corretivo:</b></p> <p>3.6.1. Este componente concentra-se na solução de problemas ou incidentes. O suporte corretivo atua de forma ágil para restabelecer a funcionalidade normal do sistema, minimizando impactos negativos e mantendo a continuidade operacional;</p> <p>3.6.2. Serviço Especializado de Suportes corretivo para xx(xxxx) meses. Serviço de Suporte especializado para ajustes, correções e configurações da solução a ser fornecida. Neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução;</p> <p>3.6.3. A contratada deverá:</p> <ul style="list-style-type: none"><li>Implementar um sistema de abertura de chamados, para registrar, rastrear e priorizar incidentes e requisições de suporte;</li><li>Atribuir números de caso exclusivos para facilitar a comunicação e o acompanhamento;</li><li>Garantir disponibilidade 24/7 para responder a incidentes críticos.</li></ul> <p>3.6.4. Deverá apresentar relatório contendo as ações adotadas para a solução do problema.</p> <p><b>3.7. Resposta a Incidentes:</b></p> <p>3.7.1. O serviço de resposta a incidentes deverá lidar com eventos imprevistos, como violações de segurança, falhas críticas ou interrupções inesperadas. deverá ser realizada por profissionais especializados e certificados pelo fabricante;</p> <p>3.7.2. Deverá realizar investigações para determinar a natureza, origem e impacto de incidentes de segurança;</p> <p>3.7.3. Desenvolver planos de mitigação e estratégia de recuperação para minimizar o impacto de incidentes;</p> <p>3.7.4. Elaborar relatórios detalhados sobre os incidentes, incluindo ações tomadas e recomendações de melhorias.</p> <p><b>4. SERVIÇO DE IMPLANTAÇÃO</b></p> <p>4.1. Nesta etapa, compreende-se a instalação e configuração da solução contratada, contados a partir da emissão da Ordem de Serviço (OS);</p> <p>4.2. O serviço de implantação abrange integralmente as fases essenciais para a integração, instalação e configuração da solução contratada, alinhando-se precisamente com as especificações técnicas e requisitos predefinidos. Esta abordagem abarca desde o planejamento inicial até a conclusão efetiva, assegurando uma transição suave dos processos existentes para a nova solução;</p> <p>4.3. O Plano de Implantação assume a forma de um documento fundamental que consolida a estratégia para instalação, configuração e entrega da solução contratada. Sua importância reside em orientar e alinhar as atividades, garantindo eficiência e uma implementação adequada da solução conforme os requisitos estabelecidos;</p> <p>4.4. O documento deverá conter no mínimo os requisitos de ambiente tecnológicos necessários para a instalação das licenças, cronograma e detalhamento das atividades a serem realizadas, topologia do ambiente pós instalação da solução, matriz de responsabilidade, plano de comunicação;</p> <p>4.5. Durante esta etapa, a equipe da Contratada deverá estar presente nos horários de instalação definidos pelo Contratante. As atividades de instalação e configuração poderão ser realizadas, conforme necessário, em horário comercial, período noturno ou final de semana;</p> <p>4.6. O Contratante disponibilizará a infraestrutura de hardware e software necessária e já existente em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução durante esta etapa.</p> <p>5. Serviço de capacitação e repasse de conhecimento (Item 12)</p> <p>5.1. Repasse de conhecimento, na forma de treinamento para técnicos, de forma virtual, para 3 (três) turmas, com carga horária mínima de 40 (quarenta) horas, abrangendo todos os softwares integrantes da suíte de solução de segurança;</p> <p>5.2. O conteúdo programático abordará tanto aspectos teóricos quanto práticos, contemplando de maneira abrangente todos os módulos relevantes da solução de segurança;</p> <p>5.3. O treinamento pode ser segmentado de acordo com o produto a ser instalado no ambiente tecnológico, contemplando, no mínimo, os seguintes módulos:</p> <p>5.3.1. Instalação do módulo de gerenciamento central;</p> <p>5.3.2. Instalação do software de Endpoint Protection em estações de trabalho e servidores;</p> <p>5.3.3. Descrição e configuração de todas as funcionalidades contratadas da solução;</p> <p>5.3.4. Melhores práticas utilizadas no mercado para otimização dos softwares e suas funcionalidades.</p>	5398



		5.4. A carga horária mínima estabelecida será de 40 (quarenta) horas, divididas em expedientes de 4 horas por dia, no horário comercial. A contratada é responsável por fornecer apostilas em formato digital que contemplem o conteúdo referente ao produto, oferecendo suporte ao aprendizado prático e teórico dos participantes; 5.5. Este treinamento visa capacitar adequadamente os usuários finais, garantindo que compreendam e aproveitem plenamente as funcionalidades da solução de segurança. O enfoque prático e teórico, aliado às melhores práticas do mercado, promove uma formação abrangente e eficaz.	
04	Serviço de treinamento	<b>5. SERVIÇO DE TREINAMENTO (ITEM 4)</b> 5.1. Repasse de conhecimento, na forma de treinamento para técnicos, de forma virtual, para 3 (três) turmas, com carga horária mínima de 40 (quarenta) horas, abrangendo todos os softwares integrantes da suíte de solução de segurança; 5.2. O conteúdo programático abordará tanto aspectos teóricos quanto práticos, contemplando de maneira abrangente todos os módulos relevantes da solução de segurança; 5.3. O treinamento pode ser segmentado de acordo com o produto a ser instalado no ambiente tecnológico, contemplando, no mínimo, os seguintes módulos: 5.3.1. Instalação do módulo de gerenciamento central; 5.3.2. Instalação do software de Endpoint Protection em estações de trabalho e servidores; 5.3.3. Descrição e configuração de todas as funcionalidades contratadas da solução; 5.3.4. Melhores práticas utilizadas no mercado para otimização dos softwares e suas funcionalidades. 5.4. A carga horária mínima estabelecida será de 40 (quarenta) horas, divididas em expedientes de 4 horas por dia, no horário comercial. A contratada é responsável por fornecer apostilas em formato digital que contemplem o conteúdo referente ao produto, oferecendo suporte ao aprendizado prático e teórico dos participantes; 5.5. Este treinamento visa capacitar adequadamente os usuários finais, garantindo que compreendam e aproveitem plenamente as funcionalidades da solução de segurança. O enfoque prático e teórico, aliado às melhores práticas do mercado, promove uma formação abrangente e eficaz. <b>DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC</b> <b>6.1. Requisitos de Capacitação</b> 6.1.1. A empresa CONTRATADA deverá realizar o repasse de conhecimento aos funcionários da CONTRATANTE que atuarão, diretamente, com a solução de segurança adquirida, contemplando instalação, parametrização, monitoramento, melhores práticas e atuação de incidentes com carga horária mínima de 40 (quarenta) horas ministrado por profissional certificado pelo fabricante. 6.1.2. O treinamento será demandado à CONTRATADA pela CONTRATANTE após a efetiva implementação e estruturação da solução de segurança em seu parque tecnológico, quando acordarão cronograma para realização do treinamento. 6.1.3. O treinamento deverá ser realizado na modalidade presencial nas dependências da CONTRATANTE a participantes da equipe técnica a serem definidos pela CONTRATANTE. 6.1.4. Os horários do curso deverão seguir a conveniência do CONTRATANTE, podendo sua realização ocorrer apenas em um dos períodos do dia (manhã ou tarde). 6.1.5. Deverá ser fornecido material didático completo e com conteúdo oficial do fabricante em língua portuguesa. Caso seja utilizado material elaborado exclusivamente pelo fabricante e fique demonstrado que este não é oferecido em língua portuguesa, será aceito o fornecimento em língua inglesa. 6.1.6. O treinamento deve conter parte teórica e prática, incluindo tópicos sobre a instalação, uso, configuração, resolução de problemas da solução, análise de relatórios, respostas a incidentes e outros. 6.1.7. As datas do treinamento devem ser previamente combinadas com o CONTRATANTE. 6.1.8. Todos os custos relativos à realização do treinamento são de exclusiva responsabilidade da CONTRATADA.	3840

<b>3. JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO OU AQUISIÇÃO:</b>
<p>A segurança da rede da Secretaria de Estado do Desenvolvimento Ambiental - SEDAM, depende da utilização de recursos de segurança cibernética, que incluem várias camadas de proteção para monitorar o comportamento dos usuários, estações de trabalho e servidores de rede, com o objetivo de proteger o ambiente da Secretaria contra ameaças básicas e avançadas.</p> <p>É fundamental tratar a informação como um recurso estratégico e econômico, devido à crescente valorização dos dados pessoais e da informação como ativos de gestão do Estado. O uso inadequado desses recursos oferece um alto risco de impactos negativos e pode resultar em consequências indesejadas, como prejuízo financeiro, problemas operacionais, danos à imagem do órgão ou governo, vazamento de informações e dados pessoais, e até mesmo sequestro de dados.</p> <p>A SEDAM possui um parque computacional para atendimento aos usuários, com mais de 500 usuários ativos na rede, mais de 60 servidores virtuais dentre outros recursos, de acordo com o levantamento realizado no ambiente de infraestrutura de TI. A aferição do comportamento das estações de usuários e servidores virtuais, tem como objetivo detectar, bloquear, investigar e responder a incidentes de segurança da informação que possam ocorrer na rede da Secretaria.</p> <p>É essencial garantir a proteção e a integridade dos dados e sistemas da SEDAM, bem como a segurança dos usuários e da informação compartilhada. Portanto, é necessário implementar medidas de monitoramento contínuo, análise de logs, detecção de anomalias e resposta rápida a incidentes, a fim de mitigar riscos e garantir um ambiente seguro e confiável para as operações da Secretaria.</p> <p>Diante desse cenário, é fundamental investir em estratégias robustas de segurança da informação, incluindo a implementação de sistemas de detecção e prevenção de ameaças, atualizações regulares de software e hardware, treinamento e conscientização dos usuários, além de políticas de segurança claras e bem definidas. Além disso, é importante contar com equipes especializadas em segurança cibernética, capazes de identificar e responder rapidamente aos incidentes, minimizando danos e prejuízos.</p> <p>A proteção dos dados pessoais e a segurança das informações são responsabilidades compartilhadas, exigindo a colaboração de todos os usuários e organizações. É essencial promover uma cultura de segurança, estimulando a adoção de boas práticas e a conscientização sobre os riscos existentes. Somente assim poderemos enfrentar os desafios cada vez mais frequentes e sofisticados no mundo da segurança cibernética e garantir a integridade e confidencialidade dos dados de forma eficaz.</p> <p>Portanto, é crucial fornecer à SEDAM recursos de segurança atualizados, capazes de monitorar e responder a infecções causadas por software malicioso desenvolvido por indivíduos com más intenções. Esses recursos abrangem desde a exposição simples de informações obtidas até a exigência de pagamento de resgate para a liberação de dados sequestrados, como ocorre nos ataques de ransomware. Além disso, é essencial que esses recursos garantam a detecção proativa de ameaças, a implementação de medidas preventivas, a resposta rápida a incidentes e a recuperação eficiente dos sistemas afetados.</p> <p>Dessa forma, a contratação de recursos adicionais para cumprir com a LGPD é uma medida indispensável para garantir a proteção e preservar a privacidade dos usuários da SEDAM. Ao implementar as medidas de proteção adequadas, a secretaria estará em conformidade com a legislação vigente, assegurando a confidencialidade, integridade e disponibilidade dos dados pessoais sob sua responsabilidade.</p> <p>A contratação em questão tem como objetivo atender às necessidades de segurança da SEDAM, garantindo o cumprimento das diretrizes da Lei Geral de Proteção de Dados Pessoais (LGPD), implantação futura do Plano Diretor de Tecnologia da Informação PDTI e da Política de Segurança da Informação (PSI) dentre outras legislações relacionadas à segurança cibernética.</p> <p>O objetivo em questão visa minimizar a vulnerabilidade dos sistemas corporativos, redes, estações de trabalho, caixas postais, implementando metodologias de segurança de antivírus corporativo, prevenindo possíveis ataques internos e externos de vírus, spams e spywares e outras ameaças virtuais ao ambiente tecnológico da Secretaria.</p> <p>Além disso, a contratação visa estabelecer práticas de segurança cibernética sólidas, alinhadas com as melhores práticas e padrões do setor. Esse enfoque na segurança cibernética é essencial para mitigar riscos e proteger a integridade dos dados da Secretaria, sendo fundamental para garantir um ambiente seguro e confiável para a manipulação e proteção dos dados pessoais, cumprindo as exigências legais e fortalecendo a postura de segurança da secretaria.</p>

4. PREVISÃO DA DESPESA NO PLANO ANUAL DE COMPRAS:				
PROCESSO	DOCUMENTO	QUADRO	ITEM	DESCRIÇÃO
<a href="#">0028.024309/2024-62</a>	Documento de Formalização de Demanda 3 <a href="#">(0056529142)</a>	Serviços	09	Contratação de solução de antivírus para desktop
<a href="#">0028.024309/2024-62</a>	Documento de Formalização de Demanda 3 <a href="#">(0056529142)</a>	Serviços	10	Contratação de solução de antivírus para servidores de rede
Observação: informamos que a referida despesa não encontra-se prevista no Plano Anual de Compras 2024, visto que esta Secretaria detinha uma licenças, e a mesma expirou. Logo, esta Secretaria no presente momento não possui segurança para armazenamento dos dados e apresentamos a previsão no Plano anual de compras de 2025.				

5. PREVISÃO DO PLANEJAMENTO ESTRATÉGICO:			
DOCUMENTO	INSTRUMENTO	PLANO	DESCRIÇÃO
( <a href="#">Link externo</a> )	PLANEJAMENTO ESTRATÉGICO 2023 - 2027	Plano 3: Melhoria da Infraestrutura de TI	3.1.1 Assegurar infraestrutura adequada para a área de TI da SEDAM e garantir a evolução do parque tecnológico da SEDAM  3.3.1 Centralizar o gerenciamento dos computadores e ativos de rede

			3.4.1 Controle e monitoramento de segurança das atividades nas instalações da SEDAM
		Plano 5: Segurança da Informação	5.1.2 Monitorar a segurança dos ativos para uma melhor visibilidade dos eventos de segurança que acontecem na rede

6. JUSTIFICATIVA DO QUANTITATIVO:

A solução de segurança a ser contratada abrange proteção de Endpoint e proteção contra ataques avançados para usuário final, com todos os serviços necessários para uma implementação completa e eficaz. Essa solução deverá atender às necessidades específicas da Secretaria de Estado do Desenvolvimento Ambiental durante um período de 36 meses. Os componentes que compõem essa solução são os seguintes:

**SOLUÇÃO DE PROTEÇÃO AVANÇADA CONTRA ATAQUES CIBERNÉTICOS PARA ESTAÇÕES DE TRABALHO (EXTENDED DETECTION AND RESPONSE - XDR) (ITEM 1)**

Visa oferecer uma camada de defesa endpoints da rede, ajudando a prevenir, detectar e responder a ataques de malware, ransomware, vírus e outras ameaças. As proteções para endpoint geralmente incluem firewalls, antivírus, antimalware, detecção de intrusão, controle de aplicativos, gerenciamento de patches e outras ferramentas de segurança. Elas são essenciais para garantir a segurança dos dispositivos e dos dados armazenados neles, especialmente em ambientes corporativos, onde a proteção dos endpoints é crucial para a segurança global da rede.

**SOLUÇÃO DE PROTEÇÃO AVANÇADA CONTRA ATAQUES CIBERNÉTICOS PARA SERVIDORES (EXTENDED DETECTION AND RESPONSE - XDR) (ITEM 2)**

A proteção para servidores em um ambiente corporativo é de extrema importância porque os servidores são peças fundamentais da infraestrutura de tecnologia da informação de uma empresa. Eles armazenam e processam dados críticos e sensíveis, além de hospedar aplicativos e serviços essenciais para o funcionamento do negócio.

**SERVIÇO DE SUPORTE PRO ATIVO, CORRETIVO E PARA RESPOSTA A INCIDENTES (ITEM 3)**

O serviço abrange suporte proativo, corretivo e resposta a incidentes, visando prevenir problemas, corrigir falhas e reagir rapidamente a eventos adversos para manter a estabilidade e segurança dos sistemas.

**SERVIÇO DE TREINAMENTO (ITEM 4)**

Esse serviço visa fornecer treinamento e transferência de conhecimento para os clientes. Ele oferece capacitação especializada, permitindo que os usuários adquiram habilidades e compreensão sobre o uso eficaz das soluções ou tecnologias implementadas, capacitando-os a gerenciar, operar e manter os sistemas.

Faz-se necessário a aquisição de 800 licenças para estações de trabalho e 300 licenças para servidores considerando o crescimento da secretaria ao longo dos anos;

Faz-se necessário a aquisição da prestação de serviços especializados para resposta a incidentes e monitoramento ativo;

Faz-se necessário a aquisição de 03 unidades de treinamento para a compreensão completa da ferramenta, permitindo a configuração, análise e autonomia por parte da secretaria.

ITEM	DESCRIÇÃO	MÉTRICA	QUANTIDADE
01	Solução de proteção avançada contra ataques cibernéticos para estações de trabalho (Extended detection and response - XDR)	Licenças	800
02	Solução de proteção avançada contra ataques cibernéticos para servidores (Extended detection and response - XDR)	Licenças	300
03	Serviços de suporte pro ativo, corretivo e para resposta a incidentes	Meses	60
04	Serviço de treinamento	Unidade	03

7. NÍVEL MÉDIO DE SERVIÇO:

Em atenção ao Art. 18, X, da Lei nº 14.133/21, apresentamos o estudo para análise de riscos para o presente objeto: <b>Registro de preço para futura e eventual contratação de empresa para fornecimento de solução de proteção para estações de trabalho e servidores contra ataques cibernéticos</b> :				
O atendimento deve ser contínuo, 24 horas por dia, 7 dias por semana, durante todo o ano, incluindo feriados, em língua portuguesa. O início do atendimento e o prazo de solução devem ser determinados de acordo com o nível de severidade exigido para o caso, conforme os índices de criticidade abaixo:				
Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço	Glosa (por evento) para eventual descumprimento
Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto nas operações críticas de negócio.  Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção.  Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 2 horas deve ter um técnico do fornecedor on-site.	Em até 8 horas	10%
		Em até 4 horas deve ter um técnico do fornecedor on-site.	Entrega da Solução pelo fabricante em até 6 dias.	
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade.  Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado.  As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Em até 4 horas deve ter um técnico do fornecedor on-site.	Em até 4 horas deve ter um técnico do fornecedor on-site.	7,50%
		Em até 2 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou retorno de chamada. Gerente técnico do fabricante deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.	Em até 16 horas	
			Entrega da Solução pelo fabricante em até 10 dias.	
Severidade 3	O defeito não gera impacto ao negócio.  Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	Um técnico do fornecedor on-site ou atendimento remoto.	Em até 24 horas.	5%
		Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato.	Entrega da Solução pelo fabricante em até 15 dias ou na próxima atualização do Software.	
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação.  Exemplos:	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 12 horas um técnico do fornecedor entra em contato.	2%

15/05/2025, 11:23		SEI/RO - 0059485479 - Estudo Técnico Preliminar			
		O problema não afetou as operações da contratante negativamente;  Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.			
<p>Para cada chamado de suporte categorizado como grau de severidade 1, o recurso previsto na tabela acima deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante. É importante destacar que todos os prazos para atendimento da garantia começarão a ser contados a partir da abertura do chamado, independentemente de ter sido feito via telefone, e-mail, site da contratada ou do fabricante. Além disso, o período de suporte deve estar diretamente atrelado ao período de garantia da solução.</p> <p>Dentro do prazo máximo de atendimento, cabe ao fornecedor dar início, junto ao contratante, às providências que serão adotadas para a solução do chamado. Considera-se plenamente solucionado o problema quando os sistemas/serviços forem restabelecidos sem restrições, ou seja, quando não se tratar de uma solução paliativa.</p> <p>Para os chamados de severidades 1 e 2, os serviços de atendimento de garantia não podem ser interrompidos até o completo restabelecimento de todas as funções do sistema paralisado, mesmo que isso exija períodos noturnos e dias não úteis (sábados, domingos e feriados). Além disso, os chamados de garantia de severidades 1 e 2 devem contar com suporte in loco da contratada para agilizar o restabelecimento do serviço.</p> <p>O fornecedor emitirá um relatório, sempre que solicitado pelo contratante, em formato eletrônico, preferencialmente em arquivo texto, contendo informações analíticas e sintéticas dos chamados da garantia abertos e fechados no período. Esse relatório deve incluir:</p> <ul style="list-style-type: none"><li>• Quantidade de ocorrências (chamados) registradas no período.</li><li>• Número do chamado registrado e nível de severidade, incluindo reaberturas. Data e hora de abertura.</li><li>• Data e hora de início e conclusão do atendimento.</li><li>• Identificação do técnico do contratante que registrou o chamado.</li><li>• Identificação do técnico do contratante que atendeu o chamado da garantia. Descrição do problema.</li><li>• Descrição da solução.</li><li>• Informações sobre eventuais escalonamentos.</li><li>• Resumo da lista de chamados concluídos fora do prazo de solução estabelecido.</li><li>• Total de chamados no mês e o total acumulado até a apresentação do relatório.</li></ul> <p>Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante.</p> <p>Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante.</p> <p>Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução.</p> <p>Para esses problemas, o fornecedor deverá, nos prazos estabelecidos nos níveis de criticidade, restabelecer o ambiente, através de uma solução de contorno e informar ao contratante, em um prazo máximo de 24 (vinte e quatro) horas, quando a solução definitiva será disponibilizada para o contratante.</p> <p>Esta solução definitiva de que trata o subitem anterior deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias úteis, no caso da necessidade de criação de um patch/fix.</p>					

8. ESTIMATIVA DA DESPESA:
Estimativa da despesa conforme Quadro Comparativo de Preços ( <a href="#">0056463759</a> ).

9. SOLUÇÕES DISPONÍVEIS NO MERCADO:

A proteção física e lógica da informação deve ser provida por ferramentas especializadas, seguras, consolidadas e, acima de tudo, que preservem a confidencialidade, a integridade e a disponibilidade da informação.

Em observância ao disposto na Instrução Normativa SGD/ME IN SGD /ME nº 94/2022, apresenta-se a seguir a avaliação de soluções e a capacidade de cada uma delas para atender aos requisitos de proteção de e-mail, endpoints e defesa contra ataques avançados.

As opções de soluções corporativas para solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados disponíveis no mercado são vastas e apresentam diversas versões. Para auxiliar na análise, segue abaixo uma lista dos 5 principais fabricantes de soluções, classificados pelo Gartner de acordo com o número de avaliações, do mais alto ao mais baixo.



Products 1 - 20 | [View by Vendor](#)

Review weighting ⓘ

☐ Reviewed in Last 12 Months

Number of Ratings, High to Low ▼

4.7 ★★★★★ 1111 Ratings


5 Star 75%

4 Star 23%

3 Star 2%

2 Star 0%

1 Star 0%



SentinelOne Singularity Platform

by SentinelOne

"Versatile Cybersecurity Tool: More Than Just Traditional Protection"

The service from our technical advisor and the support team has been quick and thorough every time I've needed help. The team is highly educated and has spent time providing answers, examples ...

[Read Reviews](#)

Competitors and Alternatives

SentinelOne vs CrowdStrike

SentinelOne vs Microsoft

SentinelOne vs Sophos

[See All Alternatives](#)

4.7 ★★★★★ 568 Ratings


5 Star 77%

4 Star 20%

3 Star 2%

2 Star 0%

1 Star 0%



CrowdStrike Falcon

by CrowdStrike

"CrowdStrike Falcon is the #1 tool your Cyber Security Team needs now. "

Crowdstrike Falcons is at the forefront of security tools all companies of all industries should have. The Falcon Sandbox has been incredibly instrumental in assisting us evaluate suspicious files we are sent ...

[Read Reviews](#)

Competitors and Alternatives

CrowdStrike vs Microsoft

CrowdStrike vs SentinelOne

CrowdStrike vs Sophos

[See All Alternatives](#)

4.7 ★★★★★ 263 Ratings


5 Star 75%

4 Star 24%

3 Star 1%

2 Star 0%

1 Star 0%



Trend Micro XDR

by Trend Micro

"Perfect security in No time"

It gives more granular level of security. It has faster detection technique which helps to prevent the infra from unknown and new attacks. It provides unified view and of various tools and attacks.

[Read Reviews](#)

Competitors and Alternatives

Trend Micro vs CrowdStrike

Trend Micro vs Microsoft

Trend Micro vs Sophos

[See All Alternatives](#)

4.5 ★★★★★ 260 Ratings


5 Star 57%

4 Star 37%

3 Star 6%

2 Star 0%

1 Star 0%



Harmony Endpoint

by Check Point Software Technologies

"Harmony Endpoint: The Protection that Creates Harmony"

Seamless integration and implementation to our existing CP products and experience. By talking with our TAM, we were able to find and identify gaps in our environment where a managed solution such ...

[Read Reviews](#)

Competitors and Alternatives

Check Point Software Technologies vs Cisco

Check Point Software Technologies vs Fortinet

Check Point Software Technologies vs Microsoft

[See All Alternatives](#)

As soluções rankeadas fornecem os recursos principais a seguir:

SOLUÇÃO	PRINCIPAIS RECUROS
Singularity XDR (SentinelOne)	<ul style="list-style-type: none"><li>• Automatização detecção e resposta de Endpoint;</li><li>• Proteção de carga de trabalho;</li><li>• Modelo de prevenção com tecnologia de IA;</li><li>• Detecção e resposta proativas em tempo real.</li></ul>
CrowdStrike Falcon (CrowdStrike)	<ul style="list-style-type: none"><li>• Antivírus de última geração (NGAV);</li><li>• Detecção e resposta de endpoint;</li><li>• Investigação gerenciada de ameaças;</li><li>• Inteligência de ciberameaça.</li></ul>
Trend Micro XDR (Trend Micro)	<ul style="list-style-type: none"><li>• Correlação avançada de ameaças;</li><li>• Investigação e resposta rápidas a ameaças;</li><li>• Detecção precoce e precisa de ameaças;</li><li>• Detecção e resposta em Endpoints.</li></ul>
Harmony Endpoint (Check Point Software Technologies)	<ul style="list-style-type: none"><li>• Proteção completa de endpoint;</li><li>• Anti-Ransomware;</li><li>• Proteções de ataque de malware e file-less;</li><li>• Prevenção de roubo de credenciais.</li></ul>
Microsoft Defender for Endpoint (Microsoft)	<ul style="list-style-type: none"><li>• Gerenciamento de vulnerabilidades com base em risco;</li><li>• Proteção habilitada para a nuvem e baseada em comportamento;</li><li>• EDR (Detecção e Resposta de Ponto de Extremidade);</li><li>• Investigação e correção automática.</li></ul>

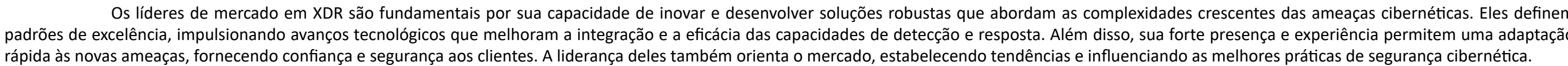
Como se pode observar, há diversas opções disponíveis no mercado com recursos avançados para proteção e segurança cibernética. Cada uma das soluções apresentadas possui características específicas que visam atender às necessidades das organizações em termos de detecção, resposta e prevenção de ameaças. Essas soluções são desenvolvidas por fabricantes renomados e reconhecidos pelo Gartner, o que confere uma qualidade e confiabilidade adicionais.

Abaixo, os quadrantes do Gartner e do Forrester Wave são ferramentas amplamente utilizadas para avaliar e comparar soluções de tecnologia em diversos setores, incluindo segurança cibernética e Extended Detection and Response (XDR). Cada um desses relatórios tem seu próprio formato e metodologia, mas ambos têm o objetivo de ajudar empresas a tomar decisões informadas sobre fornecedores e produtos:

Quadrante de fabricantes - Gratner	Quadrante de fabricantes - Forrester
------------------------------------	--------------------------------------

https://sei.sistemas.ro.gov.br/sei/controlador.php?acao=documento\_visualizar&acao\_origem=arvore\_visualizar&id\_documento=61505058&infra\_sistema=100000100&infra\_unidade\_atual=110000209&infra\_hash=6dfce1948c8ad9c7363973fb321635a9c101d65d2400290b63080bc32e7f7d0c

11/16



## 6.1. Requisitos e funcionalidades técnicos da solução

6.1.1. A especificação técnica mínima e obrigatória da solução encontra-se detalhada no Anexo I deste estudo.

## 9.2. Requisitos de manutenção e garantia

6.2.1. A empresa contratada é responsável por fornecer suporte técnico e garantia de atualização da solução pelo período de 60 meses, a contar da data de emissão do Termo de Recebimento. É importante ressaltar que essa garantia não se limita ao término da vigência contratual.

#### 6.2.2. A garantia deve incluir obrigatoriamente:

- 6.3.2.1. Atualização das versões dos softwares fornecidos, caso sejam disponibilizadas novas versões.
- 6.3.2.2. Atualização dos softwares fornecidos caso haja lançamento de novos softwares que substituam os fornecidos ou se ficar evidente a descontinuidade dos softwares fornecidos, mesmo que não se trate de substituição direta.
- 6.3.2.3. Correções dos softwares fornecidos, incluindo a aplicação de patches para corrigir eventuais falhas (bugs) de software que possam prejudicar o ambiente de produção ou vulnerabilidades que comprometam a segurança da solução.

6.3.3. A garantia deverá ser prestada durante todo o período de contrato e aditivos relacionados à atualização das licenças e proteção.

6.3.4. Durante o período de garantia, a empresa contratada compromete-se a substituir, em até 15 dias úteis, os equipamentos que apresentarem, em um período de 60 dias, duas ocorrências de defeitos por inoperância do produto ou 3 ocorrências de deficiência operacional do produto.

6.3.5. As ferramentas e equipamentos necessários à manutenção serão de responsabilidade da contratada.

## 6.4. Suporte técnico

6.4.1. Deverá ser oferecido suporte técnico da Contratada, com a possibilidade de abertura de chamados, das 7h00 às 20h00, em dias úteis, para a resolução de problemas. É importante destacar que os serviços de suporte técnico devem contemplar as manutenções corretivas e evolutivas para a solução contratada e não podem acarretar custos adicionais ao CONTRATANTE, além do que foi previamente acordado.

6.4.2. A empresa contratada deve encaminhar o chamado para o suporte do fabricante sempre que necessário, seja devido à criticidade, impacto ou urgência do problema, ou caso seja necessário o envolvimento direto do fabricante no processo de correção. É imprescindível que seja fornecido acesso ao site do fabricante para acompanhamento dos chamados, acesso à base de conhecimento e aos fóruns relacionados à solução.

6.4.3. Os serviços de suporte técnico abrangem:

- 6.4.3.1. Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução.
- 6.4.3.2. Elaboração de relatórios, estudos e diagnósticos sobre o ambiente.
- 6.4.3.3. Transferência de conhecimento aos técnicos da Contratante referente aos problemas vivenciados e às soluções aplicadas, na forma a ser determinada pelas partes.
- 6.4.3.4. Realização de instalação, atualização e configuração de novas versões dos produtos após a disponibilização das atualizações tecnológicas pelo fabricante.

6.4.4. O suporte técnico deve contemplar o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso do software ou para correção de problemas, em especial na configuração de parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução.

6.4.5. O suporte técnico deve contemplar, quando for o caso, atendimento a eventual problema de instalação ou configuração de softwares básicos e de infraestrutura de TIC (sistemas operacionais, servidores de banco de dados, servidores de aplicação, etc.) necessários ao funcionamento da solução.

4.4.6. Deve contemplar também a atualização de versões do software aplicativo, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela fabricante, num empacotamento estável do sistema. O serviço de atualização de versão tem por finalidade assegurar a devida atualização da solução durante o período de vigência da garantia. Refere-se ao fornecimento de novas versões e releases da solução lançados no período. A cada nova liberação de versão e release, serão disponibilizados em formato digital manuais e demais documentos técnicos, bem como nota informativa das funcionalidades implementadas. Em caso de lançamento de patch de correção, a CONTRATADA deverá comunicar o fato ao CONTRATANTE e indicar a forma de obtenção e os defeitos que serão corrigidos pelo patch. Em ambos os casos, a comunicação deve ser feita no prazo de até 30 dias, a contar do lançamento de nova versão ou solução de correção.

6.4.7. A CONTRATADA será responsável pelos serviços de implantação das novas versões e releases dos produtos por ela fornecidos como partes do objeto, bem como pela aplicação dos patches de correção e pacotes de serviço (service packs) relativos a esses produtos. Para a implantação das novas versões/releases, bem como para a aplicação dos patches, deverá ser aberto chamado de suporte técnico com nível de severidade adequado e a prestação dos serviços deve ser agendada com os responsáveis pela solução na CONTRATANTE;

6.4.8. Deverá ser prestado suporte técnico remoto com atendimento mediante registro de chamados em página de website, em sistema fornecido pela CONTRATADA e/ou pelo fabricante; e também através de contato telefônico. Esse serviço destina-se a esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução CONTRATADA;

6.4.9. As peças substitutas deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento e devem integrar a garantia da solução;

6.4.10. A CONTRATADA auxiliará o CONTRATANTE na reinstalação das ferramentas, caso seja necessário, ao longo do tempo de garantia da ferramenta;

**6.4.11. A CONTRATADA deverá disponibilizar os seguintes canais de acesso ao suporte técnico:**

- 6.4.11.1. Portal Web;
- 6.4.11.2. E-mail;
- 6.4.11.3. Central 0800; e/ou
- 6.4.11.4. Telefone fixo.

6.4.12. O atendimento deve ser contínuo, 24 horas por dia, 7 dias por semana, durante todo o ano, incluindo feriados, em língua portuguesa. O início do atendimento e o prazo de solução devem ser determinados de acordo com o nível de severidade exigido para o caso, conforme os índices de criticidade abaixo:

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço	Glosa (por evento) para eventual descumprimento
Severidade 1 (Alta)	Sistema parado ou produto inoperante com impacto nas operações críticas de negócio.  Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados essenciais corre risco de perda ou corrupção.  Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.	Em até 2 horas deve ter um técnico do fornecedor on-site.	Em até 8 horas	10%
		Em até 4 horas deve ter um técnico do fornecedor on-site.	Entrega da Solução pelo fabricante em até 6 dias.	
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade.  Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado.  As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Em até 4 horas deve ter um técnico do fornecedor on-site.	Em até 4 horas deve ter um técnico do fornecedor on-site.	7,5%
		Em até 2 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou retorno de chamada. Gerente técnico do fabricante deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.	Em até 16 horas	
			Entrega da Solução pelo fabricante em até 10 dias.	
Severidade 3	O defeito não gera impacto ao negócio.  Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	Um técnico do fornecedor on-site ou atendimento remoto.	Em até 24 horas.	5%
		Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato.	Entrega da Solução pelo fabricante em até 15 dias ou na próxima atualização do Software.	
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação.  Exemplos:  O problema não afetou as operações da contratante negativamente;  Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 12 horas um técnico do fornecedor entra em contato.	2%

6.4.13. Para cada chamado de suporte categorizado como grau de severidade 1, o recurso previsto na tabela acima deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante. É importante destacar que todos os prazos para atendimento da garantia começarão a ser contados a partir da abertura do chamado, independentemente de ter sido feito via telefone, e-mail, site da contratada ou do fabricante. Além disso, o período de suporte deve estar diretamente atrelado ao período de garantia da solução.

6.4.14. Dentro do prazo máximo de atendimento, cabe ao fornecedor dar início, junto ao contratante, às providências que serão adotadas para a solução do chamado. Considera-se plenamente solucionado o problema quando os sistemas/serviços forem restabelecidos sem restrições, ou seja, quando não se tratar de uma solução paliativa.

6.4.15. Para os chamados de severidades 1 e 2, os serviços de atendimento de garantia não podem ser interrompidos até o completo restabelecimento de todas as funções do sistema paralisado, mesmo que isso exija períodos noturnos e dias não úteis (sábados, domingos e feriados). Além disso, os chamados de garantia de severidades 1 e 2 devem contar com suporte in loco da contratada para agilizar o restabelecimento do serviço.

6.4.16. O fornecedor emitirá um relatório, sempre que solicitado pelo contratante, em formato eletrônico, preferencialmente em arquivo texto, contendo informações analíticas e sintéticas dos chamados da garantia abertos e fechados no período. Esse relatório deve incluir:

- 6.4.16.1. Quantidade de ocorrências (chamados) registradas no período.
- 6.4.16.2. Número do chamado registrado e nível de severidade, incluindo reaberturas. Data e hora de abertura.
- 6.4.16.3. Data e hora de início e conclusão do atendimento.
- 6.4.16.4. Identificação do técnico do contratante que registrou o chamado.
- 6.4.16.5. Identificação do técnico do contratante que atendeu o chamado da garantia. Descrição do problema.
- 6.4.16.6. Descrição da solução.
- 6.4.16.7. Informações sobre eventuais escalonamentos.
- 6.4.16.8. Resumo da lista de chamados concluídos fora do prazo de solução estabelecido.
- 6.4.16.9. Total de chamados no mês e o total acumulado até a apresentação do relatório.

6.4.17. Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante.

6.4.18. Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante.

6.4.19. Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução.

6.4.20. Para esses problemas, o fornecedor deverá, nos prazos estabelecidos nos níveis de criticidade, restabelecer o ambiente, através de uma solução de contorno e informar ao contratante, em um prazo máximo de 24 (vinte e quatro) horas, quando a solução definitiva será disponibilizada para o contratante.

6.4.21. Esta solução definitiva de que trata o subitem anterior deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias úteis, no caso da necessidade de criação de um patch/fix.

6.5. Requisitos sociais, ambientais e culturais

6.5.1. A Contratada deve aderir aos padrões estabelecidos pelo Modelo de Acessibilidade em Governo Eletrônico (e-MAG), conforme a Portaria Normativa SLTI nº 03, de 7 de maio de 2007. Essa aderência é necessária quando houver a necessidade de tornar o aplicativo acessível para solicitações de suporte técnico, visando garantir a inclusão e acessibilidade para todos os usuários.

6.5.2. Os serviços prestados pela Contratada devem sempre considerar o uso racional de recursos e equipamentos, com o objetivo de evitar o desperdício de insumos e materiais, bem como a geração excessiva de resíduos. Essa prática está alinhada com as diretrizes de responsabilidade ambiental adotadas pela Contratante.

6.5.3. A Contratada é responsável por fornecer orientações aos seus funcionários sobre a importância da racionalização de recursos no desempenho de suas atribuições, assim como sobre as diretrizes de responsabilidade ambiental adotadas pela Contratante. Essas orientações devem destacar a importância de reduzir o consumo de recursos, reutilizar materiais sempre que possível e realizar descarte adequado dos resíduos.

6.5.4. Além disso, a Contratada deve autorizar a participação de seus funcionários em eventos de capacitação e sensibilização promovidos pela Contratante, quando necessário. Esses eventos têm como objetivo fornecer conhecimentos e práticas relacionadas à racionalização de recursos e responsabilidade ambiental, visando aprimorar a conscientização e o desempenho sustentável da equipe da Contratada.

6.6. Requisitos Temporais

6.6.1. As diretrizes relacionadas aos requisitos a seguir deverão ser considerados no processo de atendimento, entrega e instalação de equipamentos e serviços:

Prazo de início de atendimento para suporte técnico e manutenção pela garantia:

6.6.1.1. O início do atendimento deve seguir o que está especificado no acordo de nível de serviço presente no Termo de Referência.

Prazo de entrega e instalação:

6.6.1.2. O prazo de entrega e instalação deve estar de acordo com o que foi especificado no Termo de Referência. Caso não haja uma definição específica, o prazo padrão será considerado conforme a ordem de serviço.

Local de entrega dos equipamentos e licenças de software:

6.6.1.3. Os equipamentos e licenças de software devem ser entregues conforme disposto no Termo de Referência.

Horário de entrega dos equipamentos/serviços:

6.6.1.4. A entrega dos equipamentos/serviços deve ocorrer entre as 07:30 e 13:30. É possível agendar uma data e hora específica previamente com a CONTRATANTE.

Verificação da conformidade dos materiais entregues:

6.6.1.5. É responsabilidade da CONTRATANTE rejeitar, total ou parcialmente, os materiais entregues que não estejam de acordo com o objeto definido no Termo de Referência.

Recebimento dos produtos:

6.6.1.6. O recebimento dos produtos será feito pela equipe designada pela CONTRATANTE. Esse recebimento ocorrerá de forma provisória no momento da entrega dos equipamentos e de forma definitiva após a instalação, configuração e teste da solução.

6.7. Requisitos de Segurança e Privacidade

6.7.1. A CONTRATADA deve seguir os regulamentos, normas e instruções de segurança da informação e comunicações adotados pela CONTRATANTE. Isso inclui a Política de Segurança da Informação e Comunicações e suas Normas Complementares durante a execução dos serviços nas instalações da Secretaria.





A implementação desta solução busca otimizar a gestão da segurança da informação, estabelecendo uma defesa coordenada e planejada que responda de maneira ágil e eficaz às ameaças digitais, sem interrupções nos serviços e de forma economicamente viável. Além disso, ao garantir um sistema de segurança contínua e inteligente, a solução visa mitigar riscos operacionais, como indisponibilidade de sistemas ou perda de dados sensíveis, que poderiam comprometer a continuidade das operações institucionais.

Em termos de infraestrutura, a solução requer integração com os ambientes tecnológicos existentes no órgão, sem necessidade de mudanças estruturais significativas. A arquitetura XDR permite uma implementação escalável e adaptável, com gestão centralizada e visibilidade completa dos pontos finais e das redes monitoradas.

Os resultados esperados com a implementação desta solução incluem:

**Continuidade das atividades operacionais:** Proteção constante contra ameaças cibernéticas, garantindo a disponibilidade dos serviços públicos.

**Redução de riscos operacionais:** Mitigação de impactos causados por ataques, como ransomware, malware, phishing e outros vetores de ameaça.

**Eficiência na gestão de segurança:** Centralização da detecção e resposta a incidentes, com relatórios analíticos e alertas em tempo real, permitindo decisões rápidas e embasadas.

**Segurança e qualidade na proteção de dados e sistemas:** Garantia de que os ambientes estejam protegidos com tecnologias atualizadas e práticas alinhadas às normas de segurança da informação.

Dessa forma, a solução como um todo proporciona uma abordagem prática e eficaz para atender às necessidades de segurança cibernética nas Secretarias do Governo do Estado de Rondônia, com foco em proteção contínua, inteligência operacional e otimização dos recursos públicos.

14. RESULTADOS PRETENDIDOS:

Com o objetivo da implantação de novas políticas de segurança, projeta-se um cenário primordial para controle e proteção contra ameaças básicas e avançadas no âmbito desta Secretaria de Estado do Desenvolvimento Ambiental - SEDAM, adotando padrões e diretrizes para melhor eficiência .

O monitoramento contínuo dos endpoints da SEDAM em busca de atividades suspeitas, garante uma segurança proativa e eficaz, permitindo a identificação e mitigação de ameaças antes que elas possam causar danos significativos à organização.

Detecção avançada de ameaças que outros sistemas de segurança podem não conseguir detectar. Por meio da análise comportamental dos endpoints, a solução pode identificar padrões suspeitos e agir de forma rápida e efetiva para lidar com os incidentes de segurança, reduzindo os danos potenciais à organização.

Resposta automatizada a incidentes, adotando medidas como bloquear o acesso ao endpoint infectado, isolá-lo da rede ou executar ações de limpeza para remover o malware. Essa resposta automatizada agiliza o tempo de resposta aos incidentes, minimizando o impacto na organização.

Análise forense aprofundada dos endpoints comprometidos. A solução é capaz de capturar registros de eventos, memória e arquivos, o que facilita a identificação da origem da ameaça e a implementação de medidas preventivas para evitar futuros incidentes no ambiente da organização.

Ao automatizar a detecção e resposta a ameaças comuns, a solução de antivírus corporativa contribui para o aumento da eficiência operacional da equipe de segurança. Isso permite que os profissionais se dediquem a tarefas mais críticas e estratégicas, reduzindo a carga de trabalho e otimizando o uso dos recursos disponíveis.

RESULTADOS A SEREM ALCANÇADOS	
01	Capacidade de detecção e resposta de ameaças em tempo real
02	Proteção contra ameaças avançadas
03	Análises avançadas de malware
04	Visibilidade gráfica detalhada do ambiente
05	Maior taxa de acurácia de detecções
06	Inteligência de ameaças
07	Implantação de atualizações automáticas e automatizadas
08	Controle avançado do inventário de endpoints
09	Capacidade de resposta a incidentes
10	Redução do risco de incidentes

15. PODERÁ HAVER A PARTICIPAÇÃO DE PESSOAS FÍSICAS E SOCIEDADE COOPERATIVA NA CONTRATAÇÃO/AQUISIÇÃO?

Em atenção ao art. 34, inciso XIV do Decreto Estadual nº 28.874/2024 e art. 16 da [Lei nº 14.133, de 01 de abril de 2021](#), justifica-se a exclusão de participação de pessoas físicas e de sociedades em forma de cooperativa no presente processo, considerando que a Administração Pública tem a obrigação de garantir a segurança e a qualidade dos itens que contrata ou adquire.

Em razão disso, é importante que os contratados tenham a capacidade técnica e a estrutura necessária para prestar o serviço de forma adequada.

Desta forma, as pessoas físicas e sociedades em forma de cooperativa, podem não possuir a mesma capacidade técnica e estrutura que empresas especializadas.

Por isso, a participação de pessoas físicas e sociedades em forma de cooperativa na aquisição pretendida pode colocar em risco a segurança e a qualidade dos serviços a serem prestados.

16. ESTIMATIVA DO VALOR DA CONTRATAÇÃO:

Conforme Quadro Comparativo de Preços ([0056463759](#)).

17. PROVIDÊNCIAS A SEREM ADOTADAS:

**Não serão necessárias** providências para promover a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, tendo em vista que não há contrato vigente no órgão para o mesmo objeto.

18. PROVIDÊNCIAS A SEREM ADOTADAS:

**Não serão necessárias** providências para promover a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, tendo em vista que não há contrato vigente no órgão para o mesmo objeto.

19. DESCREVER AS CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES:

**Não há** processo relacionado a contratação ou aquisição no qual fora solicitada.

20. POSSÍVEIS IMPACTOS AMBIENTAIS:

**Não se aplica** a solução proposta a ser adquirida, tendo em vista que trata-se de um software e não produto físico.

21. DESCRIÇÃO DAS PROVIDÊNCIAS A SEREM REALIZADAS ANTES DA CELEBRAÇÃO DO CONTRATO, SE COUBER:

**Não serão necessárias** providências adicionais ou ajustes para a utilização da solução de segurança contratada.

22. DAS CONDIÇÕES DE ENTREGA:
Por se tratar de produtos de softwares e serviços, a CONTRATADA deve se iniciar a prestação dos serviços após a celebração do CONTRATO.

23. PRAZO PARA INÍCIO DA EXECUÇÃO DO SERVIÇO E/OU ENTREGA DE MATERIAL:
Por se tratar de produtos de softwares e serviços, a CONTRATADA deve se iniciar a prestação dos serviços após a celebração do CONTRATO.

24. POSICIONAMENTO CONCLUSIVO / VIABILIDADE OU NÃO DA CONTRATAÇÃO:
Diante dos fatos apresentados, avaliamos que a aquisição de uma solução de segurança de poteção de Endpoint para estações de trabalho e servidores viruais é viável e de suma importância para a continuidade dos negócios, proteção de intelecto e dados no âmbito desta Secretaria de Estado do Desenvolvimento Ambiental.

Porto Velho, data e hora do sistema.

Elaboração  
**VICTOR DA SILVA TAVARES**  
Assessor - CTI/SEDAM  
[assinatura eletrônica]

Revisão e Validação  
**RENATA DOS SANTOS LUZ COUTINHO**  
Coordenadora de Tecnologia da Informação - SEDAM  
[assinatura eletrônica]

De acordo  
**MARCO ANTONIO RIBEIRO DE MENEZES LAGOS**  
Secretário de Estado do Desenvolvimento Ambiental - SEDAM



Documento assinado eletronicamente por **VICTOR DA SILVA TAVARES, Assessor(a)**, em 24/04/2025, às 10:08, 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 **RENATA DOS SANTOS LUZ, Coordenador(a)**, em 24/04/2025, às 10:23, 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 **MARCO ANTÔNIO RIBEIRO DE MENEZES LAGOS, Secretário(a)**, em 24/04/2025, 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](#).



A autenticidade deste documento pode ser conferida no site [portal do SEI](#), informando o código verificador **0059485479** e o código CRC **8EC80AC1**.



GOVERNO DO ESTADO DE RONDÔNIA  
Secretaria de Estado do Desenvolvimento Ambiental - SEDAM

MAPA DE RISCO

MAPA DE RISCO											
<b>OBJETO:</b> Registro de preço para futura e eventual contratação de empresa para fornecimento de solução de proteção para estações de trabalho e servidores contra ataques cibernéticos.											
<b>PROCESSO:</b> 0028.020065/2024-49											
IDENTIFICAÇÃO DE RISCO			NÍVEL DE RISCO			PRIORIZAÇÃO	RESPOSTA (M, A, T ou E)	AÇÕES SUGERIDAS	PLANO DE AÇÃO		
Risco	Causa do Risco	Consequência(s)	P	I	(P)x(I)				Quem?	Quando?	Como?
<div>( X ) ELABORAÇÃO DO ESTUDO TÉCNICO PRELIMINAR - ETP</div> <div>ETAPA: (   ) ELABORAÇÃO DO TERMO DE REFERÊNCIA - TR</div> <div>(   ) GESTÃO DO CONTRATO</div>											
Definição imprecisa do escopo técnico	Falta de clareza nas especificações	Contratação de um serviço inadequado às necessidades, necessidade de renegociação ou aditivos contratuais	2	4	8	Médio	T	Elaborar um termo de referência detalhado com apoio de especialistas técnicos.	CTI	Imediato	Definir com precisão as necessidades técnicas , administrativas e gerenciais evitando a aquisição de um equipamento inadequado.
Participantes não qualificados na licitação	Falta de critérios técnicos rigorosos na seleção dos participantes	Risco de contratação de empresas sem experiência ou capacidade técnica para atender ao projeto.	2	5	10	Médio	T	Estabelecer critérios técnicos rigorosos na análise das propostas, incluindo exigência de experiência comprovada e capacidade técnica.	CTI	Imediato	Garantir a participação de empresas qualificadas e capazes de atender às necessidades do projeto.
A contratada não entregar todos os serviços no prazo	Problemas logísticos ou falha do fornecedor	Redução na capacidade de atendimento à população	3	5	15	Alto	T	Estabelecer cláusulas contratuais com penalidades por atraso e garantir monitoramento contínuo.	CTI e COPAF	Imediato	Monitorar prazos e aplicar sanções conforme contrato.
Treinamento e capacitação do capital humano sem eficácia	Baixo engajamento dos participantes ou qualidade do treinamento	Uso ineficaz do serviços contratados devido à falta de conhecimento	2	5	10	Médio	A	Acompanhar o progresso dos treinamentos e realizar avaliações.	CTI	Imediato	Avaliar desempenho e engajamento dos participantes.
Intercorrências no processo de contratação	Atraso na finalização do processo de contratação	- Ampliação dos prazos - Impactos negativos no cronograma geral	3	5	15	Alto	A	Durante o planejamento da contratação, utilizar listas estruturadas de verificações e	SUPEL	Imediato	Priorizar as possíveis correções no ETP, TR e outros artefatos



		- Aumento do custo administrativo						documentos padrões			utilizados no processo de contratação.
Falha na estimativa dos quantitativos	- Estimativa subestimada ou superestimada, resultando em prejuízos para a administração.	- Sobrecarga orçamentária - Recursos insuficientes para execução plena - Aumento do risco de judicialização	2	5	10	Médio	T	Validar o escopo técnico com os líderes de negócio e com os gestores.  - Consultar diferentes equipes de desenvolvimento para validar a estimativa.	CTI	Imediato	- Caso a contratação tenha sido subestimada, avaliar a possibilidade de aditivo do contrato.  - Caso a contratação tenha sido superestimada, deverá faturar apenas os quantitativos que forem realizados.
Atraso no processo de implantação da solução	Problemas técnicos ou falha de planejamento	<b>Custos adicionais:</b> A necessidade de realizar trabalhos extras, como horas extras, contratação de terceiros ou aquisição de equipamentos adicionais, pode gerar custos inesperados.  <b>Perda de receita:</b> O atraso na entrega da solução pode levar à perda de receita, especialmente em projetos com prazos contratuais e penalidades por atraso.  <b>Aumento dos custos de oportunidade:</b> O dinheiro investido no projeto poderia estar sendo utilizado em outras iniciativas, gerando retornos financeiros.	3	4	12	Alto	E	Realizar reuniões de controle e aplicar penalidades em caso de atrasos.	CTI e COPAF	Imediato	Identificação dos responsáveis e processamento das sanções previstas no TR e no Contrato. Saneamento dos problemas ou, dependendo, rescisão unilateral do contrato

Para elaboração do Mapa acima foram consideradas a Matriz de Risco e a Escala abaixo:

MATRIZ DE RISCO						
IMPACTO (I)	Muito Alto 5	5 (RM)	10 (RM)	15 (RA)	20 (RE)	25 (RE)
	Alto 4	4 (RB)	8 (RM)	12 (RA)	16 (RA)	20 (RE)
	Médio 3	3 (RB)	6 (RM)	9 (RM)	12 (RA)	15 (RA)



	Baixo 2	2 (RB)	4 (RB)	6 (RM)	8 (RM)	10 (RM)
	Muito Baixo 1	1 (RB)	2 (RB)	3 (RB)	4 (RB)	5 (RM)
		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

Legenda para a coluna "RESPOSTA"			
M	A	T	E
Mitigar	Aceitar	Transferir	Evitar

Porto Velho, 26 de novembro de 2024.

VICTOR DA SILVA TAVARES  
Assessor - CTI/SEDAM

RENATA DOS SANTOS LUZ COUTINHO  
Coordenadora de Tecnologia da Informação - SEDAM



Documento assinado eletronicamente por **VICTOR DA SILVA TAVARES, Assessor(a)**, em 28/11/2024, às 09:08, 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 **RENATA DOS SANTOS LUZ, Coordenador(a)**, em 28/11/2024, às 10:32, 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 **0055171825** e o código CRC **AD005EAD**.

Referência: Caso responda este(a) Mapa de Risco, indicar expressamente o Processo nº 0028.020065/2024-49

SEI nº 0055171825

Criado por 04391339200, versão 12 por 04391339200 em 28/11/2024 09:07:42.



GOVERNO DO ESTADO DE RONDÔNIA  
Secretaria de Estado do Desenvolvimento Ambiental - SEDAM

**MINUTA DE CONTRATO**

**CONTRATANTE:** O ESTADO DE RONDÔNIA, por intermédio da **Secretaria de Estado do Desenvolvimento Ambiental - SEDAM**, inscrita no **CNPJ: 63.752.604/0001-04**, com sede na Rua Farquar, n. 2986, Complexo Rio Madeira, Bairro Pedrinhas, Rio Madeira – Edifício Rio Cautário, Curvo 2, 2º andar, no Município de Porto Velho/RO, neste ato representada pelo Secretário de Estado do Desenvolvimento Ambiental - SEDAM, o Sr. **MARCO ANTÔNIO RIBEIRO DE MENEZES LAGOS**, portador(a) do CPF nº - **\*\*\*.448.432-\*\***.

**CONTRATADA:** A Empresa XXX inscrita sob o **CNPJ nº XXX**, com endereço na Rua: XXX, Bairro: XXX, CEP: XXX, no Município de XXX, representada pelo Sr. (a) XXX, portador(a) do CPF nº **XXX**, conforme poderes que lhe são outorgados.

Celebram, por força do presente **CONTRATO ADMINISTRATIVO**, na modalidade de **PREGÃO ELETRÔNICO**, o qual se regerá pelas disposições da [Lei Federal n. 14.133/2021](#), pelo [Decreto Estadual n. 28.874/2024](#) e demais normas pertinentes, ao Termo de Referência, seus Anexos e o que mais constar nos autos do processo administrativo n.º [0028.020065/2024-49](#), mediante as seguintes cláusulas e condições a seguir estabelecidas:

1. **CLÁUSULA PRIMEIRA - DO OBJETO:**

1.1. A contratação de pessoa jurídica para a **Contratação de empresa para fornecimento de solução de proteção para estações de trabalho e servidores contra ataques cibernéticos**, do presente Termo de Referência encontra amparo legal nos seguintes dispositivos:

1.2. Art. 6, inciso XXIII e XLI, da [Lei nº 14.133, de 01 de abril de 2021](#), conforme descrito abaixo:

Art. 6º Para os fins desta Lei, consideram-se:

XXII - obras, serviços e fornecimentos de grande vulto: aqueles cujo valor estimado supera R\$ 200.000.000,00 (duzentos milhões de reais);

XLI - pregão: modalidade de licitação obrigatória para aquisição de bens e serviços comuns, cujo critério de julgamento poderá ser o de menor preço ou o de maior desconto;

1.3. Além disso, a presente contratação obedecerá aos ritos trazidos pelo art. 47, inciso XXI e art. 37 da Constituição Federal, bem como o disposto no Decreto Estadual nº 28.874 de 25 Janeiro de 2024 e Decreto 11.871 de 29 de Dezembro de 2023, que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública federal direta, autárquica e fundacional.

1.4. Neste contexto, o respectivo Termo de Referência leva em consideração as regras e diretrizes para a aquisição no âmbito da Administração Pública do Poder Executivo Estadual, utilizando-se, normas e decisões pertinentes à nova Lei.

1.5. O objeto desse Contrato é comum, nos termos do art. 6º, inciso XIII da [Lei nº 14.133, de 01 de abril de 2021](#), visto que o referido objeto detém especificações técnicas conhecidas e utilizadas no mercado, sem variações que possam causar a necessidade de análises específicas e detalhada.

1.6. Além disso, o presente objeto refuta qualquer descrição direcionada à marca, à modelo específico ou a qualquer característica suficiente para configurar restrição da competitividade licitatória, salvo nos casos em que for tecnicamente justificável, nos termos expressos do art. 41, inciso I, da [Lei nº 14.133, de 01 de abril de 2021](#).

## 2. CLÁUSULA SEGUNDA - DAS ESPECIFICAÇÕES TÉCNICAS E QUANTITATIVAS:

### 2.1. Especificações técnicas e quantitativas:

LOTE	ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	CÓDIGO CATSER
LOTE ÚNICO	01	Solução de proteção avançada contra ataques cibernéticos para estações de trabalho (Extended detection and response - XDR)	Licenças	800	24333
	02	Solução de proteção avançada contra ataques cibernéticos para servidores (Extended detection and response - XDR)	Licenças	300	24333
	03	Serviços de suporte pro ativo, corretivo e para resposta a incidentes	Meses	60	5398
	04	Serviço de treinamento	UND	03	5398

## 3. CLÁUSULA TERCEIRA - DESCRIÇÃO DA SOLUÇÃO

3.1. A solução de segurança a ser contratada abrange proteção de Endpoint e proteção contra ataques avançados para usuário final, com todos os serviços necessários para uma implementação completa e eficaz. Essa solução deverá atender às necessidades específicas da Secretaria de Estado do Desenvolvimento Ambiental durante um período de 36 meses. Os componentes que compõem essa solução são os seguintes:

### 3.2. SOLUÇÃO DE PROTEÇÃO AVANÇADA CONTRA ATAQUES CIBERNÉTICOS PARA ESTAÇÕES DE TRABALHO (EXTENDED DETECTION AND RESPONSE - XDR).(ITEM 1):

3.2.1. Visa oferecer uma camada de defesa endpoints da rede, ajudando a prevenir, detectar e responder a ataques de malware, ransomware, vírus e outras ameaças. As proteções para endpoint geralmente incluem firewalls, antivírus, antimalware, detecção de intrusão, controle de aplicativos, gerenciamento de patches e outras ferramentas de segurança. Elas são essenciais para garantir a segurança dos dispositivos e dos dados armazenados neles, especialmente em ambientes corporativos, onde a proteção dos endpoints é crucial para a segurança global da rede.

### 3.3. SOLUÇÃO DE PROTEÇÃO AVANÇADA CONTRA ATAQUES CIBERNÉTICOS PARA SERVIDORES (EXTENDED DETECTION AND RESPONSE - XDR).(ITEM 2):

3.3.1. A proteção para servidores em um ambiente corporativo é de extrema importância porque os servidores são peças fundamentais da infraestrutura de tecnologia da informação de uma empresa. Eles armazenam e processam dados críticos e sensíveis, além de hospedar aplicativos e serviços essenciais para o funcionamento do negócio.

### 3.4. SERVIÇO DE SUPORTE PRO ATIVO, CORRETIVO E PARA RESPOSTA A INCIDENTES (ITEM 3):

3.4.1. O serviço abrange suporte proativo, corretivo e resposta a incidentes, visando prevenir problemas, corrigir falhas e reagir rapidamente a eventos adversos para manter a estabilidade e segurança dos sistemas.

3.5. **SERVIÇO DE TREINAMENTO (ITEM 5):**

3.5.1. Esse serviço visa fornecer treinamento e transferência de conhecimento para os clientes. Ele oferece capacitação especializada, permitindo que os usuários adquiram habilidades e compreensão sobre o uso eficaz das soluções ou tecnologias implementadas, capacitando-os a gerenciar, operar e manter os sistemas.

4. **CLÁUSULA QUARTA - REQUISITOS DA CONTRATAÇÃO:**

4.1. **Solução de proteção avançada contra ataques cibernéticos para estações de trabalho (Extended detection and response – XDR) (ITEM 01):**

4.1.1. A solução deverá ser entregue na modalidade como um serviço (em nuvem);

4.1.2. Possuir console Web para gerenciamento e administração da ferramenta;

4.1.3. A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações e Controle de dispositivos em um único agente.

4.2. **Módulo de Proteção Anti-Malware:**

4.2.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

4.2.2. Windows 8.1 (x86/x64);

4.2.3. Windows 10 (x86/x64);

4.2.4. Windows 11 (x64).

4.2.5. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

4.2.6. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

4.2.7. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em: Processos em execução em memória principal (RAM);

4.2.8. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

4.2.9. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, MIME/uu, CAB;

4.2.10. Arquivos recebidos por meio de programas de comunicação instantânea (MSN messenger, yahoo messenger, google talk, icq, dentre outros).

4.2.11. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript, VBScript/ActiveX;

4.2.12. Deve possuir detecção heurística de vírus desconhecidos;

4.2.13. Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada; Deve permitir diferentes configurações de detecção (varredura ou rastreamento):

4.2.14. Em tempo real de arquivos acessados pelo usuário;

4.2.15. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

4.2.16. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

- 4.2.17. Automáticos do sistema com as seguintes opções:
- 4.2.18. Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;
- 4.2.19. Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);
- 4.2.20. Frequência: horária, diária, semanal e mensal;
- 4.2.21. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;
- 4.2.22. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;
- 4.2.23. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;
- 4.2.24. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;
- 4.2.25. Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;
- 4.2.26. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;
- 4.2.27. Deve possuir capacidade de escaneamento de arquivos compactados e, em caso de identificação de um arquivo malicioso, apenas este deve ser removido, mantendo os demais intactos
- 4.2.28. Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;
- 4.2.29. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;
- 4.2.30. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;
- 4.2.31. Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;
- 4.2.32. Deverá ter funcionalidade de Machine Learning em runtime para evitar possíveis métodos de obfuscação que o módulo de Machine Learning em pré-execução não consiga detectar;
- 4.2.33. Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;
- 4.2.34. Deve bloquear processos comuns associados a ransomware;
- 4.2.35. Em casos de ataques de ransomware, a solução deve ter a capacidade de interromper o processo de criptografia e restaurar os arquivos originais aos seus respectivos diretórios
- 4.2.36. Deve possuir funcionalidade de detecção de malwares conhecidos e desconhecidos por comportamento; Deve permitir a integração com solução de análise de artefatos suspeitos (sandbox) do próprio fabricante.

4.3. **Funcionalidade de Atualização:**

- 4.3.1. Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;



- 4.3.2. Deve permitir atualização incremental da lista de definições de vírus;
- 4.3.3. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;
- 4.3.4. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;
- 4.3.5. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;
- 4.3.6. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;
- 4.3.7. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

4.4. **Funcionalidade de Administração:**

- 4.4.1. Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;
- 4.4.2. Deve possibilitar instalação "silenciosa";
- 4.4.3. Deve permitir o bloqueio por nome de arquivo;
- 4.4.4. Deve permitir o travamento de pastas e diretórios;
- 4.4.5. Deve permitir o travamento de compartilhamentos;
- 4.4.6. Deve permitir o rastreamento e bloqueio de infecções;
- 4.4.7. Deve possuir mecanismo de detecção de ameaças baseado em comportamento de processos que estão sendo executados nas estações de trabalho e notebooks;
- 4.4.8. Deve desinstalar automática e remotamente a solução de antivírus atual, sem requerer outro software ou agente;
- 4.4.9. Deve permitir a desinstalação através da console de gerenciamento da solução;
- 4.4.10. Deve ter a possibilidade de exportar/importar configurações da solução através da console de gerenciamento;
- 4.4.11. Deve permitir a deleção dos arquivos quarentenados;
- 4.4.12. Deve permitir remoção automática de clientes inativos por determinado período;
- 4.4.13. Deve permitir integração com serviço de autenticação como Active Directory para acesso a console de administração;
- 4.4.14. Deve permitir criação de diversos perfis e usuários para acesso a console de administração;
- 4.4.15. Deve permitir que a solução utilize consulta externa a base de reputação de sites integrada e gerenciada através da solução de anti-malware, com opção de configuração para estações dentro e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;
- 4.4.16. Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante;
- 4.4.17. Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;
- 4.4.18. Deve possuir solução de reputação de sites local para sites já conhecidos como maliciosos integrada e gerenciada através da solução de antivírus, com opção de configuração para estações dentro

e fora da rede, cancelando a conexão de forma automática baseado na resposta à consulta da base do fabricante;

4.4.19. Deve registrar no sistema de monitoração de eventos da console de anti-malware informações relativas ao usuário logado no sistema operacional;

4.4.20. Deve prover ao administrador relatório de conformidade do status dos componentes, serviços, configurações das estações de trabalho e notebooks que fazem parte do escopo de gerenciamento da console de antivírus;

4.4.21. Deve prover criptografia para as comunicações entre o servidor e os agentes de proteção; Deve suportar múltiplas florestas e domínios confiáveis do Active Directory;

4.4.22. Deve utilizar de chave de criptografia que seja/esteja em conformidade com o Active Directory para realizar uma conexão segura entre servidor de antivírus e o controlador de domínio;

4.4.23. Deve permitir a criação de usuários locais de administração da console de anti-malware;

4.4.24. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de anti-malware;

4.4.25. Deve permitir criação de diversos perfis de usuários que permitam acessos diferenciados e customizados a diferentes partes da console de gerenciamento;

4.4.26. Deve se utilizar de mecanismo de autenticação da comunicação entre o servidor de administração e os agentes de proteção distribuídos nas estações de trabalho e notebooks;

4.4.27. Deve permitir a gerência de domínios separados para usuários previamente definidos;

4.4.28. Deve ser capaz de enviar notificações específicas aos respectivos administradores de cada domínio definido na console de administração;

4.4.29. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto.

#### 4.5. **Funcionalidade de Controle de Dispositivos:**

4.5.1. As configurações da funcionalidade de controle de dispositivos devem ser aplicadas por usuário;

4.5.2. Deve permitir políticas e ações diferentes para dispositivos conectados à rede interna e aqueles utilizados na rede externa (conectado à Internet, por exemplo);

4.5.3. Deve possuir controle de acesso a discos removíveis reconhecidos como dispositivos de armazenamento em massa através de interfaces USB e outras, com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura, e bloqueio total;

4.5.4. Deve possuir o controle de acesso a drives de mídias de armazenamento como CD-ROM, DVD, com as opções de acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

4.5.5. Deve ser capaz de identificar smartphones e tablets como destinos de cópias de arquivos e tomar ações de controle da transmissão;

4.5.6. Deve possuir o controle a drives mapeados com as seguintes opções: acesso total, leitura e escrita, leitura e execução, apenas leitura e bloqueio total;

4.5.7. Deve permitir escaneamento dos dispositivos removíveis e periféricos (USB, disquete, cdrom) mesmo com a política de bloqueio total ativa;

4.5.8. Para ação de restrição como o bloqueio, a solução deve permitir adicionais dispositivos USB autorizados, bem como apontar executáveis específicos como exceção ao bloqueio;

4.5.9. Deve ter a capacidade de bloquear a função de Autorun nos dispositivos;

4.5.10. Deve permitir controle de permissão ou bloqueio para dispositivos que não armazenam dados tendo, pelo menos, os seguintes tipos de dispositivos: adaptadores bluetooth, dispositivos de

imagem, modems, interfaces wireless externas, cartões PCMCIA, dispositivos infravermelhos e portas COM/LPT.

4.6. **Módulo de Proteção Anti-Malware para estações MacOS:**

- 4.6.1. O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais:
- 4.6.2. macOS 12 (Monterey);
- 4.6.3. macOS 11 (Big Sur) macOS 10.15 (Catalina);
- 4.6.4. macOS 10.14 (Mojave); macOS 10.13 (High Sierra);
- 4.6.5. Suporte ao Apple Remote Desktop para instalação remota da solução;
- 4.6.6. Gerenciamento integrado à console de gerência central da solução;
- 4.6.7. Proteção em tempo real contra vírus, trojans, worms, cavalos-de-troia, spyware, adwares e outros tipos de códigos maliciosos;
- 4.6.8. Permitir a verificação das ameaças da maneira manual e agendada;
- 4.6.9. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus; Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infecções a arquivos;
- 4.6.10. Deve possuir mecanismo de proteção contra uso não autorizado no qual o agente do antivírus deve ser protegido contra mudança do seu estado (não possibilitar que um administrador da estação de trabalho e notebook possa parar o serviço do antivírus) bem como mecanismo para restaurar seu estado normal;
- 4.6.11. Deve possuir no mecanismo de autoproteção as seguintes proteções:
- 4.6.12. Proteção e verificação dos arquivos de assinatura;
- 4.6.13. Proteção dos processos do agente de segurança;
- 4.6.14. Proteção das chaves de registro do agente de segurança;
- 4.6.15. Proteção do diretório de instalação do agente de segurança.

4.7. **Funcionalidade de HIPS – Host IPS e Host Firewall:**

- 4.7.1. Deve ser capaz de realizar a detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais:
- 4.7.2. Windows 8.1 (x86/x64);
- 4.7.3. Windows 10 (x86/x64);
- 4.7.4. Windows 11 (x64).
- 4.7.5. Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;
- 4.7.6. As regras de vulnerabilidades deverão possuir a opção de desativar a regra de forma individual;
- 4.7.7. Todas as regras das funcionalidades de firewall e IPS de host devem permitir apenas detecção (log) ou prevenção (bloqueio);
- 4.7.8. Deve permitir ativar e desativar o produto sem a necessidade de remoção;
- 4.7.9. Deve permitir que o usuário altere as configurações de níveis de segurança e exceções;
- 4.7.10. Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo;
- 4.7.11. O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança; O modulo de HIPS deverá possuir regras pra proteger contra ameaças do tipo Ransomware;

4.7.12. O modulo de HIPS deverá conter regras contra exploit, vulnerabilidades e genericas protegendo contra ameaças conhecidas ou desconhecidas;

4.7.13. O módulo de HIPS deverá permitir que o administrador monitore apenas ou realize o bloqueio das tentativas de exploração de vulnerabilidades;

4.7.14. Deve suportar configuração de parâmetros de pacotes como quantidade máxima de conexões TCP e timeout para pacotes UDP;

4.7.15. Deve ter a capacidade de proteção contra exploração de vulnerabilidades do sistema operacional e de aplicações terceiras instaladas na estação de trabalho;

4.7.16. A lista de regras deve permitir que o administrador realize buscas e tenha rápida visibilidade do tipo da aplicação, em que modo a regra encontra-se (bloqueio ou monitoramento), CVE, CVSS score, quando aplicável.

#### 4.8. **Módulo para Controle De Aplicações:**

4.8.1. Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais:

4.8.2. Windows 8.1 (x86/x64);

4.8.3. Windows 10 (x64);

4.8.4. Windows 11 (x64).

4.8.5. As regras de controle de aplicação devem permitir as seguintes ações:

4.8.6. Permissão de execução;

4.8.7. Bloqueio de execução;

4.8.8. Bloqueio de novas instalações.

4.8.9. A regra de liberação para o controle de aplicação deverá permitir que o programa liberado efetue ou não a execução de outros processos,

4.8.10. As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra;

4.8.11. As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações:

4.8.12. Assinatura SHA-1 e SHA-256 do executável;

4.8.13. Atributos do certificado utilizado para assinatura digital do executável;

4.8.14. Caminho lógico do executável;

4.8.15. Base de assinaturas de cortiçados digitais válidos e seguros.

4.8.16. As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;

4.8.17. As políticas de segurança devem permitir a utilização de múltiplas regras de controle de aplicações;

4.8.18. O módulo de controle de aplicativos deve possuir uma lista de aplicações mal-intencionados para bloqueio e monitoramento tendo, pelo menos, as categorias de KeyLoggers, anonimizadores de proxy, P2P, crackers de senhas;

4.8.19. Deve permitir a busca por aplicações ou fabricante destas;

4.8.20. Deve possuir ferramenta para extrair o hash de um ou um grupo de executáveis, permitindo a importação destes hashes através de arquivo CSV.

#### 4.9. **Módulo de Detecção e Resposta:**

4.9.1. A solução deve ser compatível com os sistemas operacionais Windows, Linux e MacOS;

- 4.9.2. O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK®, identificando técnicas e táticas dos ataques;
- 4.9.3. A solução deve possuir módulo de investigação e detecção integrados;
- 4.9.4. Deve fazer uso de inteligência artificial e inteligência de ameaças do fabricante da solução para analisar e correlacionar as atividades dos sensores do ambiente;
- 4.9.5. Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho;
- 4.9.6. Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;
- 4.9.7. Apresentar os alertas consolidados e correlacionados de ameaças para melhor investigação e resposta;
- 4.9.8. Fornece a capacidade de realizar buscas avançadas para localizar dados ou objetos no ambiente para análise avançada de atividades ou detecções;
- 4.9.9. Capacidade de construir sequências de buscas poderosas para localizar os dados ou objetos em seu ambiente que você deseja examinar;
- 4.9.10. Deve prover diferentes métodos de pesquisa, filtros e uma linguagem de consulta do tipo Kibana para identificar, categorizar e recuperar os resultados da pesquisa;
- 4.9.11. Deve ser possível realizar buscas através de strings parciais, exatas, valores nulos, wildcards e caracteres especiais;
- 4.9.12. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;
- 4.9.13. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;
- 4.9.14. Deve permitir que as detecções sejam correlacionadas com módulos de servidores, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;
- 4.9.15. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;
- 4.9.16. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;
- 4.9.17. O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos; Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;
- 4.9.18. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;
- 4.9.19. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;
- 4.9.20. Permitir investigar os alertas gerados pelos modelos de detecção por meio de uma análise impacto e análise de causa-raiz;
- 4.9.21. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento;
- 4.9.22. Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade;
- 4.9.23. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;
- 4.9.24. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;



- 4.9.25. Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta;
- 4.9.26. Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;
- 4.9.27. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;
- 4.9.28. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada estação de trabalho;
- 4.9.29. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;
- 4.9.30. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;
- 4.9.31. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);
- 4.9.32. Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas;
- 4.9.33. Deve informar qual o escopo de impacto ou dimensionar o impacto em servidores, estações de trabalho e usuários, indicando a quantidade de componentes afetados no ataque;
- 4.9.34. Deve permitir que o analista possa alterar o status dos incidentes de acordo com seu tratamento e indicar falsos positivos para a plataforma;
- 4.9.35. Deve permitir adicionar arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores; Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores; Deve permitir terminar processos ativos executados nas estações de trabalhos e servidores; Permitir coletar e fazer o download de um arquivo para investigação local detalhada;
- 4.9.36. Isolar a estação de trabalho desconectando-a da rede e permitindo se comunicar exclusivamente com a
- 4.9.37. console de gerenciamento do fabricante;
- 4.9.38. Restaurar a conectividade da estação de trabalho com a rede;
- 4.9.39. Iniciar uma sessão de shell remoto na estação de trabalho selecionada para execução de comandos remotos para investigação;
- 4.9.40. Deve ser possível fazer o download do histórico da sessão após finalizar a sessão remota do shell na estação de trabalho para fins de auditoria.

4.10. **SOLUÇÃO DE PROTEÇÃO AVANÇADA CONTRA ATAQUES CIBERNÉTICOS PARA SERVIDORES (EXTENDED DETECTION AND RESPONSE - XDR)\_(ITEM 2):**

4.11. **SOLUÇÃO DE SEGURANÇA PARA CARGAS DE TRABALHO HÍBRIDAS COM DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO:**

4.12. **Características Gerais Da Solução:**

- 4.12.1. A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais:
- 4.12.2. Windows Server 2000;
- 4.12.3. Windows Server 2003 SP1 e 2003 R2 SP2; Windows Server 2008 e 2008 R2;
- 4.12.4. Windows Server 2012 e 2012 R2;
- 4.12.5. Windows Server 2016;
- 4.12.6. Windows Server 2019;
- 4.12.7. Windows Server 2022;

- 4.12.8. Red Hat Enterprise 5, 6, 7 e 8;
- 4.12.9. CentOS 5, 6, 7 e 8;
- 4.12.10. AIX 6.1, 7.1 e 7.2;
- 4.12.11. Oracle Linux 5, 6, 7 e 8;
- 4.12.12. SUSE Linux Enterprise Server 10, 11, 12 e 15;
- 4.12.13. Ubuntu 10, 12, 14, 16, 18 e 20;
- 4.12.14. Debian 6, 7, 8, 9 e 10;
- 4.12.15. Rocky Linux 8;
- 4.12.16. AlmaLinux 8;
- 4.12.17. Cloud Linux 5, 6, 7 e 8; Solaris 10 1/13 Sparc; Solaris 10 1/13 (x86/x64); Solaris 11.2/ 11.3 Sparc; Solaris 11.2/ 11.3 (x86/x64);
- 4.12.18. Solaris 11.4 (x86, x64 ou SPARC) Amazon Linux e Amazon Linux 2 (x64).
- 4.12.19. A solução deverá ser totalmente compatível e homologada com o ambiente Vmware;
- 4.12.20. A console de gerenciamento deverá ser em nuvem, permitindo o gerenciamento das políticas de segurança através da Internet;
- 4.12.21. A solução deverá ser gerenciada por console Web, compatível com pelo menos os browsers Internet Explorer, Google Chrome e Firefox. Deve ainda suportar certificado digital para gerenciamento;
- 4.12.22. A solução deverá permitir a integração com pelo menos as seguintes plataformas de nuvem: Vmware vCloud, MS Azure e AWS;
- 4.12.23. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;
- 4.12.24. A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;
- 4.12.25. A console de administração deverá permitir o envio de notificações via SMTP;
- 4.12.26. Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;
- 4.12.27. A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas;
- 4.12.28. A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;
- 4.12.29. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;
- 4.12.30. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob- demanda, ou agendado com o envio automático do relatório via e-mail;
- 4.12.31. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;
- 4.12.32. A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;
- 4.12.33. A solução deverá prover relatórios contendo no mínimo as seguintes informações; malware, regras de IPS aplicadas e Firewall;

- 4.12.34. Em caso de solução e nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade; A solução de segurança ter a capacidade de identificar ataques entre containeres;
- 4.12.35. Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";
- 4.12.36. Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar novas políticas de segurança;
- 4.12.37. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;
- 4.12.38. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;
- 4.12.39. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;
- 4.12.40. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;
- 4.12.41. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;
- 4.12.42. Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;
- 4.12.43. Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;
- 4.12.44. Para servidores Linux, a solução deverá possibilitar a atualização automática da versão quando o agente reiniciar;
- 4.12.45. Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;
- 4.12.46. Deve permitir a remoção automática de agentes inativos, definindo o período para, pelo menos 1 semana, 1 mês e 12 meses;
- 4.12.47. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;
- 4.12.48. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;
- 4.12.49. A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação; A solução deverá mostrar quais máquinas estão usando determinada política;
- 4.12.50. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;
- 4.12.51. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;
- 4.12.52. A solução deverá permitir a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;
- 4.12.53. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;
- 4.12.54. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;
- 4.12.55. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;

- 4.12.56. A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;
- 4.12.57. A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;
- 4.12.58. A solução deverá ter a capacidade de se integrar com o Amazon SNS e os principais softwares de SIEMs contemplando, no mínimo: Splunk, IBMQradar e HP ArcSight de modo a permitir enviar os seus logs para essas soluções;
- 4.12.59. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;
- 4.12.60. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;
- 4.12.61. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;
- 4.12.62. As atualizações de assinaturas deverão ocorrer de forma agendada e automática possibilitando ser até mesmo de hora em hora;
- 4.12.63. Após a atualização deve ser informado o que foi modificado ou adicionado;
- 4.12.64. Deve ser possível baixar as assinaturas na console de gerenciamento, mas não as distribuir aos clientes;
- 4.12.65. A console de gerenciamento deve apresentar a capacidade de gerar roll back de suas atualizações de regras;
- 4.12.66. A solução deverá ter capacidade de gerar pacote de autodiagnóstico de modo a coletar arquivos relevantes para envio ao suporte do produto;
- 4.12.67. Deverá ter a capacidade de colocar etiquetas para a ocorrência de determinados eventos de modo a facilitar o gerenciamento, relatórios e visualização;
- 4.12.68. No gerenciamento de licenças, deve ser informada quantidade contratada e quantidade em utilização de clientes;
- 4.12.69. Solução deverá ter mecanismo de procura em sua console de gerenciamento de modo que seja facilitada a busca de regras;
- 4.12.70. Deverá possuir a capacidade de classificar eventos para que facilite a identificação e a visualização de eventos críticos em servidores críticos;
- 4.12.71. Deverá possibilitar colocar etiquetas em eventos para que se possam visualizar apenas os eventos desejados;
- 4.12.72. O fabricante deverá participar do programa "Microsoft Application Protection Program" para obtenção de informações de modo a permitir a criação de regras de proteção antes mesmo dos patches serem publicados pelo fabricante;
- 4.12.73. A console de gerenciamento deve se integrar com o Vmware vCloud, de modo a importar e sincronizar os objetos (hosts vmware e guests vm) para a console de gerenciamento da solução;
- 4.12.74. O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos; A solução deve possuir API documentada para integração na esteira de automação;
- 4.12.75. A documentação da API deve conter exemplos prontos para implementação de determinadas funcionalidades, como cookbooks;
- 4.12.76. Precisa ter a capacidade de detectar e aplicar as regras necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e sem a intervenção do administrador;
- 4.12.77. A solução deve permitir desabilitar os módulos individualmente;
- 4.12.78. Precisa ter a capacidade de desabilitar as regras não mais necessárias dos módulos de IDS/IPS, Monitoramento de Integridade e Inspeção de Logs, para cada servidor, de forma automática e

sem a intervenção do administrador.

#### 4.13. **Antimalware:**

4.13.1. A solução deve permitir a proteção contra códigos maliciosos através da instalação de agentes, permitindo rastrear ameaças em tempo real, varredura sob demanda e conforme agendamento, possibilitando a tomada de ações distintas para cada tipo de ameaça;

4.13.2. A solução deve possibilitar a criação de listas de exclusão, para que o processo do antivírus não execute a varredura de determinados diretórios ou arquivos do SO;

4.13.3. A solução deve possuir listas de exclusão separadas por módulo da proteção antimalware como exclusão das detecções por comportamento, exclusão por machine learning e exclusão por assinatura;

4.13.4. Em plataforma Windows, a solução deve permitir criar exclusões de escaneamento a partir do certificado digital das aplicações;

4.13.5. A solução deve possibilitar a verificação de ameaças dentro de arquivos compactados, efetuando a limpeza apenas de arquivos maliciosos em casos de detecção. A limpeza deve ocorrer sem a descompactação do arquivo;

4.13.6. Em servidores Windows, deve identificar e bloquear ameaças através de métodos de Machine Learning, quarentenando arquivos identificados;

4.13.7. A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas;

4.13.8. A solução deverá oferecer escanear processos em memória em busca de Malware;

4.13.9. O scan de arquivos comprimidos deverá ser de no mínimo 6 camadas de compressão;

4.13.10. O scan de arquivos comprimidos do tipo OLE deverá ser de no mínimo 20 camadas de compressão;

4.13.11. Para servidores Windows, a solução deverá permitir que o escaneamento agendado ocorra, ainda que o agente esteja offline na console de gerenciamento;

4.13.12. A solução deverá possuir ações pré-configuradas para cada tipo de ameaça detectada ou tomar uma ação baseada na configuração padrão da ferramenta;

4.13.13. Em servidores Windows, a solução deverá integrar-se com interface AMSI (Antimalware Scan Interface);

4.13.14. A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado; Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware; Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;

4.13.15. Deve possibilitar o controle do consumo de memória durante as varreduras a fim de minimizar os impactos de desempenho no servidor;

4.13.16. A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs; Em servidores Windows, deve possuir capacidade de detectar ameaças por comportamento;

4.13.17. Deverá ter a possibilidade de escanear drivers de rede mapeados nos servidores.

#### 4.14. **Proteção Contra URLs Maliciosas:**

4.14.1. Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;

4.14.2. A lista de URLs deve ser fornecida e atualizada automaticamente pelo fabricante, permitindo a consulta em uma base local ou na nuvem da reputação das URLs acessadas;

4.14.3. A solução deve permitir alterar o nível de sensibilidade para detecção de URLs maliciosas tendo, pelo menos, os níveis Alto, médio e baixo;



- 4.14.4. Deve permitir a criação de listas de exclusão, permitindo que usuários acessem determinadas URLs especificadas pelo administrador do sistema;
- 4.14.5. Deve permitir configurar notificações personalizadas para detecções desse módulo, deixando a cargo do administrador exibir ou não tais notificações;
- 4.14.6. Deverá ter capacidade de identificar acessos a URLs maliciosas além das portas padrão 80 e 443;
- 4.14.7. A solução deve permitir que o administrador reclassifique uma URL através do site do fabricante para evitar falsos positivos;
- 4.14.8. A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança.
- 4.14.9. Firewall.
- 4.14.10. Operar como firewall de host, através da instalação de agente nos servidores protegidos;
- 4.14.11. Precisa ter a capacidade de controlar o tráfego baseado no Endereço MAC, Frame types, Tipos de Protocolos, Endereços IP e intervalo de portas;
- 4.14.12. Precisa ter a capacidade de controlar conexões TCP baseado nas Flags TCP; Precisa ter a capacidade de definir regras distintas para interfaces de rede distintas;
- 4.14.13. A solução deverá ser capaz de reconhecer e possibilitar o bloqueio endereços IP que estejam realizando Network Scan, Port Scan, TCP Null Scan, TCP FYN SYN Scan, TCP Xmas Scan e Computer OS Fingerprint por até 30 minutos;
- 4.14.14. Precisa ter a capacidade de implementação de regras em determinados horários que podem ser customizados pelo administrador;
- 4.14.15. Precisa ter a capacidade de definição de regras para contextos específicos;
- 4.14.16. Para facilitar a criação e administração de regras de firewall, as mesmas poderão se apoiar em objetos que podem ser lista de ips, lista de MACs, lista de portas;
- 4.14.17. Regras de firewall poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo, se está no domínio ou não);
- 4.14.18. Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana; O firewall deverá ser stateful bidirecional;
- 4.14.19. O firewall deverá permitir liberar ou apenas logar eventos;
- 4.14.20. O firewall deverá ser passível de criação de regras através do protocolo, origem do tráfego, frame type, TCP header flags, destino e direção;
- 4.14.21. As regras de Firewall deverão ter as seguintes ações, ou equivalentes: Allow, log only, bypass, force allow, deny;
- 4.14.22. A solução, para facilidade de administração, deverá utilizar o conceito de regras implícitas para a regra ALLOW, negando o tráfego para todo o restante que não estiver liberado;
- 4.14.23. As ações também deverão ser possíveis de terem prioridades diferentes, sendo que a prioridade maior prevalece sobre a prioridade menor;
- 4.14.24. Deverá realizar pseudo stateful em tráfego UDP; Deverá logar a atividade stateful;
- 4.14.25. Deverá permitir limitar o número de conexões entrantes e o número de conexões de saída de um determinado computador;
- 4.14.26. Deverá permitir limitar o número de meias conexões vindas de um computador; Deverá prevenir ack storm;
- 4.14.27. Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;

4.14.28. Deverá identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um período de tempo configurado pelo administrador;

4.14.29. Deverá permitir criar lista de exceções para identificar os Ips autorizados a realizar varreduras de portas ou da rede;

4.14.30. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.

4.15. **Proteção De Vulnerabilidades de SO e Aplicações:**

4.15.1. Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

4.15.2. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;

4.15.3. A solução deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;

4.15.4. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;

4.15.5. Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;

4.15.6. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

4.15.7. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;

4.15.8. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;

4.15.9. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para

4.15.10. fins de investigação do incidente;

4.15.11. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;

4.15.12. Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;

4.15.13. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);

4.15.14. Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana; Deverá ser capaz de inspecionar tráfego criptografado de entrada;

4.15.15. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;

4.15.16. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

- 4.15.17. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;
- 4.15.18. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;
- 4.15.19. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;
- 4.15.20. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;
- 4.15.21. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;
- 4.15.22. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;
- 4.15.23. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs; As regras de IPS poderão ter sua capacidade de LOG desabilitado;
- 4.15.24. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta; As regras devem ser atualizadas automaticamente pelo fabricante;
- 4.15.25. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas.
- 4.16. **Monitoramento De Integridade:**
- 4.16.1. A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;
- 4.16.2. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;
- 4.16.3. Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux; Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional; Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;
- 4.16.4. Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;
- 4.16.5. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de monitoramento de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;
- 4.16.6. O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;
- 4.16.7. Deverá alertar toda vez que uma modificação ocorrer em tempo real para ambiente Windows e pseudo real-time para ambiente Linux;
- 4.16.8. Deverá logar e colocar em relatório todas as modificações que ocorram;
- 4.16.9. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;
- 4.16.10. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;
- 4.16.11. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;
- 4.16.12. Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente.
- 4.17. **Inspeção De Logs:**

- 4.17.1. A solução deverá permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX;
- 4.17.2. Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;
- 4.17.3. Precisa ter a capacidade de varrer o sistema operacional e aplicações, recomendando e aplicando automaticamente regras de inspeção de logs de acordo com o resultado desta varredura. Esta varredura deverá poder ser executada sob demanda ou agendada;
- 4.17.4. Precisa permitir a criação de regras de inspeção de logs adicionais para auditoria de logs de aplicações terceiras;
- 4.17.5. Precisa permitir a customização de regras existentes, adicionando, removendo ou modificando regras de inspeção de logs;
- 4.17.6. Deverá rastrear e indicar/sugerir ao administrador do sistema quais softwares estão instalados e que possuem logs passíveis de inspeção;
- 4.17.7. Deverá possibilitar a criação de regras de inspeção de logs para aplicações customizadas;
- 4.17.8. Deverá ter inteligência para que a cada violação relevante no log inspecionado que possa comprometer a segurança do ambiente ou do servidor seja alertada;
- 4.17.9. Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita no servidor seja alertada;
- 4.17.10. Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram; As regras poderão ser modificadas por severidade de ocorrência de eventos;
- 4.17.11. As regras devem se atualizar automaticamente pelo fabricante;
- 4.17.12. Permitir modificação pelo administrador em regras para adequação ao ambiente.
- 4.18. **Controle De Aplicações:**
- 4.18.1. A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;
- 4.18.2. O controle de aplicações deverá ser realizado através de Hash, suportando no mínimo MD5, SHA1 e SHA256;
- 4.18.3. O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina; A console deverá exibir eventos de no mínimo 30 dias;
- 4.18.4. A solução deverá possuir um mecanismo ao qual permita a execução de aplicações e scripts automaticamente, sem intervenção manual, por um determinado período que deve ser no máximo 10 horas;
- 4.18.5. A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente.
- 4.19. **Deteção e Resposta:**
- 4.19.1. A solução deve ser compatível com Linux e Windows Server 2008 R2 e superiores; A solução deve possuir módulo de investigação, detecção integrados.
- 4.19.2. Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;
- 4.19.3. A console de correlação deve estar disponível na nuvem do próprio fabricante, o qual deve ser responsável pelas manutenções, atualizações e disponibilidade;
- 4.19.4. Deve possuir capacidade de encaminhar as atividades suspeitas identificadas nos servidores para a console de correlação centralizada;

- 4.19.5. O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos; Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;
- 4.19.6. A console de correlação centralizada deve possuir informações a respeito dos principais ataques que estão ocorrendo no mundo, quais plataformas e países são afetados, além de links para obter mais informações;
- 4.19.7. A solução deve permitir realizar buscas em todos os dados de atividades enviadas pelos servidores e demais sensores que estejam conectados na console, ainda que estas não sejam detectadas como maliciosas;
- 4.19.8. A console deve permitir o Single Sign-On através de SAML ou padrão equivalente;
- 4.19.9. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;
- 4.19.10. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;
- 4.19.11. Deve permitir o envio de notificações para os administradores através de email, API e integrações com SIEMs;
- 4.19.12. Deve prover visualização em linha do tempo com informações dos eventos monitorados em cada servidor;
- 4.19.13. Deve permitir a visualização entre usuários, servidores, processos/comandos, arquivos e demais componentes correlacionados em determinado ataque;
- 4.19.14. Deverá informar com qual técnica e tática do MITRE ATT&CK framework o ataque está relacionado, além de possuir link direto para o site da organização;
- 4.19.15. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos, usuários, servidores);  
Ao clicar em quaisquer dos objetos, a solução deve permitir realizar buscar específicas pelo objeto ou ainda executar ações como executar investigações mais aprofundadas.

4.20. **SERVIÇO DE SUPORTE PRO ATIVO, CORRETIVO E PARA RESPOSTA A INCIDENTES (ITEM 3):**

- 4.20.1. O serviço de suporte proativo, corretivo e para resposta a incidentes compreende um conjunto abrangente de atividades destinadas a assegurar o pleno funcionamento e a continuidade operacional de sistemas, soluções ou serviços. Este serviço é estrategicamente desenhado para atender às demandas dinâmicas do ambiente tecnológico, oferecendo suporte preventivo, corretivo e uma resposta ágil a incidentes de segurança.
- 4.20.2. Todo o Serviço de Suporte deverá ser prestado por profissional certificado pelo Fabricante da Solução, em nível compatível com a prestação do serviço. Deverá ser apresentada comprovação da certificação dos profissionais responsáveis no ato da assinatura do contrato.
- 4.20.3. Deverá disponibilizar um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução ofertada;
- 4.20.4. deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução.

4.21. **Suporte Proativo:**

- 4.21.1. O suporte proativo deverá antecipar potenciais problemas, identificando e resolvendo questões antes mesmo que impactem o desempenho e a segurança do ambiente;
- 4.21.2. A contratada deverá notificar a contratante sobre atualizações de segurança, patches e correções assim que estiverem disponíveis, caso autorizado aplicar as atualizações de segurança e evolutiva dos produtos;
- 4.21.3. Deverá realizar análises preditivas, buscando otimizar a performance e prevenir falhas nos produtos, além de detectar padrões que possam indicar uma possível violação de segurança, proporcionando um ambiente mais estável e seguro;



4.21.4. Deverá realizar avaliações regulares de riscos para identificar possíveis vulnerabilidades e pontos fracos nos sistemas e, implementar medidas corretivas com base nos resultados das avaliações de riscos;

4.21.5. Realizar auditorias regulares para garantir que as melhores práticas e os controles de segurança estejam operacionais e, utilizar resultados de auditorias para implementar melhorias contínuas;

4.21.6. A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução do problema.

4.22. **Suporte Corretivo:**

4.22.1. Este componente concentra-se na solução de problemas ou incidentes. O suporte corretivo atua de forma ágil para restabelecer a funcionalidade normal do sistema, minimizando impactos negativos e mantendo a continuidade operacional;

4.22.2. Serviço Especializado de Suportes corretivo para xx(xxxx) meses. Serviço de Suporte especializado para ajustes, correções e configurações da solução a ser fornecida. Neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução;

4.22.3. A contratada deverá:

- a) Implementar um sistema de abertura de chamados, para registrar, rastrear e priorizar incidentes e requisições de suporte;
- b) Atribuir números de caso exclusivos para facilitar a comunicação e o acompanhamento;
- c) Garantir disponibilidade 24/7 para responder a incidentes críticos.

4.22.4. Deverá apresentar relatório contendo as ações adotadas para a solução do problema.

4.23. **Resposta a Incidentes:**

4.23.1. O serviço de resposta a incidentes deverá lidar com eventos imprevistos, como violações de segurança, falhas críticas ou interrupções inesperadas. deverá ser realizada por profissionais especializados e certificados pelo fabricante;

4.23.2. Deverá realizar investigações para determinar a natureza, origem e impacto de incidentes de segurança;

4.23.3. Desenvolver planos de mitigação e estratégia de recuperação para minimizar o impacto de incidentes;

4.23.4. Elaborar relatórios detalhados sobre os incidentes, incluindo ações tomadas e recomendações de melhorias.

4.24. **SERVIÇO DE IMPLANTAÇÃO:**

4.24.1. Nesta etapa, compreende-se a instalação e configuração da solução contratada, contados a partir da emissão da Ordem de Serviço (OS);

4.24.2. O serviço de implantação abrange integralmente as fases essenciais para a integração, instalação e configuração da solução contratada, alinhando-se precisamente com as especificações técnicas e requisitos predefinidos. Esta abordagem abarca desde o planejamento inicial até a conclusão efetiva, assegurando uma transição suave dos processos existentes para a nova solução;

4.24.3. O Plano de Implantação assume a forma de um documento fundamental que consolida a estratégia para instalação, configuração e entrega da solução contratada. Sua importância reside em orientar e alinhar as atividades, garantindo eficiência e uma implementação adequada da solução conforme os requisitos estabelecidos;

4.24.4. O documento deverá conter no mínimo os requisitos de ambiente tecnológicos necessários para a instalação das licenças, cronograma e detalhamento das atividades a serem realizadas, topologia do ambiente pós instalação da solução, matriz de responsabilidade, plano de comunicação;

4.24.5. Durante esta etapa, a equipe da Contratada deverá estar presente nos horários de instalação definidos pelo Contratante. As atividades de instalação e configuração poderão ser realizadas, conforme necessário, em horário comercial, período noturno ou final de semana;

4.24.6. O Contratante disponibilizará a infraestrutura de hardware e software necessária e já existente em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução durante esta etapa.

4.25. **Serviço de capacitação e repasse de conhecimento (Item 12):**

4.25.1. Repasse de conhecimento, na forma de treinamento para técnicos, de forma virtual, para 1 (uma) turma, com carga horária mínima de 40 (quarenta) horas, abrangendo todos os softwares integrantes da suíte de solução de segurança;

4.25.2. O conteúdo programático abordará tanto aspectos teóricos quanto práticos, contemplando de maneira abrangente todos os módulos relevantes da solução de segurança;

4.25.3. O treinamento pode ser segmentado de acordo com o produto a ser instalado no ambiente tecnológico, contemplando, no mínimo, os seguintes módulos:

4.25.4. Instalação do módulo de gerenciamento central;

4.25.5. Instalação do software de Endpoint Protection em estações de trabalho e servidores;

4.25.6. Descrição e configuração de todas as funcionalidades contratadas da solução;

4.25.7. Melhores práticas utilizadas no mercado para otimização dos softwares e suas funcionalidades.

4.25.8. A carga horária mínima estabelecida será de 40 (quarenta) horas, divididas em expedientes de 4 horas por dia, no horário comercial. A contratada é responsável por fornecer apostilas em formato digital que contemplem o conteúdo referente ao produto, oferecendo suporte ao aprendizado prático e teórico dos participantes;

4.25.9. Este treinamento visa capacitar adequadamente os usuários finais, garantindo que compreendam e aproveitem plenamente as funcionalidades da solução de segurança. O enfoque prático e teórico, aliado às melhores práticas do mercado, promove uma formação abrangente e eficaz.

4.26. **SERVIÇO DE TREINAMENTO (ITEM 4):**

4.26.1. Repasse de conhecimento, na forma de treinamento para técnicos, de forma virtual, para 1 (uma) turma, com carga horária mínima de 40 (quarenta) horas, abrangendo todos os softwares integrantes da suíte de solução de segurança;

4.26.2. O conteúdo programático abordará tanto aspectos teóricos quanto práticos, contemplando de maneira abrangente todos os módulos relevantes da solução de segurança;

4.26.3. O treinamento pode ser segmentado de acordo com o produto a ser instalado no ambiente tecnológico, contemplando, no mínimo, os seguintes módulos:

4.26.4. Instalação do módulo de gerenciamento central;

4.26.5. Instalação do software de Endpoint Protection em estações de trabalho e servidores;

4.26.6. Descrição e configuração de todas as funcionalidades contratadas da solução;

4.26.7. Melhores práticas utilizadas no mercado para otimização dos softwares e suas funcionalidades.

4.26.8. A carga horária mínima estabelecida será de 40 (quarenta) horas, divididas em expedientes de 4 horas por dia, no horário comercial. A contratada é responsável por fornecer apostilas em formato digital que contemplem o conteúdo referente ao produto, oferecendo suporte ao aprendizado prático e teórico dos participantes;

4.26.9. Este treinamento visa capacitar adequadamente os usuários finais, garantindo que compreendam e aproveitem plenamente as funcionalidades da solução de segurança. O enfoque prático e teórico, aliado às melhores práticas do mercado, promove uma formação abrangente e eficaz.

**4.27. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC:****4.28. Requisitos de Capacitação**

4.28.1. A empresa CONTRATADA deverá realizar o repasse de conhecimento aos funcionários da CONTRATANTE que atuarão, diretamente, com a solução de segurança adquirida, contemplando instalação, parametrização, monitoramento, melhores práticas e atuação de incidentes com carga horária mínima de 40 (quarenta) horas ministrado por profissional certificado pelo fabricante.

4.28.2. O treinamento será demandado à CONTRATADA pela CONTRATANTE após a efetiva implementação e estruturação da solução de segurança em seu parque tecnológico, quando acordarão cronograma para realização do treinamento.

4.28.3. O treinamento deverá ser realizado na modalidade presencial nas dependências da CONTRATANTE a participantes da equipe técnica a serem definidos pela CONTRATANTE.

4.28.4. Os horários do curso deverão seguir a conveniência do CONTRATANTE, podendo sua realização ocorrer apenas em um dos períodos do dia (manhã ou tarde).

4.28.5. Deverá ser fornecido material didático completo e com conteúdo oficial do fabricante em língua portuguesa. Caso seja utilizado material elaborado exclusivamente pelo fabricante e fique demonstrado que este não é oferecido em língua portuguesa, será aceito o fornecimento em língua inglesa.

4.28.6. O treinamento deve conter parte teórica e prática, incluindo tópicos sobre a instalação, uso, configuração, resolução de problemas da solução, análise de relatórios, respostas a incidentes e outros.

4.28.7. As datas do treinamento devem ser previamente combinadas com o CONTRATANTE.

4.28.8. Todos os custos relativos à realização do treinamento são de exclusiva responsabilidade da CONTRATADA.

**4.29. REQUISITOS E FUNCIONALIDADES TÉCNICOS DA SOLUÇÃO:**

4.29.1. A especificação técnica mínima e obrigatória da solução encontra-se detalhada no Anexo I deste estudo.

**4.30. Requisitos de manutenção e garantia:**

4.30.1. A empresa contratada é responsável por fornecer suporte técnico e garantia de atualização da solução pelo período de 36 meses, a contar da data de emissão do Termo de Recebimento. É importante ressaltar que essa garantia não se limita ao término da vigência contratual.

4.30.2. A garantia deve incluir obrigatoriamente:

a) Atualização das versões dos softwares fornecidos, caso sejam disponibilizadas novas versões.

b) Atualização dos softwares fornecidos caso haja lançamento de novos softwares que substituam os fornecidos ou se ficar evidente a descontinuidade dos softwares fornecidos, mesmo que não se trate de substituição direta.

c) Correções dos softwares fornecidos, incluindo a aplicação de patches para corrigir eventuais falhas (bugs) de software que possam prejudicar o ambiente de produção ou vulnerabilidades que comprometam a segurança da solução.

4.30.3. A garantia deverá ser prestada durante todo o período de contrato e aditivos relacionados à atualização das licenças e proteção.

4.30.4. Durante o período de garantia, a empresa contratada compromete-se a substituir, em até 15 dias úteis, os equipamentos que apresentarem, em um período de 60 dias, duas ocorrências de defeitos por inoperância do produto ou 3 ocorrências de deficiência operacional do produto.

4.30.5. As ferramentas e equipamentos necessários à manutenção serão de responsabilidade da contratada.

**4.31. Suporte Técnico:**

4.31.1. Deverá ser oferecido suporte técnico da Contratada, com a possibilidade de abertura de chamados, das 7h00 às 20h00, em dias úteis, para a resolução de problemas. É importante destacar que os serviços de suporte técnico devem contemplar as manutenções corretivas e evolutivas para a solução contratada e não podem acarretar custos adicionais ao CONTRATANTE, além do que foi previamente acordado.

4.31.2. A empresa contratada deve encaminhar o chamado para o suporte do fabricante sempre que necessário, seja devido à criticidade, impacto ou urgência do problema, ou caso seja necessário o envolvimento direto do fabricante no processo de correção. É imprescindível que seja fornecido acesso ao site do fabricante para acompanhamento dos chamados, acesso à base de conhecimento e aos fóruns relacionados à solução.

4.31.3. Os serviços de suporte técnico abrangem:

- a) Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução.
- b) Elaboração de relatórios, estudos e diagnósticos sobre o ambiente.
- c) Transferência de conhecimento aos técnicos da Contratante referente aos problemas vivenciados e às soluções aplicadas, na forma a ser determinada pelas partes.
- d) Realização de instalação, atualização e configuração de novas versões dos produtos após a disponibilização das atualizações tecnológicas pelo fabricante.

4.31.4. O suporte técnico deve contemplar o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso do software ou para correção de problemas, em especial na configuração de parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução.

4.31.5. O suporte técnico deve contemplar, quando for o caso, atendimento a eventual problema de instalação ou configuração de softwares básicos e de infraestrutura de TIC (sistemas operacionais, servidores de banco de dados, servidores de aplicação, etc.) necessários ao funcionamento da solução.

4.31.6. Deve contemplar também a atualização de versões do software aplicativo, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela fabricante, num empacotamento estável do sistema. O serviço de atualização de versão tem por finalidade assegurar a devida atualização da solução durante o período de vigência da garantia. Refere-se ao fornecimento de novas versões e releases da solução lançados no período. A cada nova liberação de versão e release, serão disponibilizados em formato digital manuais e demais documentos técnicos, bem como nota informativa das funcionalidades implementadas. Em caso de lançamento de patch de correção, a CONTRATADA deverá comunicar o fato ao CONTRATANTE e indicar a forma de obtenção e os defeitos que serão corrigidos pelo patch. Em ambos os casos, a comunicação deve ser feita no prazo de até 30 dias, a contar do lançamento de nova versão ou solução de correção.

4.31.7. A CONTRATADA será responsável pelos serviços de implantação das novas versões e releases dos produtos por ela fornecidos como partes do objeto, bem como pela aplicação dos patches de correção e pacotes de serviço (service packs) relativos a esses produtos. Para a implantação das novas versões/releases, bem como para a aplicação dos patches, deverá ser aberto chamado de suporte técnico com nível de severidade adequado e a prestação dos serviços deve ser agendada com os responsáveis pela solução na CONTRATANTE;

4.31.8. Deverá ser prestado suporte técnico remoto com atendimento mediante registro de chamados em página de website, em sistema fornecido pela CONTRATADA e/ou pelo fabricante; e também através de contato telefônico. Esse serviço destina-se a esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução CONTRATADA;

4.31.9. As peças substitutas deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento e devem integrar a garantia da solução;

4.31.10. A CONTRATADA auxiliará o CONTRATANTE na reinstalação das ferramentas, caso seja necessário, ao longo do tempo de garantia da ferramenta;

4.31.11. A CONTRATADA deverá disponibilizar os seguintes canais de acesso ao suporte técnico:

- I - Portal Web;
- II - E-mail;
- III - Central 0800; e/ou
- IV - Telefone fixo.

4.31.12. O atendimento deve ser contínuo, 24 horas por dia, 7 dias por semana, durante todo o ano, incluindo feriados, em língua portuguesa. O início do atendimento e o prazo de solução devem ser determinados de acordo com o nível de severidade exigido para o caso, conforme os índices de criticidade abaixo:

Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço	Glosa (por evento) para eventual descumprimento
Severidade 1 (Alta)	<p>Sistema parado ou produto inoperante com impacto nas operações críticas de negócio.</p> <p>Exemplos: Servidor de produção ou outro sistema inicial está inativo. Parte substancial dos dados</p>	Em até 2 horas deve ter um técnico do fornecedor on-site.	Em até 8 horas	10%
	<p>essenciais corre risco de perda ou corrupção.</p> <p>Operações relacionadas ao negócio foram afetadas, falha que compromete a integridade geral do sistema ou dos dados.</p>	Em até 4 horas deve ter um técnico do fornecedor on-site.	Entrega da Solução pelo fabricante em até 6 dias.	



Criticidade	Descrição	Prazo Máximo de Atendimento	Prazo Máximo de Restauração de Serviço	Glosa (por evento) para eventual descumprimento
Severidade 2 (Média/Alta)	Alto impacto no ambiente de produção ou grande restrição de funcionalidade. Exemplo: Ocorreu um problema no qual um recurso importante foi gravemente danificado. As operações podem continuar de forma limitada, embora a produtividade a longo prazo possa ser afetada negativamente.	Em até 4 horas deve ter um técnico do fornecedor on-site.	Em até 4 horas deve ter um técnico do fornecedor on-site.	7,50%
		Em até 2 horas um Engenheiro de Suporte do fabricante deve iniciar o atendimento através de transferência ao telefone ou retorno de chamada. Gerente técnico do fabricante deve estar disponível 24x7 e ser automaticamente notificado na abertura do caso.	Em até 16 horas	
			Entrega da Solução pelo fabricante em até 10 dias.	
Severidade 3	O defeito não gera impacto ao negócio. Exemplo: Ocorreu um erro que causou impacto negativo limitado na operações.	Um técnico do fornecedor on-site ou atendimento remoto.	Em até 24 horas.	5%
		Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato.	Entrega da Solução pelo fabricante em até 15 dias ou na próxima atualização do Software.	
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. Exemplos: O problema não afetou as	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 12 horas um técnico do fornecedor	2%

<b>Criticidade</b>	<b>Descrição</b>	<b>Prazo Máximo de Atendimento</b>	<b>Prazo Máximo de Restauração de Serviço</b>	<b>Glosa (por evento) para eventual descumprimento</b>
	operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos recursos ou aprimoramento do software licenciado.		entra em contato.	

4.31.13. Para cada chamado de suporte categorizado como grau de severidade 1, o recurso previsto na tabela acima deverá ser notificado e iniciará o auxílio na condução do processo internamente junto ao fabricante. É importante destacar que todos os prazos para atendimento da garantia começarão a ser contados a partir da abertura do chamado, independentemente de ter sido feito via telefone, e-mail, site da contratada ou do fabricante. Além disso, o período de suporte deve estar diretamente atrelado ao período de garantia da solução.

4.31.14. Dentro do prazo máximo de atendimento, cabe ao fornecedor dar início, junto ao contratante, às providências que serão adotadas para a solução do chamado. Considera-se plenamente solucionado o problema quando os sistemas/serviços forem restabelecidos sem restrições, ou seja, quando não se tratar de uma solução paliativa.

4.31.15. Para os chamados de severidades 1 e 2, os serviços de atendimento de garantia não podem ser interrompidos até o completo restabelecimento de todas as funções do sistema paralisado, mesmo que isso exija períodos noturnos e dias não úteis (sábados, domingos e feriados). Além disso, os chamados de garantia de severidades 1 e 2 devem contar com suporte in loco da contratada para agilizar o restabelecimento do serviço.

4.31.16. O fornecedor emitirá um relatório, sempre que solicitado pelo contratante, em formato eletrônico, preferencialmente em arquivo texto, contendo informações analíticas e sintéticas dos chamados da garantia abertos e fechados no período. Esse relatório deve incluir:

- I - Quantidade de ocorrências (chamados) registradas no período.
- II - Número do chamado registrado e nível de severidade, incluindo reaberturas. Data e hora de abertura.
- III - Data e hora de início e conclusão do atendimento.
- IV - Identificação do técnico do contratante que registrou o chamado.
- V - Identificação do técnico do contratante que atendeu o chamado da garantia. Descrição do problema.
- VI - Descrição da solução.
- VII - Informações sobre eventuais escalonamentos.
- VIII - Resumo da lista de chamados concluídos fora do prazo de solução estabelecido.
- IX - Total de chamados no mês e o total acumulado até a apresentação do relatório.

4.31.17. Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante.

4.31.18. Deverá ser emitido um relatório de histórico e revisão de casos, fornecido pelo gerente técnico do fabricante, sob os chamados abertos ou de responsabilidade do fabricante.

4.31.19. Não se encaixam nos prazos descritos nos itens referentes aos níveis de criticidade, problemas cuja solução dependa de correção de falhas (bugs) ou da liberação de novas versões e patches de correção, desde que comprovados pelo fabricante da solução.

4.31.20. Para esses problemas, o fornecedor deverá, nos prazos estabelecidos nos níveis de criticidade, restabelecer o ambiente, através de uma solução de contorno e informar ao contratante, em um prazo máximo de 24 (vinte e quatro) horas, quando a solução definitiva será disponibilizada para o contratante.

4.31.21. Esta solução definitiva de que trata o subitem anterior deverá ser disponibilizada no prazo máximo de 60 (sessenta) dias úteis, no caso da necessidade de criação de um patch/fix.

4.32. **Requisitos Sociais, Ambientais e Culturais:**

4.32.1. A Contratada deve aderir aos padrões estabelecidos pelo Modelo de Acessibilidade em Governo Eletrônico (e-MAG), conforme a Portaria Normativa SLTI nº 03, de 7 de maio de 2007. Essa aderência é necessária quando houver a necessidade de tornar o aplicativo acessível para solicitações de suporte técnico, visando garantir a inclusão e acessibilidade para todos os usuários.

4.32.2. Os serviços prestados pela Contratada devem sempre considerar o uso racional de recursos e equipamentos, com o objetivo de evitar o desperdício de insumos e materiais, bem como a geração excessiva de resíduos. Essa prática está alinhada com as diretrizes de responsabilidade ambiental adotadas pela Contratante.

4.32.3. A Contratada é responsável por fornecer orientações aos seus funcionários sobre a importância da racionalização de recursos no desempenho de suas atribuições, assim como sobre as diretrizes de responsabilidade ambiental adotadas pela Contratante. Essas orientações devem destacar a importância de reduzir o consumo de recursos, reutilizar materiais sempre que possível e realizar descarte adequado dos resíduos.

4.32.4. Além disso, a Contratada deve autorizar a participação de seus funcionários em eventos de capacitação e sensibilização promovidos pela Contratante, quando necessário. Esses eventos têm como objetivo fornecer conhecimentos e práticas relacionadas à racionalização de recursos e responsabilidade ambiental, visando aprimorar a conscientização e o desempenho sustentável da equipe da Contratada.

4.33. **Requisitos Temporais:**

4.33.1. As diretrizes relacionadas aos requisitos a seguir deverão ser considerados no processo de atendimento, entrega e instalação de equipamentos e serviços:

4.34. **Prazo de início de atendimento para suporte técnico e manutenção pela garantia:**

4.34.1. O início do atendimento deve seguir o que está especificado no acordo de nível de serviço presente no Termo de Referência.

4.35. **Requisitos de Segurança e Privacidade**

4.35.1. A CONTRATADA deve seguir os regulamentos, normas e instruções de segurança da informação e comunicações adotados pela CONTRATANTE. Isso inclui a Política de Segurança da Informação e Comunicações e suas Normas Complementares durante a execução dos serviços nas instalações da Secretaria.

4.36. **Devolução de informações confidenciais:**

4.36.1. Toda informação confidencial gerada e/ou manipulada em decorrência do contrato, seja ela armazenada em meio físico, magnético ou eletrônico, deve ser devolvida nas seguintes situações:

- a) término ou rompimento do contrato; ou
- b) solicitação da CONTRATANTE. A formalização entre as partes é necessária nesses casos.

4.37. **Utilização de ferramentas de proteção e segurança de informações:**

4.37.1. É imprescindível o uso de ferramentas de proteção e segurança de informações para evitar acesso não autorizado aos sistemas e softwares. Isso se aplica tanto aos sistemas sob responsabilidade

direta da CONTRATADA quanto aos disponibilizados à CONTRATANTE, mesmo que por meio de link.

4.38. **Realização de alterações para sanar problemas de segurança ou vulnerabilidade:**

4.38.1. Quando formalmente solicitado pela CONTRATANTE, a CONTRATADA deve priorizar e realizar alterações para solucionar possíveis problemas de segurança ou vulnerabilidade nos sistemas ou softwares utilizados para a execução do serviço contratado.

4.39. **Comunicação de atualizações ou mudanças na configuração dos serviços:**

4.39.1. A CONTRATADA deve informar formalmente e de forma tempestiva ao CONTRATANTE sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados.

4.40. **Prestação de esclarecimentos e informações:**

4.40.1. É responsabilidade da CONTRATADA prestar os esclarecimentos necessários à CONTRATANTE, bem como fornecer informações sobre a natureza e o andamento dos serviços executados ou em execução.

4.41. **Garantia da integridade e disponibilidade dos documentos e informações:**

4.41.1. A empresa CONTRATADA deve garantir a integridade e disponibilidade dos documentos e informações que estão sob sua guarda em função do contrato. Caso ocorram perdas ou danos, a CONTRATADA será responsabilizada.

4.42. **Confidencialidade das informações:**

4.42.1. A CONTRATADA não pode divulgar, mesmo que em caráter estatístico, quaisquer informações originadas na CONTRATANTE sem prévia autorização.

Controle de acesso e identificação dos profissionais:

4.42.2. O acesso às instalações da CONTRATADA onde os serviços serão realizados deve ser controlado e permitido apenas para pessoas autorizadas. Os profissionais da CONTRATADA devem estar devidamente identificados por crachás durante o trabalho. Qualquer profissional considerado inconveniente à boa ordem ou que viole as normas disciplinares da CONTRATANTE deve ser substituído imediatamente.

4.43. **Conhecimento e observância das normas disciplinares da CONTRATANTE:**

4.43.1. A CONTRATADA deve garantir que seus profissionais tenham conhecimento das normas disciplinares do CONTRATANTE e exijam sua fiel observância, especialmente em relação à utilização e segurança das instalações.

4.43.2. A CONTRATADA deve manter sigilo absoluto sobre todas as informações provenientes dos serviços realizados, documentos elaborados e informações obtidas dentro do ambiente da CONTRATANTE.

4.44. **Requisitos Legais:**

4.44.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021 (Lei de Licitações e Contratos Administrativos), à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

5. **CLÁUSULA QUINTA - DO TRATAMENTO DOS DADOS**

5.1. O cadastramento dos itens deve estar devidamente alinhado com a Lei nº 13.709/2018, Lei Geral de Proteção de Dados - LGPD, visando maior segurança jurídica ao estado no contrato a ser firmado;

5.2. A contratada deve seguir as normas relativas ao tratamento de dados pessoais, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD) e no que couber, as orientações contidas nas normas ABNT NBR ISO/IEC 29151:2020 (estabelece objetivos de controle para atender aos requisitos identificados por uma avaliação de risco e impacto relacionada à proteção de dados pessoais) e ABNT NBR ISO/IEC 27701:2019 (especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação).

5.3. A CONTRATADA não pode divulgar, mesmo que em caráter estatístico, quaisquer informações originadas na CONTRATANTE sem prévia autorização.

5.4. A CONTRATADA deve seguir os regulamentos, normas e instruções de segurança da informação e comunicações adotados pela CONTRATANTE. Isso inclui a Política de Segurança da Informação e Comunicações e suas Normas Complementares durante a execução dos serviços nas instalações da Secretaria.

5.5. A empresa CONTRATADA deve assegurar a disponibilidade, integridade, confidencialidade e sigilo dos documentos e informações relacionados ao contrato e aos serviços prestados. Qualquer pessoa que cause perdas e danos à CONTRATANTE ou a terceiros poderá ser responsabilizada legalmente.

## 6. **CLÁUSULA SEXTA - DO LOCAL/PRAZO E CONDIÇÕES DE ENTREGA E RECEBIMENTO**

### 6.1. **Local de Entrega:**

6.1.1. Havendo a necessidade de entrega de equipamento para compor a solução, a entrega do mesmo deverá ocorrer a contar do recebimento da Nota de Empenho, nas dependências da Gerência de Patrimônio e Almoxarifado - GPA, sito à Estrada do Santo Antônio, nº 5323, bairro triangulo, CEP 76805-696, Porto Velho – RO, no horário das 07:30 às 13:30 horas, sempre através de documento hábil que comprove as quantidades recebidas, indicando o nome e matrícula do responsável pelo recebimento.

6.1.2. Na entrega dos produtos/serviços deverão fazer-se acompanhar, além da nota fiscal/fatura, e o certificado de garantia.

### 6.2. **Prazo/Cronograma de Entrega:**

6.2.1. Os veículos serão entregues mediante solicitação da SEDAM, conforme a necessidade/demanda.

6.2.2. A entrega deverá ocorrer no prazo de até 20 (vinte) dias corridos, após o recebimento da nota de empenho e ordem de fornecimento.

6.2.3. Findo o prazo previsto no item anterior, a contratada terá um prazo adicional de até 10 (dez) dias de tolerância para entrega dos materiais, a critério do ordenador de despesas, desde que, comunique o fato a contratante com antecedência mínima de 48(quarenta e oito) horas do término do prazo, acompanhado de justificativa que comprove o impedimento para o cumprimento da obrigação, no qual esta Secretaria por sua vez, decidirá a possibilidade de prorrogação do prazo, ou determinará a cominação das multas cabíveis, que ocorrerá a partir da efetiva notificação.

### 6.3. **Do recebimento:**

6.3.1. O recebimento, conforme o art. 140 da [Lei nº 14.133, de 01 de abril de 2021](#), se dará na forma abaixo:

### 6.4. **Do recebimento provisório:**

6.4.1. Serão os objetos deste Termo de Referência recebidos **PROVISORIAMENTE, pelo seu responsável por seu acompanhamento e fiscalização**, para efeito da verificação da conformidade dos materiais fornecidos, em relação à qualidade e quantidades conforme especificações exigidas, o prazo máximo de 10 (dez) dias úteis contados da data de sua efetiva entrega.

6.4.2. O fiscal do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico, no qual elaborará o laudo de averiguação.

6.4.3. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

6.4.4. Independente de aceitação, a **CONTRATADA** garantirá a qualidade e segurança dos objetos contra defeitos de fabricação, pelo prazo mínimo de 12 (doze) meses, bem como oferecer durante todo o prazo de garantia, efetuando a substituição do produto no prazo de 10 (dez) dias corridos, evitando assim a descontinuidade dos serviços desta Secretaria.



6.5. **Do recebimento definitivo:**

6.6. Serão os objetos deste Termo de Referência recebidos **DEFINITIVAMENTE**, por servidor ou comissão designada pela autoridade competente, após a comprovação da qualidade e quantidades entregues, conforme especificações exigidas, no prazo máximo de 10 (dez) dias da emissão do **TERMO DE RECEBIMENTO PROVISÓRIO**;

6.7. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da [Lei nº 14.133, de 01 de abril de 2021](#), comunicando-se à empresa para emissão de Nota Fiscal no que pertinente à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

6.8. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

6.9. **Das condições gerais de recebimento de bens:**

6.9.1. Todo os serviços deverão ser entregues em perfeito estado de conservação e utilização.

6.9.2. **O recebimento provisório ou definitivo**, não exclui a responsabilidade civil, pela qualidade, correção solidez, e segurança do objeto contratual, nem ético profissional, pela perfeita execução do contrato;

6.9.3. Não serão recebidos ainda que provisoriamente produtos que:

- a) Sejam entregues para recebimento com as especificações diferentes das contidas no Termo de Referência;
- b) Caso suas embalagens apresentem amassados, rasgados ou qualquer deformidade que possa ter comprometido do produto, ou que apresente defeito.

6.9.4. Os equipamentos deverão obedecer as especificações do objeto, bem como todas as outras condições previstas neste Contrato e no Termo de Referência e seus anexos.

6.9.5. O prazo de entrega somente poderá ser prorrogado mediante o cumprimento, pela **CONTRATADA**, dos seguintes requisitos cumulativos:

- a) solicitação de prorrogação protocolada dentro do prazo de entrega;
- b) comprovação documental da ocorrência de motivo imprevisível (caso fortuito, força maior ou fato do príncipe), ocorrido depois da apresentação de sua proposta, que tenha correlação direta de causa e efeito sobre a necessidade do atraso.

6.9.6. Não se admitirá prorrogação se:

- a) o atraso ocorrer por culpa da **CONTRATADA**;
- b) se não cumprir os requisitos da entrega/execução do objeto; ou
- c) houver interesse público devidamente justificado nos autos que demonstre ser a escolha mais vantajosa para a administração.

6.10. A fatura dos equipamentos serão recebidos e analisados pela comissão nomeada através de portaria vigente na data de elaboração deste Contrato, na sede desta SEDAM, sito à Av. Farquar, nº 2986, Bairro Pedrinhas, Edifício Rio Cautário, Curvo 2, 2º andar, CEP 76.801-361 – Porto Velho – RO, telefone nº (69)98482-8704, no horário das 07:30 às 13:30 horas de segunda à sexta.

6.11. Os equipamentos deverão obedecer as especificações do objeto, bem como todas as outras condições previstas no Termo de Referência e seus anexos, devendo os mesmos serem produtos originais ou compatíveis com as originais do fabricante.

6.12. A execução do contrato deverá ser acompanhada e fiscalizada por 1 (um) fiscal de contrato, ou membros de comissão de fiscalização, representantes da Administração especialmente designados conforme requisitos estabelecidos no art. 7º da [Lei nº 14.133, de 01 de abril de 2021](#), ou pelos respectivos substitutos, permitida a contratação de terceiros para assisti-los e subsidiá-los com informações pertinentes a essa atribuição.

## 7. CLÁUSULA SÉTIMA - DA VIGÊNCIA

7.1. Após a homologação da licitação, o adjudicatário terá o prazo de 10 dias úteis, contados a partir de sua convocação, para assinar o Termo de Contrato, conforme art. 105 a 114, da [Lei nº 14.133, de 01 de abril de 2021](#).

7.2. Prazo de vigência do contrato será de até 12 (doze) meses contados da data de assinatura do contrato, podendo ser prorrogado na forma da [Lei nº 14.133, de 01 de abril de 2021](#).

7.3. Em caso de descumprimento de quaisquer das condições estabelecidas no presente instrumento, à rescisão do contrato, seja administrativa ou amigável, será efetuada de acordo com as disposições da [Lei nº 14.133, de 01 de abril de 2021](#) e demais ordenamentos jurídicos, pertinentes ao caso.

7.4. A empresa **CONTRATADA**, deverá apresentar como **condição para assinatura do contrato** a declaração, sob as penas da lei e em cumprimento ao artigo [12º da Constituição do Estado de Rondônia](#), que não possui nenhum vínculo com a administração pública:

Art. 12. Nenhum servidor poderá ser diretor ou integrar conselho de empresa fornecedora do Estado, ou que realize qualquer modalidade de contrato com o Estado, sob pena de demissão do serviço público, salvo quando o contrato obedecer a cláusulas uniformes.

## 8. CLÁUSULA OITAVA - DA ALTERAÇÃO E RESCISÃO CONTRATUAL

Fundamentação Legal: [Lei nº 14.133, de 01 de abril de 2021](#) e [Decreto Estadual nº 28.874/2024](#).

8.1. A rescisão contratual consensual será efetuada na esfera administrativa, em conformidade com as disposições do Art. 137 e seguintes da [Lei nº 14.133, de 01 de abril de 2021](#) e legislação pertinente.

8.2. A rescisão do instrumento contratual, poderá ocorrer nos casos descritos no art. 137 da [Lei nº 14.133, de 01 de abril de 2021](#), conforme citado abaixo:

Art. 137. Constituirão motivos para extinção do contrato, a qual deverá ser formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa, as seguintes situações:

I - não cumprimento ou cumprimento irregular de normas editalícias ou de cláusulas contratuais, de especificações, de projetos ou de prazos;

II - desatendimento das determinações regulares emitidas pela autoridade designada para acompanhar e fiscalizar sua execução ou por autoridade superior;

III - alteração social ou modificação da finalidade ou da estrutura da empresa que restrinja sua capacidade de concluir o contrato;

IV - decretação de falência ou de insolvência civil, dissolução da sociedade ou falecimento do contratado;

V - caso fortuito ou força maior, regularmente comprovados, impeditivos da execução do contrato;

VI - atraso na obtenção da licença ambiental, ou impossibilidade de obtê-la, ou alteração substancial do anteprojeto que dela resultar, ainda que obtida no prazo previsto;

VII - atraso na liberação das áreas sujeitas a desapropriação, a desocupação ou a servidão administrativa, ou impossibilidade de liberação dessas áreas;

VIII - razões de interesse público, justificadas pela autoridade máxima do órgão ou da entidade contratante;

IX - não cumprimento das obrigações relativas à reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz.

8.3. A Administração, a qualquer tempo, poderá promover a extinção antecipada do Termo Contratual, nas formas descritas abaixo:

a) Pela Administração Pública, determinada por ato unilateral e escrito;

b) Consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas;

c) Judicial, determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

8.4. O instrumento contratual também poderá ser rescindido pela Contratada, conforme dispõe o art. 137, § 2º da [Lei nº 14.133, de 01 de abril de 2021](#):

§ 2º O contratado terá direito à extinção do contrato nas seguintes hipóteses:

I - supressão, por parte da Administração, de obras, serviços ou compras que acarrete modificação do valor inicial do contrato além do limite permitido no [art. 125 desta Lei](#);

II - suspensão de execução do contrato, por ordem escrita da Administração, por prazo superior a 3 (três) meses;

III - repetidas suspensões que totalizem 90 (noventa) dias úteis, independentemente do pagamento obrigatório de indenização pelas sucessivas e contratualmente imprevistas desmobilizações e mobilizações e outras previstas;

IV - atraso superior a 2 (dois) meses, contado da emissão da nota fiscal, dos pagamentos ou de parcelas de pagamentos devidos pela Administração por despesas de obras, serviços ou fornecimentos;

V - não liberação pela Administração, nos prazos contratuais, de área, local ou objeto, para execução de obra, serviço ou fornecimento, e de fontes de materiais naturais especificadas no projeto, inclusive devido a atraso ou descumprimento das obrigações atribuídas pelo contrato à Administração relacionadas a desapropriação, a desocupação de áreas públicas ou a licenciamento ambiental.

§ 3º As hipóteses de extinção a que se referem os incisos II, III e IV do § 2º deste artigo observarão as seguintes disposições:

I - não serão admitidas em caso de calamidade pública, de grave perturbação da ordem interna ou de guerra, bem como quando decorrerem de ato ou fato que o contratado tenha praticado, do qual tenha participado ou para o qual tenha contribuído;

II - assegurarão ao contratado o direito de optar pela suspensão do cumprimento das obrigações assumidas até a normalização da situação, admitido o restabelecimento do equilíbrio econômico-financeiro do contrato, na forma da [alínea "d" do inciso II do caput do art. 124 desta Lei](#).

## 9. CLÁUSULA NONA - DO REAJUSTE E REEQUILÍBRIO CONTRATUAL

Fundamentação Legal: [Lei nº 14.133, de 01 de abril de 2021](#) e [Decreto Estadual nº 28.874/2024](#).

9.1. O reajuste de preços poderá ser utilizado na presente contratação, desde que seja observado o interregno mínimo de 01 (um) sendo a data-base vinculada à data do orçamento estimado para contratação.

9.2. O contrato será reajustado ou corrigido monetariamente tendo como base os requisitos trazidos no art. 25 da [Lei nº 14.133, de 01 de abril de 2021](#), §§ 7º e 8º, conforme citado abaixo:

§ 7º Independentemente do prazo de duração do contrato, será obrigatória a previsão no edital de índice de reajustamento de preço, com data-base vinculada à data do orçamento estimado e com a possibilidade de ser estabelecido mais de um índice específico ou setorial, em conformidade com a realidade de mercado dos respectivos insumos.

§ 8º Nas licitações de serviços contínuos, observado o interregno mínimo de 1 (um) ano, o critério de reajustamento será por:

I - reajustamento em sentido estrito, quando não houver regime de dedicação exclusiva de mão de obra ou predominância de mão de obra, mediante previsão de índices específicos ou setoriais;

II - repactuação, quando houver regime de dedicação exclusiva de mão de obra ou predominância de mão de obra, mediante demonstração analítica da variação dos custos.

9.3. Conforme arts. 152 e 155 do [Decreto Estadual nº 28.874/2024](#), o pedido de reajuste, repactuação e revisão deverá ser instruído com os seguintes documentos:

Art. 152. Os pedidos de reajustamento em sentido estrito, repactuação e revisão, além da documentação específica relativa ao requerimento elencada nos artigos seguintes, deverão ser instruídos com:

I - requerimento expresso do contratado, contados da publicação do índice ajustado contratualmente, no caso de reajuste em sentido estrito, ou da entrada em vigor do acordo,

convenção ou dissídio coletivo, no caso de repactuação;

II - análise técnica acerca da correção do requerimento do contratado, inclusive quanto aos cálculos, a ser realizada pela Pasta responsável pelo contrato;

III - documentação comprobatória da disponibilidade de recursos orçamentários previstos para fazer frente à despesa a ser assumida, como pedido de reserva ou documento equivalente, além da declaração da compatibilidade da despesa com a legislação orçamentária;

IV - autorização expressa por parte da autoridade máxima da Pasta.

Art. 155.O pedido de reajuste do contrato deverá ser devidamente fundamentado e instruído, além daqueles

constante no art. 152, com os seguintes documentos:

I - planilha de custos demonstrando a equação inicial do contrato, quando esta já não constar do processo

licitatório; e

II - planilha de custos demonstrando a equação atual do contrato, a qual deverá demonstrar a variação do preço,

levando em consideração o índice de reajuste pré-fixado no instrumento convocatório e no contrato.

9.4. Considerando que o reajuste de preços pode ser efetuado mediante a aplicação de índice – reajuste indexação – ou por meio de demonstração analítica de variação dos custos índices aplicar-se-á aos cálculos o índice **IGP-M (Índice Geral dos Preços – Mercado)** ou **IPC-A (Índice Nacional de Preços ao Consumidor – Amplo)**, sendo o critério de aplicação, aquele que de forma mais vantajosa se adequar às especificidades do objeto.

9.5. Os reajustes serão precedidos obrigatoriamente de solicitação da CONTRATADA, acompanhada de memória do cálculo, conforme for a variação de custos objeto do reajuste;

9.6. É vedada a inclusão, por ocasião do reajuste de itens não previstos na proposta inicial, exceto quando se tornarem obrigatórios por força de instrumento legal.

9.7. O pedido de reajuste e reequilíbrio contratual será analisado por esta Secretaria em até 60 (sessenta) dias.

9.8. A análise quanto ao reajuste ou repactuação ficará suspensa em caso de pendência de atos ou apresentação de documentação por parte da CONTRATADA.

## 10. CLÁUSULA DÉCIMA - GARANTIA CONTRATUAL

**Fundamentação Legal:** [Lei nº 14.133, de 01 de abril de 2021](#) e Decreto Estadual nº 28.874/2024.

10.1. O adjudicatário, no prazo de 5 (cinco dias) após a assinatura do Termo de Contrato, prestará garantia no valor correspondente a 2% (dois por cento) do valor do Contrato, que será liberada de acordo com as condições previstas neste Termo de Referência, conforme disposto no art. 96 [Lei nº 14.133, de 01 de abril de 2021](#), desde que cumpridas as obrigações contratuais, optando por uma das seguintes modalidades:

- a) caução em dinheiro ou títulos da dívida pública;
- b) seguro – garantia;
- c) fiança bancária; ou
- d) Título de capitalização custeado por pagamento único.

10.2. A garantia contratual não poderá ultrapassar a 5% do valor inicial do contrato, envolvendo alta complexidade técnica e riscos financeiros consideráveis, demonstrados nos autos do processo, hipótese em que o limite pode chegar até 10%.

10.3. A garantia prestada pela Contratada será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração, e, quando em dinheiro, atualizada

monetariamente, deduzidos eventuais valores devido à Contratante.

**11. CLÁUSULA DÉCIMA PRIMEIRA - DO VALOR**

11.1. O valor total da contratação será de XXX.

**12. CLÁUSULA DÉCIMA SEGUNDA - DO PRAZO E CONDIÇÕES DE GARANTIA**

12.1. A garantia dos referidos serviços concernentes ao objeto deste Termo de Referência serão regidos conforme os dispositivos da Lei 8.078/90 (Código de Defesa do Consumidor - CDC), bem como o disposto na [Lei nº 14.133, de 01 de abril de 2021](#).

12.2. Os serviços deverão fazer-se acompanhar da nota fiscal discriminativa para efetivação de sua entrega.

12.3. A garantia deverá ser fornecida com prazo mínimo de 12 (doze) meses, contadas a partir da emissão do Termo de Recebimento Definitivo emitido por esta Secretaria.

12.4. A garantia deverá atender a todos os componentes físicos e lógicos que fazem parte do objeto do presente instrumento;

12.5. Em caso de garantia superior ao previsto no subitem 12.3, não poderá esta impor nenhum custo adicional a contratante.

12.6. O pedido de substituição ou reparo do objeto, durante o período de garantia, poderá ser formalizado por telefone, e-mail, ofício ou outro meio hábil de comunicação disponibilizado pela CONTRATADA.

**13. CLÁUSULA DÉCIMA TERCEIRA - DAS CONDIÇÕES DE PAGAMENTO**

Fundamentação Legal: [Lei nº 14.133, de 01 de abril de 2021](#) e [Decreto Estadual nº 28.874/2024](#).

13.1. O pagamento das notas fiscais seguirá os moldes definidos pela [Lei nº 14.133, de 01 de abril de 2021](#) e [Decreto Estadual nº 28.874/2024](#) em seu art. 190.

13.2. O pagamento será efetuado mediante Nota Fiscal de Bens certificada pela Comissão de Recebimento de Bens e de acordo com o art. 190 do [Decreto Estadual nº 28.874/2024](#), que deverão ser apresentadas juntamente com a entrega dos produtos, devendo conter no corpo da referida Nota Fiscal/Fatura, a descrição do objeto, o número do contrato e o número da Conta Bancária da **CONTRATADA**, para efetivação do pagamento, o qual deverá ser realizado no prazo de até 15 (quinze) dias após a emissão de Termo de Recebimento Definitivo.

13.3. Na hipótese da apresentação de mais de uma nota fiscal/fatura, e, se alguma delas apresentarem erros ou dúvidas quanto à exatidão ou documentação, a **CONTRATANTE** poderá pagar apenas àquela que se encontra correta, no prazo fixado para pagamento, ressalvado o direito da **CONTRATADA** de reapresentar, para cobrança àquelas inexatas devidamente corrigidas, com as justificativas necessárias (nestes casos também a **CONTRATANTE** terá o prazo de até 15 (quinze) dias, a partir do recebimento, para efetuar uma análise e o pagamento).

13.4. A(s) Nota(s) Fiscal (is)/Fatura (s) deverá (ao) vir acompanhada (s) das seguintes comprovações:

- a) da regularidade fiscal, mediante as Fazendas Federal, Estadual e Municipal
- b) do cumprimento das obrigações trabalhistas;
- c) do relatório das manutenções realizadas, contemplando a descrição dos serviços, dos itens substituídos.
- d) O cumprimento das obrigações trabalhistas, previdenciárias e as relativas ao FGTS.

13.5. Os pagamentos obedecerão a ordem cronológica, disposta no art. 191 do [Decreto Estadual nº 28.874/2024](#), conforme citado abaixo:

- 1. fornecimento de bens;
- 2. locações;

3. prestação de serviços;
4. realização de obras.

13.6. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pela Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

$$I = (TX/100)$$

$$365$$

$$EM = I \times N \times VP, \text{ onde:}$$

**I = Índice de atualização financeira;**

**TX = Percentual da taxa de juros de mora anual;**

**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.**

13.7. Ocorrendo erro no documento da cobrança, este será devolvido e o pagamento será susgado para que a **CONTRATADA** tome as medidas necessárias, passando o prazo para o pagamento a ser contado a partir de data da reapresentação do mesmo.

13.8. Caso se constate erro ou irregularidade na Nota Fiscal, a **ADMINISTRAÇÃO**, a seu critério, poderá devolvê-la, para as devidas correções, ou aceitá-las, com a glosa da parte que considerar indevida.

13.9. Na hipótese de devolução, a Nota Fiscal será considerada como não apresentada, para fins de atendimento das condições contratuais.

13.10. A administração não pagará, sem que tenha autorização prévia e formalmente, 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.

13.11. Os eventuais encargos financeiro, processuais e outros, decorrentes da inobservância, pela empresa de prazo de pagamento, serão de sua exclusiva responsabilidade.

13.12. A **ADMINISTRAÇÃO** efetuará retenção, na fonte, dos tributos e contribuições sobre todos os pagamentos à **CONTRATADA**, conforme Instrução Normativa nº 34/2023/SEFIN-COTES.

#### 14. **CLÁUSULA DÉCIMA QUARTA - DA DOTAÇÃO ORÇAMENTÁRIA**

14.1. As despesas com a prestação de que trata o objeto deste Contrato sairão do seguinte crédito orçamentário:

**Unidade Gestora:** 18001 - SEDAM

**Fontes:** 1.708.0.00001 e/ou 2.708.0.00001 - Transferência da União Referente à Compensação Financeira de Recursos Minerais.

**P/A:** P/A: 2580 - PROMOVER A INOVAÇÃO NA GESTÃO, GOVERNANÇA E SOLUÇÕES TECNOLÓGICAS;

**Elemento de Despesa:** 33.90.40 - Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica.

#### 15. **CLÁUSULA DÉCIMA QUINTA - DOS DEVERES E OBRIGAÇÕES**

##### 15.1. **DA CONTRATANTE**

a) Acompanhar e fiscalizar a execução do contrato, nos termos da [Lei nº 14.133, de 01 de abril de 2021](#) e Decreto Estadual nº 28.874/2024;



- b) Promover o acompanhamento e o recebimento do objeto, verificando se está em conformidade com o que foi solicitado nas especificações/quantitativos contidos neste Termo.
- c) Permitir o livre acesso dos empregados da **CONTRATADA** às dependências do contratante para tratar de assuntos pertinentes aos serviços contratados;
- d) Rejeitar, no todo ou em parte, os serviços e/ou objetos realizados em desacordo com o contrato;
- e) Proceder ao pagamento do contrato, na forma e no prazo pactuado;
- f) Comunicar prontamente à **CONTRATADA**, qualquer anormalidade no objeto do instrumento contratual ou equivalente, podendo recusar o recebimento, caso não esteja de acordo com as especificações e condições estabelecidas no Termo de Referência;
- g) Notificar previamente à **CONTRATADA**, quando da aplicação de sanções administrativa;
- h) Efetuar o pagamento à **CONTRATADA**, de acordo com o estabelecido neste Termo de Referência.
- i) Designar servidor habilitado responsável por acompanhar a realização dos serviços.
- j) Fiel observância ao que tange às prerrogativas da Administração Pública em relação ao Regime Jurídico dos contratos administrativos, consoante ao disposto na [Lei nº 14.133, de 01 de abril de 2021](#).

## 15.2. DA CONTRATADA/FORNECEDOR

15.2.1. Além daquelas determinadas por leis, decretos, regulamentos e demais dispositivos legais que regem os procedimentos licitatórios e os princípios da administração pública, nas obrigações da **CONTRATADA**, além das previstas no presente Termo de Referência, também se incluem os dispositivos a seguir:

- a) Assinar o contrato ou retirar a nota de empenho quando convocada a fazê-lo, no prazo máximo de 10 (dez) dias.
- b) Comunicar a **CONTRATANTE**, verbalmente no prazo de 12 (doze) horas e, por escrito, no prazo de 48 (quarenta e oito) horas, quaisquer alterações ou acontecimento que impeçam mesmo temporariamente, de cumprir seus deveres e responsabilidades relativos à execução da Nota de Empenho, total ou parcialmente, por motivo de caso fortuito ou força maior;
- c) Cumprir fielmente o prazo estabelecido no presente Termo de Referência para o fornecimento do objeto constante do mesmo;
- d) Responsabilizar-se, integralmente, pela entrega dos serviços, não podendo repassar nenhum dos itens do presente a terceiros;
- e) Responsabilizarem-se, integralmente, por todos os tributos, taxas e contribuições (inclusive para-fiscais), que direta ou indiretamente, incidam ou vierem a incidir sobre a presente contratação;
- f) Responsabilizar-se pelos atrasos e/ou prejuízos decorrentes de paralisação parcial ou total da entrega dos materiais/bens;
- g) Permitir e oferecer condições para a mais ampla e completa fiscalização durante a vigência do Contrato;
- h) Manter, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas no TR, informando à Secretaria qualquer adversidade, nos termos do Art. 92, inciso XVI da [Lei nº 14.133, de 01 de abril de 2021](#);

- i) Responsabilizar-se totalmente e as suas expensas com (impostos, taxas e pessoal) pelo transporte/frete dos bens/materiais até o destino final, bem como, quando apresentar defeitos de qualquer natureza, correrá por conta e risco da **CONTRATADA**;
- j) Prestar todos os esclarecimentos que lhe forem solicitados no concernente ao objeto do presente Termo de Referência, inclusive documentação e atos praticados até o recebimento definitivo e cujas reclamações formalmente realizadas obriga-se a atender prontamente;
- k) Responder, integralmente, por perdas e danos que vier a causar à **CONTRATANTE** ou a terceiros, em razão de ação ou omissão dolosa ou culpa, sua ou dos seus prepostos, independentemente de outras cominações contratuais ou legais a que estiver sujeita;
- l) Responsabilizar-se pelos encargos trabalhistas, previdenciários e comerciais, bem como pelos custos de frete e de tributos, resultantes da execução do contrato;
- m) Prover todos os meios necessários à garantia da plena operacionalidade do fornecimento, inclusive considerados os casos de greve ou paralisação de qualquer natureza;
- n) Apresentar Nota Fiscal onde constem detalhadamente indicações de marca, fabricante, modelo, tipo, procedência e prazo de garantia;
- o) Garantir a titularidade e/ou permissão de uso de todo e qualquer direito de propriedade industrial envolvido nos bens, assumindo a responsabilidade por eventuais ações e/ou reclamações, de modo a assegurar à SEDAM a plena utilização dos bens adquiridos, ou a respectiva indenização;
- p) Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, [Lei nº 8.078, de 11 de setembro de 1990 \(Código de Defesa do Consumidor\)](#);
- q) Prestar todo o suporte solicitado, sem ônus para a **CONTRATANTE**, seja via telefone, seja através de correio eletrônico, seja, ainda, presencialmente.
- r) Responsabilizar-se quanto a reparação, correção, remoção, reconstrução ou substituição, no total ou em parte, o objeto em comento caso seja verificado vícios, defeitos ou incorreções resultantes da execução ou do material empregado, conforme determina o art. 119 da [Lei nº 14.133, de 01 de abril de 2021](#);
- s) pelo adequado tratamento de dados pessoais, seguindo instruções fornecidas pelo Contratante e observando suas próprias instruções e normas sobre a matéria;
- t) pelo registro das operações de tratamento de dados pessoais;
- u) pela guarda de sigilo dos dados pessoais tratados ou por informações de cunho restrito ou confidencial que tenha acesso em decorrência da execução do contrato;
- v) pela formulação de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao objeto do contrato;
- w) pela adoção de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;
- x) por notificar/informar imediatamente à Contratante os casos de incidentes de segurança da informação que envolvam o objeto de contrato;
- y) pelo descarte seguro dos dados pessoais tratados após o término de seu tratamento;

z) pelo não compartilhamento dos dados pessoais com outras organizações ou pessoas sem autorização da Contratante e nem tratá-los de forma incompatível com as finalidades do contrato;

aa) por seguir as normas relativas ao tratamento de dados pessoais, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD), regulamentações expedidas pela Autoridade nacional de Proteção de Dados Pessoais (ANPD) e pelo Comitê Gestor de Privacidade e proteção de Dados Pessoais do Estado de Rondônia (CGPD); e

ab) por seguir, no que couber, as orientações contidas nas normas ABNT NBR ISO/IEC 29151:2020 (estabelece objetivos de controle para atender aos requisitos identificados por uma avaliação de risco e impacto relacionada à proteção de dados pessoais) e ABNT NBR ISO/IEC 27701:2019 (especifica os requisitos e fornece as diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Privacidade da Informação).

## 16. CLÁUSULA DÉCIMA SEXTA - DO ACOMPANHAMENTO E FISCALIZAÇÃO

16.1. A execução do Contrato, nos termos da [Lei nº 14.133, de 01 de abril de 2021](#), em seu art. 117, será acompanhada e fiscalizada por servidores da Gerência de Patrimônio e Almoxarifado - GPA e Gerência de Contratos - GCON, que serão oportunamente designados pela Coordenadoria de Patrimônio Administração e Finanças e/ou Diretoria Executiva e/ou Gabinete.

16.2. A responsável pela fiscalização e acompanhamento do processo será **Victor da Silva Tavares, Matrícula: \*\*\*.\*\*\*.597, E-mail: victortavares@sedam.ro.gov.br**.

16.3. Será anotado em registro próprio todas as ocorrências relacionadas com o recebimento dos objetos, determinando o que for necessário à regularização das faltas ou defeitos observados, e atestará as notas fiscais/faturas apresentadas, para fins de pagamento, conforme traz o art. 117, § 1º da [Lei nº 14.133, de 01 de abril de 2021](#).

16.4. Conforme traz o art. 20 do Decreto Estadual nº 28.874/2024, as atribuições do **Gestor do Contrato**, serão:

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;

[...]

16.5. No que tange as atribuições vinculadas ao Fiscal do Contrato, estão especificadas:

Art. 22. A função de fiscal de contrato deve ser atribuída a servidor com experiência e conhecimento na área relativa ao objeto contratado, designado para auxiliar o gestor do contrato quanto à fiscalização dos aspectos administrativos e técnicos do contrato, cabendo-lhe, dentre outras atribuições inerentes à função:

- I - conhecer o termo de contrato e todos os seus Anexos, especialmente o Projeto Básico ou o Termo de Referência, certificando-se de que a contratada está cumprindo todas as obrigações assumidas;
- II - confrontar os preços e quantidades constantes da nota fiscal com os estabelecidos no contrato;
- III - no caso específico de obras e prestação de serviços de engenharia, cumpre ainda aos fiscais:
  - a) fazer constar todas as ocorrências no Diário de Obras, com vistas a compor o processo documental, de modo a contribuir para dirimir dúvidas e embasar informações acerca de eventuais reivindicações futuras, tomando as providências que estejam sob sua alçada e dando ciência ao gestor quando excederem as suas competências;
  - b) zelar pela fiel execução da obra, sobretudo no que concerne à qualidade dos materiais utilizados e dos serviços prestados, bem como quanto aos aspectos ambientais;
  - c) atestar o funcionamento de equipamentos e registrar a conformidade em documento;
  - d) acompanhar e analisar os testes, ensaios, exames e provas necessários ao controle de qualidade dos materiais, serviços e equipamentos a serem aplicados na execução do objeto contratado, quando houver;
  - e) informar ao gestor ocorrências que possam gerar dificuldades à conclusão da obra ou em relação a terceiros; e
  - f) proceder, conforme cronograma físico-financeiro, às medições dos serviços executados, conforme disposto em contrato.

16.6. A fiscalização da execução dos serviços abrange, ainda, as seguintes rotinas:

- a) Observar o fiel adimplemento das disposições contratuais;
- b) Solicitar a imediata substituição de funcionário da **CONTRATADA** que embaraçar ou dificultar o seu atendimento e a sua fiscalização, a seu exclusivo critério;
- c) Rejeitar, no todo ou em parte, os serviços fornecidos em desacordo com as especificações deste Termo de Referência;
- d) Suspender a execução do fornecimento contratados, sem prejuízo das penalidades a que se sujeita a **CONTRATADA**, garantido o contraditório e a ampla defesa.

16.7. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da **CONTRATADA**, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica em corresponsabilidade da **CONTRATANTE** ou de seus agentes e prepostos, de conformidade com o art. 120 da [Lei nº 14.133, de 01 de abril de 2021](#)

#### 17. CLÁUSULA DÉCIMA SÉTIMA - DO ACRÉSCIMO E SUPRESSÃO

17.1. Os acréscimos ou supressões não poderão exceder a 25% do valor inicial atualizado do contrato, conforme estabelece o art. 125 da [Lei nº 14.133, de 01 de abril de 2021](#).

17.2. O contratado fica obrigado a aceitar, nas mesmas condições contratuais, as supressões resultantes de acordo celebrado entre os contratantes.

#### 18. CLÁUSULA DÉCIMA OITAVA - DAS INFRAÇÕES E DAS SANÇÕES ADMINISTRATIVAS

Fundamentação Legal: [Lei nº 14.133, de 01 de abril de 2021](#) e [Decreto Estadual nº 28.874/2024](#).

18.1. Sem prejuízo das sanções cominadas no art. 156, I, III e IV, da [Lei nº 14.133, de 01 de abril de 2021](#) e art. 185, § único do [Decreto Estadual nº 28.874/2024](#), pela inexecução total ou parcial do contrato, a Administração poderá, garantida a prévia e ampla defesa, aplicar à **CONTRATADA** multa de até 10% (dez por cento) sobre a parcela inadimplida.

18.2. 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 contratado*.

18.3. A interessada, adjudicatária ou **CONTRATADA** que, convocada dentro do prazo de validade de sua proposta, não celebrar o instrumento contratual, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução de seu objeto, não mantiver a

proposta, falhar ou fraudar na execução do instrumento contratual, comportar-se de modo inidôneo ou cometer fraude fiscal, garantida a prévia e ampla defesa, ficará impedida de licitar e contratar com a União, Estados Distrito Federal e Municípios, e será descredenciado no Cadastro de Fornecedores dos Órgãos da Administração Pública e Estadual, pelo prazo de até 03 (três) anos, sem prejuízo das multas previstas no Termo de Referência e das demais cominações legais, devendo ser incluída a penalidade no SICAFI e no CAGEFIMP - Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual;

18.4. 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) dias úteis, contados de sua intimação, para efetuar o pagamento da multa. Após esse prazo, não sendo efetuado o pagamento seus dados serão encaminhados ao órgão competente para que seja inscrita na dívida ativa, podendo, ainda a administração proceder à cobrança judicial da multa.

18.5. As multas previstas não eximem a adjudicatória ou **CONTRATADA** da reparação dos eventuais danos, perdas ou prejuízos que seu ato punível venha causar a Administração.

18.6. De acordo com a gravidade do descumprimento, poderá ainda a interessada 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 Administração pelos prejuízos resultantes e depois de decorrido o prazo da sanção aplicada com base na legislação vigente.

18.7. 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 significativo.

18.8. São exemplos de infrações administrativas, nos termos da [Lei nº 14.133, de 01 de abril de 2021](#), em seu art. 155, conforme disposto abaixo:

Art. 155. O licitante ou o contratado será responsabilizado administrativamente pelas seguintes infrações:

I - dar causa à inexecução parcial do contrato;

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

III - dar causa à inexecução total do contrato;

IV - deixar de entregar a documentação exigida para o certame;

V - não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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

VII - ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

VIII - apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

IX - fraudar a licitação ou praticar ato fraudulento na execução do contrato;

X - comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

XI - praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

XII - praticar ato lesivo previsto no [art. 5º da Lei nº 12.846, de 1º de agosto de 2013](#).

Art. 156. Serão aplicadas ao responsável pelas infrações administrativas previstas nesta Lei as seguintes sanções:

- I - advertência;
- II - multa;
- III - impedimento de licitar e contratar;
- IV - declaração de inidoneidade para licitar ou contratar.

18.9. No caso de atraso injustificado na execução do contrato, a CONTRATADA estará sujeita à multa de mora, no valor de 0,4% do valor inicial contratado por dia, estando sujeita ainda as outras penalidades previstas neste Termo de Referência e/ou no Contrato, nos termos do art. 162 da [Lei nº 14.133, de 01 de abril de 2021](#), conforme citado abaixo:

Art. 162. O atraso injustificado na execução do contrato sujeitará o contratado a multa de mora, na forma prevista em edital ou em contrato.

Parágrafo único. A aplicação de multa de mora não impedirá que a Administração a converta em compensatória e promova a extinção unilateral do contrato com a aplicação cumulada de outras sanções previstas nesta Lei.

18.10. 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.

18.11. Para efeito de aplicação de multas, às infrações são atribuídos graus, com percentuais de multa 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*
01	Permitir situação que crie a possibilidade ou cause dano físico, lesão corporal ou consequências letais; por ocorrência.	06	4,0% por dia
02	Usar indevidamente informações sigilosas a que teve acesso; por ocorrência	06	4,0% por dia
03	Suspender, interromper ou recusar-se, salvo por motivo de força maior ou caso fortuito, a entrega dos produtos e nas condições estabelecidas, por dia e por unidade de atendimento;	05	3,2% por dia
04	Destruir ou danificar documentos por culpa ou dolo de seus agentes; por ocorrência.	05	3,2% por dia
05	Recusar-se a executar serviço determinado pela FISCALIZAÇÃO, sem motivo justificado; por ocorrência;	04	1,6 % por dia
06	Manter funcionário sem qualificação para a execução dos serviços; por empregado e por dia.	03	0,8 % por dia
07	Executar serviço incompleto, paliativo substitutivo como por caráter permanente, ou deixar de providenciar recomposição complementar; por ocorrência.	02	0,4 % por dia
08	Fornecer informação pérfida de serviço ou substituição de material; por ocorrência.	02	0,4 % por dia
<b>ITEM</b>	<b>Para os itens a seguir, deixar de:</b>	<b>GRAU</b>	<b>MULTA*</b>
01	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
02	Refazer serviço não aceito pela FISCALIZAÇÃO, nos prazos estabelecidos no contrato ou determinado pela	03	0,8% por dia



ITEM	DESCRIÇÃO DA INFRAÇÃO	GRAU	MULTA*
	FISCALIZAÇÃO; por unidade de tempo definida para determinar o atraso.		
03	Cumprir prazo previamente estabelecido com a FISCALIZAÇÃO para fornecimento de materiais ou execução de serviços; por unidade de tempo definida para determinar o atraso.	03	0,8 % por dia
04	Iniciar execução de serviço nos prazos estabelecidos pela FISCALIZAÇÃO, observados os limites mínimos estabelecidos por este Contrato; por serviço, por ocorrência.	02	0,4% por dia
05	Disponibilizar equipamentos, insumos e materiais necessários à realização dos serviços do escopo do contrato; por ocorrência.	02	0,4% por dia
06	Efetuar a entrega dos produtos nos prazos estabelecidos, observadas as condições estabelecidas por este Contrato, por ocorrência.	02	0,4% por dia
07	Ressarcir o órgão por eventuais danos causados por sua culpa, ou de seus prepostos.	02	0,4% por dia
08	Manter a documentação de habilitação atualizada; por item, por ocorrência.	01	0,2% por dia

*\* incidente sobre a parte inadimplida do contrato"*

18.12. As sanções aqui previstas poderão ser aplicadas concomitantemente, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 15 (quinze) dias úteis.

18.13. Após 30 (trinta) dias da falta de execução do objeto, será considerada inexecução total do contrato, o que ensejará a rescisão contratual.

18.14. As sanções de natureza pecuniária serão diretamente descontadas de créditos que eventualmente detenha a **CONTRATADA** ou efetuada a sua cobrança na forma prevista em lei.

18.15. As sanções previstas não poderão ser relevadas, salvo ficar comprovada a ocorrência de situações que se enquadrem no conceito jurídico de força maior ou casos fortuitos, devidos e formalmente justificados e comprovados, e sempre a critério da autoridade competente, conforme prejuízo auferido.

18.16. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

18.17. Também ficam sujeitas às penalidades de suspensão de licitar e impedimento de contratar com o órgão licitante e de declaração de inidoneidade, previstas no subitem anterior, as empresas ou profissionais que, em razão do contrato decorrente desta licitação:

- a) Tenham sofrido condenações definitivas por praticarem, por meio dolosos, fraude fiscal no recolhimento de tributos;
- b) Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;
- c) Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

18.18. Atender no que pede a [Instrução Normativa nº 1/2021/SUPEL/ASJUR](#), que regula o rito processual administrativo.

**19. CLÁUSULA DÉCIMA NONA- DA SUBCONTRATAÇÃO**

19.1. É vedada a subcontratação, cessão e/ou transferência total ou parcial do objeto deste termo de referência, conforme art. 122, §2º da [Lei nº 14.133, de 01 de abril de 2021](#).

**20. CLÁUSULA VIGÉSIMA- DA SUSTENTABILIDADE**

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

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

20.3. 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;

20.4. A **CONTRATADA** deverá cumprir as orientações dispostas referente aos critérios de Sustentabilidade Ambiental, no que couber, conforme art. 144 da [Lei nº 14.133, de 01 de abril de 2021](#).

20.5. A **CONTRATADA** deverá preencher modelo de declaração de sustentabilidade ambiental presente no **ANEXO III** do Termo de Referência.

**21. CLÁUSULA VIGÉSIMA PRIMEIRA - NORMAS DE PREVENÇÃO A CORRUPÇÃO**

21.1. Para a execução deste Contrato, nenhuma das partes poderá oferecer dar ou se comprometer a dar a quem quer que seja, ou aceitar ou se comprometer a aceitar de quem quer que seja, tanto por conta própria quanto por intermédio de outrem, qualquer pagamento, doação, compensação, vantagens financeiras ou benefícios de qualquer espécie, seja de forma direta ou indireta quanto ao objeto deste Contrato, ou de outra forma a ele não relacionada, o que deve ser observado, ainda, pelos prepostos e colaboradores.

**22. CLÁUSULA VIGÉSIMA SEGUNDA - DOS CASOS OMISSOS**

22.1. As omissões, dúvidas e casos não previstos neste instrumento, serão resolvidos e decididos aplicando-se as regras da [Lei nº 14.133, de 01 de abril de 2021](#), bem como demais ordenamentos jurídicos correlatos, levando-se sempre em consideração os princípios que regem a Administração Pública

**23. CLÁUSULA VIGÉSIMA TERCEIRA- DA MATRIZ DE RISCO**

23.1. A Matriz de Risco, apresentada no Item Anexos do Termo de Referência, e anexo do Edital, é uma ferramenta que permite aos gestores mensurar, avaliar e ordenar os eventos de riscos que podem afetar o alcance dos objetivos do processo da unidade e, conseqüentemente, os objetivos estratégicos da presente Contratação.

23.2. A **CONTRATADA** é integral, e exclusivamente, responsável por todos os riscos colocados como de sua competência, relacionados ao objeto do contrato, inclusive, mas sem limitação, conforme estabelecido na Matriz de Risco.

23.3. A **CONTRATADA** não é responsável pelos riscos relacionados ao objeto do contrato, cuja responsabilidade é da **CONTRATANTE**, conforme estabelecido na Matriz de Risco.

23.4. Constitui peça integrante deste contrato, independentemente de transcrição no instrumento respectivo, a Matriz de Risco.

23.5. O termo risco neste contrato é designado como um evento ou uma condição incerta que, se ocorrer, tem um efeito em pelo menos um objetivo da Contratação.

23.6. Além disso, o risco é o resultado da combinação entre probabilidade de ocorrência de determinado evento futuro e o impacto resultante caso ele ocorra.

23.7. Portanto, a análise dos riscos associados a Contratação é realizada com base nas informações da Matriz de Risco.

**24. CLÁUSULA VIGÉSIMA QUARTA- DA PUBLICAÇÃO**

24.1. Incumbirá à Contratante providenciar a publicação deste instrumento no Portal Nacional de Contratações Públicas (PNCP) e/ou no sítio eletrônico oficial do Estado de Rondônia, conforme definido em Decreto.

25. **CLÁUSULA VIGÉSIMA QUINTA- DO FORO**

25.1. Fica eleito o Foro da Comarca de Porto Velho/RO, para dirimir quaisquer dúvidas referentes à Licitação e procedimentos dela resultantes, com renúncia expressa de qualquer outro, por mais privilegiado que seja.

26. **CLÁUSULA VIGÉSIMA SEXTA- DAS ASSINATURAS E DATA DE CELEBRAÇÃO**

26.1. Considerando que esta 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.

**Parágrafo único.** Este instrumento jurídico foi elaborado na forma do art. 23, I, da LCE 620/2011, segundo as informações e documentos constantes dos autos do processo identificado neste instrumento.

Para firmeza e como prova do acordado, este Contrato, o qual, depois de lido e achado conforme, vai assinado eletronicamente pelas partes.



Documento assinado eletronicamente por **Sara Midia Gomes Pascoal, Gerente**, em 07/05/2025, às 12:17, 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 **0059625571** e o código CRC **534239AB**.

**Referência:** Caso responda este(a) Minuta de Contrato, indicar expressamente o Processo nº 0028.020065/2024-49

SEI nº 0059625571

Criado por [02476212261](#), versão 27 por [02124030280](#) em 07/05/2025 12:16:55.

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	PREÇO MÍNIMO (D)	PREÇO MÉDIO (E)	PREÇO MEDIANO (F)	DESVIO PADRÃO	COEFICIENTE DE VARIAÇÃO	PARÂMETRO UTILIZADO (MÍNIMO/MÉDIO)	SUBTOTAL GERAL [F + G]
LOTE ÚNICO														
1	Solução de proteção avançada contra ataques cibernéticos para estações de trabalho (Extended detection and response - XDR)	LICENÇAS	800	R\$ 396,84	R\$ 310,00	R\$ 472,00	R\$ 275,50	R\$ 275,50	R\$ 363,59	R\$ 353,42	88,49	24,34%	MÉDIO	R\$ 290.872,00
2	Solução de proteção avançada contra ataques cibernéticos para servidores (Extended detection and response - XDR)	LICENÇAS	300	R\$ 767,79	R\$ 740,00	R\$ 540,00	NC	R\$ 540,00	R\$ 682,60	R\$ 740,00	124,27	18,21%	MÉDIO	R\$ 204.780,00
3	Serviços de suporte pro ativo, corretivo e para resposta a incidentes	MESES	60	R\$ 750,00	R\$ 605,38	R\$ 831,00	7000*	R\$ 605,38	R\$ 728,79	R\$ 750,00	114,30	15,68%	MÉDIO	R\$ 43.727,40
4	Serviço de treinamento	UND	3	R\$ 17.578,00	R\$ 12.300,00	R\$ 14.400,00	R\$ 18.000,00	R\$ 12.300,00	R\$ 15.569,50	R\$ 15.989,00	2.707,94	17,39%	MÉDIO	R\$ 46.708,50
VALOR DO LOTE ÚNICO														R\$ 586.087,90
VALOR TOTAL														R\$ 586.087,90
VALOR DO LOTE ÚNICO														R\$ 586.087,90

LEGENDA:  
NC = Não encontrado  
\* = Valores excluídos por elevar a taxa de desvio padrão acima de 25,99% conforme estipulado na Instrução Normativa nº 01/2024/SUPEL-CPEAP

NOTA EXPLICATIVA:  
IDENTIFICAÇÃO DAS COTAÇÕES

EMP1	BANCO DE PREÇOS
EMP2	BANCO DE PREÇOS
EMP3	BANCO DE PREÇOS
EMP4	CONTRATO 03/2024 - ANTAQ

1) As descrições foram reduzidas neste quadro comparativo, porém se encontra completas no termo de referência ().



GOVERNO DO ESTADO DE RONDÔNIA  
Secretaria de Estado do Desenvolvimento Ambiental - SEDAM

SAMS

Órgão Requisitante: Secretaria de Estado do Desenvolvimento Ambiental - SEDAM

Processo Administrativo nº: [0028.020065/2024-49](#)

Unidades Gestoras: **Unidade Gestora:** 18001 - SEDAM; **Fontes:** 1.708.0.00001 e/ou 2.708.0.00001 - Transferência da União Referente à Compensação Financeira de Recursos Minerais; **P/A:** 2580 - PROMOVER A INOVAÇÃO NA GESTÃO, GOVERNANÇA E SOLUÇÕES TECNOLÓGICAS; **Elemento de Despesa:** 33.90.40 - Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica.

Exposição de Motivo: **Contratação de empresa para fornecimento de solução de proteção para estações de trabalho e servidores contra ataques cibernéticos.**

LOTE	ITEM	DESCRIÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
LOTE ÚNICO	01	Solução de proteção avançada contra ataques cibernéticos para estações de trabalho (Extended detection and response - XDR)	Licenças	800		
	02	Solução de proteção avançada contra ataques cibernéticos para servidores (Extended detection and response - XDR)	Licenças	300		
	03	Serviços de suporte pro ativo, corretivo e para resposta a incidentes	Meses	60		
	04	Serviço de treinamento	UND	03		


Local:	Responsável pela cotação da Empresa:	USO EXCLUSIVO DA SEDAM - SUPEL	Valor da Proposta:	
Data:	Fone:		Validade Proposta:	
Banco:			Prazo de Entrega:	
Agência:				
C/C:				


**ELABORAÇÃO:**  
**ANDREZA DOS SANTOS BARBOSA**  
Assessor III


**REVISÃO:**  
**SARA MIDIÃ GOMES PASCOAL**  
Gerente Administrativa GAD/COPAF/SEDAM


**ESPECIFICAÇÃO E REVISÃO TÉCNICA:**  
**RENATA DOS SANTOS LUZ COUTINHO**  
Coordenadora de Tecnologia da Informação


**De acordo e autorizado nos termos da lei:**  
**MARCO ANTÔNIO RIBEIRO DE MENEZES LAGOS**  
Secretário de Estado do Desenvolvimento Ambiental

 Documento assinado eletronicamente por **Andreza dos Santos Barbosa, Assessor(a)**, em 30/09/2024, às 13:08, 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 **Sara Midia Gomes Pascoal, Gerente**, em 30/09/2024, às 13:09, 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 **RENATA DOS SANTOS LUZ, Coordenador(a)**, em 08/10/2024, às 09:44, 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 **MARCO ANTÔNIO RIBEIRO DE MENEZES LAGOS, Secretário(a)**, em 08/10/2024, às 12:06, 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](#).

 A autenticidade deste documento pode ser conferida no site [portal do SEI](#), informando o código verificador **0053337368** e o código CRC **D928B1C3**.