Diário Oficial do Estado de Rondônia nº 52
Disponibilização: 19/03/2025
Publicação: 19/03/2025

Governo do Estado de
RONDÔNIA

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

Portaria nº 29 de 14 de março de 2025

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

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

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

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

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

CONSIDERANDO os autos do Processo Administrativo Id. 0043.000155/2024-25 c/c 0043.000304/2024-56,

R E S O L V E :

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

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

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

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

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

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

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

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

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

IX - Marina Dias de Moraes Taufmann, matrícula n.º ******886;

X - Maíza Braga Barbeto, matrícula n.º *******844;

XI - Ronaldo Alves dos Santos, matrícula n.º ******353; e

XII - Valdenir Gonçalves Júnior, matrícula n.º ******985.

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

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

I - Ayanne Carmencita Ramos Dias, matrícula n.º ******964;

II - Elenilson José Satimo Frelik, matrícula n.º ******795;

III - Johnnescley Anes de Morais, matrícula n.º ******669;

IV - Josélia Pagani Ferreira, matrícula n.º ******627;

V - Letícia Carpina Farias Casara, matrícula n.º ******797;

VI - Luciana Pereira de Souza, matrícula n.º ******520;

VII - Letícia Helen Almeida Ferreira, matrícula n.º ******088;

VIII - Matheus Breves Chíxaro Lobo, matrícula n.º ******032;

IX - Sidmar Wesley Correa dos Santos, matrícula n.º ******595;

X - Thales Silva Souza, matrícula n.º ******450; e

XI - Yago da Silva Teixeira, matrícula n.º ******800.

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

I - Aline Cruz de Oliveira, matrícula n.º ******696;

II - Ana Nayanne Batista Lemos, matrícula n.º *****137;

III - Bruna da Silva e Souza, matrícula n.º *****559;

IV - Letícia Helen Almeida Ferreira, matrícula n.º ******088;

V - Franciara Sobrinho do Nascimento Ximenes, matrícula n.º *****832;

VI - Gabriel Henrique Ortiz Aguiar, matrícula n.º *****249;

VII - Guilherme Guimarães dos Santos Ferreira, matrícula n.º ******004;

VIII - Ingrid Tainara Xavier Pedroza, matrícula n.º *****608;

IX - Janaina Muniz Lobato, matrícula n.º ******481;

X - Johnnescley Anes de Morais, matrícula n.º *****669;

XI - Josineide Barbosa Leite Anastácio Ferreira, matrícula n.º ******255;

XII - Júlia Nunes Martins, matrícula n.º *****838;

XIII - Kelvin Klysman de Oliveira Leal, matrícula n.º *****236;

XIV - Krishna Sonniê Teixeira Meneses, matrícula n.º ******433;

XV - Lindainês Bárbara Pereira de Araújo Mendes, matrícula n.º *****240;

XVI - Maria Carolina de Carvalho, matrícula n.º ******197;

XVII - Nadiane da Costa Laia, matrícula n.º ******769;

XVIII - Roberta Arroio, matrícula n.º ******701;

XIX - Tatiana Rachid Bruxel, matrícula n.º ******493;

XX - Wanderly Lessa Mariaca, matrícula n.º ******599; e

XXI - Raiane Jéssica do Nascimento, matrícula n.º ******061; e

XXII - Charles Cunha Menezes Júnior, matrícula n.º ******795.

§ 1º Núcleo de Atendimento:

I - Suélen Torres da Silva, matrícula n.º*******853.

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

Art. 3º Revogar a Portaria nº 83 de 17 de outubro de 2024 Id. (0053907080), publicada no DOE n.º 94, pp. 70-72, de 25 de outubro de 2024, bem como a Portaria nº 89 de 01 de novembro de 2024, publicada no DOE 207, pp. 99-100, de 04 de novembro de 2024.

Parágrafo Único. Os atos praticados pelos membros designados antes da entrada em vigor deste ato normativo permanecem válidos, em conformidade com as regras estabelecidas no normativo revogado, exceto aqueles que vierem a ser substituídos pelas disposições previstas nesta Portaria, que contarão com efeito retroativo indicado no Art. 4º.

Art. 4º Esta portaria entra em vigor na data de sua publicação, com efeitos retroativos a contar do dia 10 de fevereiro de 2025, para os incisos atualizados por este ato normativo.

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

FABÍOLA MENEGASSO DIAS
Superintendente Estadual de Compras e Licitações - SUPEL - Em substituição
Portaria nº 01 de 04 de Janeiro de 2023 (0034842927)

Documento assinado eletronicamente por **Fabíola Menegasso Dias**, **Superintendente**, em 19/03/2025, às 12:55, 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 **0058238338** e o código CRC **2B1F38BB**.

Referência: Caso responda esta Portaria, indicar expressamente o Processo nº 0043.000017/2025-27 SEI nº 0058238338

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

INSTRUMENTO CONVOCATÓRIO

PREGÃO ELETRÔNICO Nº 90428/2024/SUPEL/RO

PARA TODOS OS ITENS, APLICA-SE A AMPLA PARTICIPAÇÃO SEM A RESERVA DE COTA NO TOTAL DE ATÉ 25% ÀS EMPRESAS ME/EPP.

RESUMO DOS DADOS

ABERTURA DA SESSÃO PÚBLICA: 14/04/2025, às 11h00 (horário de Brasília) sítio: http://www.comprasgovernamentais.gov.br.	Limite para esclarecimentos e impugnações ao edital: 09/04/2025.

OBJETO
Aquisição de um software antivírus para atender a estação de trabalho (usuários), baseando- se no fato de que o antivírus corporativo é um software de proteção contra ameaças cibernéticas, desenvolvido com mais recursos e robustez do que as soluções voltadas para dispositivos pessoais. Antivírus para usuários finais são mais simples, focando na defesa contra sites maliciosos, spam e outras ameaças comuns. Já as soluções corporativas incluem pacotes de serviços exclusivos para empresas, capacitando-as a lidar com grandes volumes de dados e diversas variedades de ciberataques e Licença de Antivírus para equipamento do tipo servidor físico ou virtual para implementar os ativos do *Data Center* da SEPOG.
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 : 0035.003501/2023-45
UASG: 925373 **ENDEREÇO ELETRÔNICO :** https://www.gov.br/compras/pt-br.
VALOR ESTIMADO DA CONTRATAÇÃO

ORÇAMENTO ANUAL	R$ 279.388,50 (duzentos e setenta e nove mil trezentos e oitenta e oito reais e cinquenta centavos).
VISTORIA	**INSTRUMENTO CONTRATUAL**

Não	Contrato

DOCUMENTOS DE HABILITAÇÃO (INFORMAR ITEM DO ANEXO I)	
Requisitos Básicos: **1. Habilitação jurídica**: Conforme estabelecido no item 21 do Termo de Referência. **2. Qualificação econômico e financeira**: Conforme estabelecido no item 21.2 do Termo de Referência. **3. Regularidade Fiscal, social e trabalhista**: Conforme estabelecido no item 22 do Termo de Referência. **4. Qualificação técnica:** Conforme estabelecido no item 21.3 do Termo de Referência.	**Requisitos Específicos:**

CONTRATAÇÃO EXCLUSIVA ME/EPP?	**RESERVA COTA ME/EPP?**	**EXIGE AMOSTRA/DEMONSTRAÇÃO?**
Não	Não	Não
CRITÉRIO DE JULGAMENTO	**MODO DE DISPUTA**	**AQUISIÇÃO**
Menor Preço por Item	Aberto	Sim

TELEFONES PARA CONTATO	**E-MAIL PARA CONTATO:**
Telefone: 69.3212-9243	atendimento@supel.ro.gov.br

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

SUMÁRIO

1. DO PREÂMBULO

1.1. A SUPERINTENDÊNCIA ESTADUAL DE LICITAÇÕE S, por meio da **Portaria nº 29/2025/GAB/SUPEL**, publicada no DOE na data 14 de março de 2025, torna público que se encontra autorizada a realização da licitação na modalidade de **PREGÃO,** na forma **ELETRÔNICA, sob o nº 90428/2024/SUPEL/RO**, do tipo **MENOR PREÇO POR ITEM,** com o **Método de Disputa: ABERTO**, em conformidade com a Lei Federal nº. 14.133, de 2021 e Decreto Estadual nº 28.874/2024, a Lei Complementar nº 123/06 e Decreto Estadual nº 21.675/2017, e suas alterações, e demais legislações vigentes, tendo como interessado (a) **Secretaria de Estado de Planejamento, Orçamento e Gestão - SEPOG/RO.**

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

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

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

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

2. DO OBJETO

2.1. O objeto da presente licitação é a aquisição de um software antivírus para atender a estação de trabalho (usuários), baseando- se no fato de que o antivírus corporativo é um software de proteção contra ameaças cibernéticas, desenvolvido com mais recursos e robustez do que as soluções voltadas para dispositivos pessoais. Antivírus para usuários finais são mais simples, focando na defesa contra sites maliciosos, spam e outras ameaças comuns. Já as soluções corporativas incluem pacotes de serviços exclusivos para empresas, capacitando-as a lidar com grandes volumes de dados e diversas variedades de ciberataques e Licença de Antivírus para equipamento do tipo servidor físico ou virtual para implementar os ativos do *Data Center* da SEPOG, a fim de garantir uma proteção eficaz para um ambiente crítico e altamente ativo por um período de 36 (trinta e seis) meses, 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 4.3 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 4.4 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 n o item 4 e seus subitens e 26 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 no item 26.10 e 26.11 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 27 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 13.1 e subitens, 13.3 e subitens, 13.4 e seus subitens e 13.5.2 e seus 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 13.7 e subitens, 15 e 17 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 24.2 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 24.1 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 31 e subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

3. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

3.1. De acordo com o Art. 164, da Lei nº 14.133, de 2021, 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**:** atendimento@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, 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.

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 19 do Anexo I - Termo de Referência.

4.6.7 **Da subcontratação**: 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.

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 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos § 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021;

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

5.2.3. 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 20 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 inexequível.

7.7. O procedimento seguirá de acordo com o modo de disputa Aberto, conforme item 20.4 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/lotes 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 inexequibilidade da proposta de preço, será oportunizado ao licitante o Princípio do Contraditório e da Ampla Defesa, para que querendo esclareça a composição do preço da sua proposta, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, na forma do artigo 59 da Lei Federal n° 14.133/2021.

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

8.7. 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 20 e seus subitens 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)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 n° 11.802, de 28/11/2023.

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

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

9.13.1. 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 21.2 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 21.3 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. 7° da Constituição Federal.

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

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 JUL GAMENTO 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 25 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 de Planejamento, Orçamento e Gestão**, conforme estabelecido no item 14 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

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

ANEXO I - Termo de Referência (0058149249);

ANEXO II - Estudo Técnico Preliminar (0051127927);

ANEXO III - Mapa de Risco (0048233556);

ANEXO IV - SAMS (0052986162);

ANEXO V – Quadro Estimativo de Preços (0053169892);

Porto Velho-RO, 26 de março de 2025.

CAMILA CAROLINE ROCHA PERES

Pregoeira da/SUPEL/RO

Elaborado por:
Kelvin Klysman de Oliveira Leal
Membro da Comissão de Processamento e Apoio - SUPEL/RO
Portaria nº 29 /2025/GAB-SUPEL/RO

Revisado por:
Sidmar Wesley C. dos Santos
Membro da Comissão de Processamento e Apoio - SUPEL/RO
Portaria nº 29 /2025/GAB-SUPEL/RO

Documento assinado eletronicamente por **Camila Caroline Rocha Peres**, **Pregoeiro(a)**, em 26/03/2025, às 13:34, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **0057585856** e o código CRC **DDDA3832**.

Governo do Estado de
RONDÔNIA

GOVERNO DO ESTADO DE RONDÔNIA
Secretaria de Estado do Planejamento, Orçamento e Gestão - SEPOG

TERMO DE REFERÊNCIA

1. IDENTIFICAÇÃO

Unidade Orçamentária: Secretaria de Estado do Planejamento, Orçamento e Gestão-SEPOG.

Departamento: Assessoria de Tecnologia da Informação e Comunicação - ASTIC/DIREX/SEPOG/RO.

2. REQUISITOS LEGAIS

2.1. O presente Termo de Referência foi elaborado em atendimento aos regulamentos legais a seguir:

a) Constituição Federal;

b) Lei Federal nº 14.133/21 (Nova Lei de Licitações);

c) Decreto nº 28.874, DE 25 DE JANEIRO DE 2024 (Regulamenta a Lei nº 14.133/2021);

d) Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e,

e) Lei nº 12.527/2021 (Lei de Acesso à Informação).

2.2. **Da equipe de planejamento**

Portaria nº 279 de 14 de junho de 2024 (0049760241), de Comissão de Planejamento de Contratação de bens e serviços no âmbito da Secretaria de Estado Planejamento, Orçamento e Gestão - SEPOG.

3. MODELOS PADRONIZADOS

O modelo padrão utilizado foi o Termo de Referência (TR) para serviços de TIC da Secretaria de Estado do Planejamento, Orçamento e Gestão - SEPOG do processo Sei nº 0035.001852/2024-01, modelo este aprovado pela PGE-SEPOG, conforme Parecer 35 (0049449993).

4. CONDIÇÕES GERAIS DA CONTRATAÇÃO

4.1. **Do Objeto**

4.1.1. Aquisição de um software antivírus para atender a estação de trabalho (usuários), baseando- se no fato de que o antivírus corporativo é um software de proteção contra ameaças cibernéticas, desenvolvido com mais recursos e robustez do que as soluções voltadas para dispositivos pessoais. Antivírus para usuários finais são mais simples, focando na defesa contra sites maliciosos, spam e outras ameaças comuns. Já as soluções corporativas incluem pacotes de serviços exclusivos para empresas, capacitando-as a lidar com grandes volumes de dados e diversas variedades de ciberataques e Licença de Antivírus para equipamento do tipo servidor físico ou virtual para implementar os ativos do *Data Center* da SEPOG, a fim de garantir uma proteção eficaz para um ambiente crítico e altamente ativo por um período de 36 (trinta e seis) meses.

4.1.2. A contratação deve respeitar as especificações e condições estabelecidas neste Termo de Referência e no Anexo I da referida contratação.

4.2. **Do Objetivo**

4.2.1. A presente contratação visa garantir a proteção dos equipamentos da SEPOG contra ameaças virtuais, como URLs infectadas, spam, fraude, ataques de *phishing* e ameaças persistentes avançadas (APTs), é essencial. A exposição da infraestrutura tecnológica da SEPOG à internet aumenta a vulnerabilidade, tornando a aquisição das licenças uma medida essencial para garantir a proteção contra a rápida propagação de vírus e *malwares*. A continuidade do suporte e das atualizações do antivírus é vital para manter a eficácia do software na proteção dos ativos computacionais.

4.2.2. Destaca-se ainda a importância do antivírus na proteção contra o aumento exponencial de riscos associados ao crescente número de equipamentos e soluções digitais. A necessidade de aquisição de Antivírus é apresentada como uma premência iminente, alinhada ao Planejamento de Contratação Anual (PCA) e o Plano Plurianual (PPA) da SEPOG. A adoção de aquisição de Antivírus é justificada pela necessidade crítica de proteger os ativos computacionais da SEPOG contra as constantes ameaças cibernéticas, garantindo a continuidade dos serviços públicos e a segurança das informações.

4.3. **Das Especificações Técnicas/quantidade**

Item	Descrição	Especificação	Unid.	Quant.	CATMAT/CATSER
01	Antivírus - Estação de trabalho (usuários)	**ANEXO I (0051097159)**	Licença	200	27502
02	Licença de Antivírus para equipamento do tipo Servidor físico ou virtual por 36 meses (sendo 25 licenças por pacote)	**ANEXO I (0051097159)**	Pacote com 25 licenças (cada)	02	

4.4. **Das condições Gerais e Garantia do Serviço/Materiais**

4.4.1. Prover garantia de correção e atualização motivadas por falhas técnicas e mudanças pelo período mínimo de validade da licença, contados a partir da data de emissão da licença.

4.4.2. Caso a correção ou atualização exija nova licença, a empresa contratada deverá efetuar a nova emissão, no prazo de 3 (três) dias úteis, contados da data de notificação, sem ônus adicional para a SEPOG.

4.5. **Classificação dos bens comuns**

A aquisição que constitui o objeto deste Termo de Referência enquadram-se no conceito de *serviços comum* onde os requisitos técnicos são suficientes para determinar e ainda se verificou que este serviço é fornecido comercialmente por mais de uma empresa no mercado.

4.6. **Ciclo de vida do objeto**

Considerando o disposto no art. 6º, XXIII, c, da Lei nº 14.133/2021, referente ao ciclo de vida do objeto, destaca-se que, devido a natureza do serviço proposto, com um prazo inicial de 36 (trinta e seis) meses, sendo uma prática comum no mercado, o ciclo de vida do software é intrinsecamente limitado a esse período. É importante salientar que, conforme a necessidade e o interesse da administração, o contrato poderá ser prorrogado, desde que seja comprovada a vantajosidade dessa extensão.

A prorrogação do contrato além do período inicial de 36 (trinta e seis) meses estará condicionada à verificação de que a continuidade do software atende aos objetivos da SEPOG de maneira eficaz e econômica. Caso contrário, a administração terá a flexibilidade de explorar a possibilidade de contratar o software com outro fornecedor que ofereça condições mais vantajosas.

Essa abordagem assegura não apenas a conformidade com as diretrizes legais e normativas, mas também a adaptação à dinâmica do mercado e às necessidades em evolução da SEPOG, garantindo flexibilidade e oportunidade para buscar as soluções mais eficientes e adequadas ao longo do tempo.

5. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

Considerando o Estudo Técnico Preliminar-ETP (0051127927), a solução da proposta consiste na aquisição de softwares de Antivírus Corporativo para Estação de Trabalho (usuários) e para Equipamento Licença de Antivírus para equipamento do tipo Servidor físico ou virtual por 36 meses. Esta escolha é respaldada pela análise técnica e econômica, considerando os requisitos específicos do ambiente e dos usuários da SEPOG, conforme especificações abaixo:

ITEM 1: Antivírus Corporativo para Estação de Trabalho (usuários):

Licenciamento:

- Licenciamento válido por 36 meses;
- Inclui manutenções corretivas e atualizações sem custos adicionais para a Contratante, durante todo o ciclo de vida do software indicado pelo fabricante;
- Idioma deve ser em português.
- Acompanhar as inovações tecnológicas mais recentes.

Compatibilidade com os seguintes sistemas operacionais:

- Microsoft Windows Server 2008 R2;
- Microsoft Windows Server 2016;
- Microsoft Windows Server 2019;
- Microsoft Windows Server 2022;
- Microsoft Windows 7 (todas as edições, 32 e 64 bits);
- Microsoft Windows 8.1 (todas as edições, 32 e 64 bits);
- Microsoft Windows 10 (todas as edições, 32 e 64 bits).
- Microsoft Windows 11 (todas as edições, 32 e 64 bits).

Características:

- Possuir console de gerenciamento baseada no modelo cliente/servidor acessada WEB, todo o custo de instalação é por conta da contratada exceto sistemas operacional
- Deve permitir atribuição de perfis para os administradores da licença;

- Expirada sua validade o produto deverá permanecer funcional contra códigos maliciosos utilizando das definições até o momento da expiração da licença;,
- Possuir ferramenta de remoção de soluções antivírus próprio ou de outros fabricantes;
- Capacidade de instalar e desinstalar remotamente a licença de antivírus, com integração ao Active Directory, incluindo descobrimento de máquinas com ou sem agente;
- A console deve permitir visualizar o número total de licenças gerenciadas;
- A console deve ter a capacidade de gerar relatórios em HTML ou PDF, visualizar eventos e gerenciar políticas;
- Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
- Capacidade de desinstalar remotamente qualquer software da ferramenta nas máquinas cliente;
- Capacidade de definir diferentes políticas de configuração para grupos de estações;
- Capacidade de fornecer informações básicas sobre os computadores: se o antivírus está instalado, iniciado, atualizado, última conexão com o servidor administrativo, tempo desde a última atualização das vacinas, sistema operacional etc; Capacidade de enviar e-mail em caso de determinados eventos, como ocorrência de vírus etc;
- Capacidade de escolher quais módulos serão instalados em cada cliente ou grupo de clientes;
- Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis";
- Capacidade de agendar varreduras nos clientes;
- Capacidade de acesso remoto nos clientes;
- Prover segurança para estações de trabalho, sejam físicas ou em ambiente virtualizado;
- Possuir console de gerenciamento que permita realizar configurações do antivírus, antispyware, firewall, detecção de intrusão, controle de dispositivos e controle de aplicações;
- O produto deverá ter a capacidade de remoção do software de antivírus já instalado e ser instalado de forma remota pela console de gerenciamento;
- As licenças não deve fazer distinção de servidor (Windows Server, File Serve, Linuz) e estação de trabalho.
- As licenças do antivírus deverá ser a última versão do mercado.

ITEM 2: Licença de Antivírus para equipamento do tipo Servidor físico ou virtual por 36 meses:

SOLUÇÃO DE DECTEÇÃO E RESPOSTA

Características:

- O antivírus deve conter políticas de segurança e playbooks básicos pré-definidos, sem que haja a necessidade de criação manual;
- O antivírus deve possuir integração nativa com soluções de controle de acesso;
- O antivírus deve possuir integração nativa com soluções de SIEM (Security Information and Event Management);
- O antivírus deve possuir integração nativa com soluções de firewall;
- O antivírus deve permitir o isolamento de um dispositivo através da integração de um NAC de acordo com a categoria do evento detectado;
- O antivírus deve permitir adicionar endereços IP maliciosos detectados em um ou mais firewalls remotos integrados;
- O antivírus deve exigir que uma senha seja desabilitada por aplicativo de terceiros;
- O antivírus deve permitir a configuração de perfis nas informações coletadas para a função de pesquisa de ameaças;
- O antivírus deve permitir exclusões de informações que não serão coletadas na função de pesquisa de ameaças;
- O antivírus deve ser certificada pela Microsoft como uma licença de antivírus e ser capaz de se integrar com o Windows Security Center;
- O antivírus deve entregar informações geradas pelos serviços de inteligência na nuvem para a tomada de decisão sobre um evento detectado;
- O antivírus deve permitir que os serviços em nuvem recategorizem uma classificação de evento;
- O antivírus deve permitir que os administradores desabilitem as notificações para um evento de descoberta;
- O antivírus deve permitir que as funções de filtragem da web sejam realizadas bloqueando o acesso a páginas da web categorizadas como maliciosas;
- O antivírus deve identificar e prevenir tentativas de elevação de privilégios;
- O antivírus deve bloquear ataques de ransomware conhecidos;
- O antivírus deve ter a capacidade de descobrir dispositivos IOT não gerenciados na rede;
- O antivírus deve ter a capacidade de detectar dispositivos não gerenciados e protegidos pela licença com sistemas operacionais Linux e Windows.

CARACTERÍSTICAS DA CONSOLE DE ADMINISTRAÇÃO:

- A console de gerenciamento deve permitir a integração com o “Active Directory” para garantir o cumprimento dos requisitos da política de senhas da organização;
- A console de gerenciamento deve permitir o uso de autenticação de dois fatores (2FA);
- A console de gerenciamento deve permitir a integração com SAML para autenticação de usuários;
- A console de gerenciamento deve permitir o uso de funções granulares para administradores;
- A console de gerenciamento deve permitir o gerenciamento por meio de API;
- A console de gerenciamento deve permitir a visualização dos eventos registrados nos dispositivos que requeiram atenção;
- A console de gerenciamento deve permitir a visualização do estado dos agentes instalados;
- A console de gerenciamento deve permitir a desinstalação remota do agente instalado nos dispositivos;
- A console de gerenciamento deve permitir a desativação/ativação remota do agente instalado nos dispositivos;
- A console de gerenciamento deve permitir a criação de relatórios executivos contendo um resumo que descreva os eventos de segurança e o status do sistema;
- A console de gerenciamento deve permitir a criação de grupos organizacionais de dispositivos nos quais cada grupo possa ter regras de proteção independentes dos demais;
- A console de gerenciamento deve permitir a exportação dos logs locais gerados pelos agentes;
- A console de gerenciamento deve permitir a criação de relatórios de inventário dos agentes contendo informações como: Endereço IP, Nome do Host, Sistema Operacional, Endereço MAC, Versão do Agente, Status do Agente;
- A console de gerenciamento deve ter visibilidade dos eventos gerados pelos dispositivos ou eventos de acordo com o processo executado;
- A console de gerenciamento deve permitir a integração de um SMTP externo para envio de alertas por e-mail;
- A console de gerenciamento deve permitir auditorias de alterações feitas por administradores/operadores. Essas auditorias também devem poder ser exportadas em formato CSV.

CARACTERÍSTICAS DO AGENTE DE PROTEÇÃO:

O antivírus deve ser compatível com os seguintes sistemas operacionais:

- Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 e 2022;
- RedHat Enterprise Linux e CentOS 6.8 ou superior, 7.2 ou superior, 8 ou superior e 9 ou superior;
- Ubuntu Server 16.04, 18.04, 20.04 e 22.04;
- Oracle Linux 6.10, 7.7 ou superior e 8.2 ou superior.
- O antivírus deve ser compatível com ambientes de Virtual Desktop Infrastructure (VDI) em VMware Horizons 6 e 7 e Citrix XenDesktop 7;
- O antivírus deve ter um consumo máximo de 350 MB de memória RAM;
- O antivírus deve ter um consumo médio de menos de 2% do uso da CPU;
- O antivírus deve ter a capacidade de atualizar o agente sem interação do usuário e sem exigir uma reinicialização;
- O antivírus deve ter proteção “anti-violação” no agente;
- O antivírus deve funcionar sem depender de assinaturas hash locais conhecidas para a detecção de arquivos maliciosos;
- O antivírus deve ser capaz de registrar em tempo real informações do processo e informações adicionais;
- O antivírus deve ter a opção de definir uma senha para desinstalar o agente;
- O antivírus deve ser capaz de gerar um instalador para Windows pré-configurado. Esta configuração deve permitir a instalação sem a necessidade de interação ou configuração por parte do usuário;
- O agente deve ser capaz de funcionar através de um proxy.
- FUNCIONALIDADES DE DETECÇÃO DE MALWARE
- O antivírus deve ser capaz de funcionar no modo “offline” sem que o agente esteja conectado à rede corporativa;
- O antivírus deve ser capaz de detectar, eliminar e retornar ao seu valor inicial as alterações feitas por processos maliciosos no registro do Windows;
- O antivírus deve ser capaz de detectar conexões de rede a partir do dispositivo;
- O antivírus deve ser capaz de incorporar inteligência de ameaças ao esquema de detecção;
- O antivírus deve ser capaz de incorporar as técnicas do MITRE ATT&CK no esquema de detecção e mostrar quais dessas técnicas foram utilizadas;
- O antivírus deve ter a capacidade de pesquisar ameaças em Sistema Operacional Windows usando indicadores de comprometimento (IOC), como: nome, hash e ações relacionadas a arquivos (Criação, Exclusão, Renomear);

- O antivírus deve ter a capacidade de pesquisar ameaças em Sistema Operacional Windows usando indicadores de comprometimento (IOC), como ações relacionadas a processos (Terminação de Processo, Criação de Processo, Carregamento de Executáveis)
- O antivírus deve ter a capacidade de pesquisar ameaças em Sistema Operacional Windows usando indicadores de comprometimento (IOC), como ações relacionadas ao uso da rede (Socket Connect, Socket Close, Socket Brind);
- O antivírus deve ter a capacidade de pesquisar ameaças em Sistema Operacional Windows usando indicadores de comprometimento (IOC), como ações relacionadas log de eventos;
- O antivírus deve ter a capacidade de pesquisar ameaças em Sistema Operacional Windows usando indicadores de comprometimento (IOC), como ações relacionadas ao registro do Sistema Operacional (criação de chave, exclusão de chave, conjunto de valores);
- O antivírus deve ter a capacidade de realizar consultas para filtrar as informações disponíveis para pesquisa de ameaças;
- O antivírus deve ter capacidade de armazenar pesquisas realizadas para serem reutilizadas no futuro;
- O antivírus deve ter a capacidade de agendar pesquisas armazenadas;
- O antivírus deve identificar atividades maliciosas conhecidas;
- O antivírus deve ter a capacidade de receber atualizações diárias de inteligência;
- O antivírus deve ter a capacidade de classificar os eventos detectados em diferentes categorias.

FUNCIONALIDADES DE PREVENÇÃO DE MALWARE:

- O antivírus deve ter a capacidade de prevenir a execução de arquivos maliciosos;
- O antivírus deve incorporar mecanismo de proteção baseado no kernel do sistema operacional, com capacidade de “Aprendizado de Máquina” (Machine Learning);
- O antivírus deve ter a capacidade de controlar dispositivos USB;
- O antivírus deve ter a capacidade de criar exceções para dispositivos USB com base no nome do dispositivo;
- O antivírus deve ter a capacidade de criar exceções para dispositivos USB com base no fornecedor do dispositivo;
- O antivírus deve ter a capacidade de criar exceções para dispositivos USB com base no número de série do dispositivo;
- O antivírus deve ter a capacidade de criar exceções para dispositivos USB com base em uma combinação de: nome do dispositivo, fornecedor, número de série;
- O antivírus deve ser capaz de bloquear o tráfego malicioso de exfiltração de dados;
- O antivírus deve ser capaz de bloquear tráfego de comunicação malicioso para C&C (Comando e Controle);
- O antivírus deve ser capaz de impedir violações de segurança e tentativas de ransomware em tempo real;
- O antivírus deve ser capaz de evitar a criptografia causada por ransomware e modificação de arquivos ou registro de dispositivos. Caso isso ocorra, a licença deverá restaurar os arquivos afetados/modificados para o seu estado original em tempo real;
- O antivírus deve permitir que as políticas nela contidas sejam modificadas permitindo vários estados tais como: ativo, inativo ou apenas criar “logs”;
- O antivírus deve ser capaz de ser configurada em modo onde nenhum bloqueio é feito, mas todas as atividades maliciosas são registradas;
- O antivírus deve ser capaz de permitir a modificação das regras de detecção de eventos maliciosos de forma que essas regras apenas armazenem um registro ou fiquem em modo de bloqueio;
- O antivírus deve ser capaz de permitir verificações periódicas dos arquivos contidos nos dispositivos com o agente instalado.
- FUNCIONALIDADES DE DIFUSÃO (PÓS-INFECÇÃO)
- O antivírus deve permitir o isolamento automático do tráfego de rede de um dispositivo onde foi encontrada atividade causada por malware
- O antivírus deve permitir alterar as políticas atribuídas de um dispositivo onde foi encontrada atividade causada por malware;
- O antivírus deve permitir o bloqueio de atividades realizadas por arquivos maliciosos;
- O antivírus deve ter a capacidade de criar exceções para processos com base na localização do arquivo (caminho do arquivo);
- O antivírus deve ter a capacidade de criar exceções para processos com base no destino do tráfego gerado por este;
- O antivírus deve ter a capacidade de criar exceções para os processos baseados no usuário que o executou;
- O antivírus deve ter a capacidade de criar exceções manualmente para falsos positivos e evitar a ocorrência de ocorrências futuras;
- O antivírus deve ter a capacidade de reclassificar automaticamente a atividade como um falso positivo e evitar a ocorrência de detecções semelhantes;
- O antivírus deve permitir a criação de exceções de eventos com base em endereços IP, aplicações e protocolos.

FUNCIONALIDADES DE RESPOSTA A INCIDENTE:

- O antivírus deve armazenar metadados gerados pelos dispositivos para que possam ser usados em investigações forenses;
- O antivírus deve permitir a integração com soluções de SIEM através de um syslog;
- O antivírus deve ter a capacidade de obter instantâneos ou “dumps” de memória que permitam a realização de processos forenses;
- O antivírus deve ter a capacidade de abrir tickets em plataformas de gerenciamento como ServiceNow e JIRA;
- O antivírus deve permitir a integração através de API onde tem a capacidade de entregar informações geradas em um evento como: endereço IP, nome do host, usuário, data/hora ocorrida, atividade suspeita etc.;
- O antivírus deve ter a capacidade de encerrar um processo com base em sua classificação;
- O antivírus deve ter a capacidade de excluir um arquivo com base em sua classificação;
- O antivírus deve ter a capacidade de restaurar as configurações de registro básicas com base na classificação de atividade predefinida;
- O antivírus deve ter a capacidade de isolar os dispositivos infectados da rede;
- O antivírus deve ter a capacidade de restringir automaticamente o acesso do dispositivo à rede de acordo com a classificação do processo detectado;
- O antivírus deve obter visibilidade total da cadeia de ataques e alterações maliciosas;
- O antivírus deve permitir a limpeza automática do dispositivo e reverter alterações maliciosas, mantendo o tempo de atividade do dispositivo;
- O antivírus deve permitir o envio de executáveis para análise em um sandbox, a fim de determinar se são maliciosos ou inofensivos;
- O antivírus deve possuir integração com Active Directory a fim de possibilitar a utilização de playbooks para resposta a incidentes de segurança;
- O antivírus deve fornecer vários mecanismos de proteção, incluindo o encerramento de um processo, a exclusão de um arquivo malicioso e o bloqueio de uma conexão de rede.
- FUNCIONALIDADES DE CONTROLE DE VULNERABILIDADES E COMUNICAÇÃO
- O antivírus deve ter a capacidade de descobrir aplicativos que estão se comunicando através da rede e que representam risco para o dispositivo;
- O antivírus deve ter capacidade para realizar um patch virtual, através da restrição de acessos nas aplicações vulneráveis
- O antivírus deve permitir a redução das superfícies de ataque utilizando políticas de comunicação proativas baseadas no risco de acordo com o CVE e a qualificação ou reputação que uma aplicação possa ter;
- O antivírus deve ter a capacidade de impedir que aplicativos não autorizados se comuniquem pela rede;
- O antivírus deve ter a capacidade de criar políticas que tenham a capacidade de impedir a comunicação de aplicativos de acordo com a versão do aplicativo instalado;
- O antivírus deve ser capaz de detectar e identificar todas as aplicações nos dispositivos que se comunicam na rede;
- O antivírus deve ser capaz de fornecer informações sobre o uso de aplicativos de rede mostrando, por exemplo, quais dispositivos geram tráfego para um aplicativo e os destinos IP do tráfego gerado pelo aplicativo.
- O antivírus de referência adotada nesta especificação técnica se baseia no modelo FortiEDR;

A citação do modelo se pauta na necessidade da oferta dos licitantes ser totalmente integrada com os ativos FORTINET presentes em nosso ambiente, composto de diversas soluções da referida fabricante.

6. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

6.1. DO PROBLEMA

O antivírus desempenha um papel necessário na proteção contra vírus, malware e trojans, essencial para garantir a continuidade dos serviços e a segurança das informações. O problema central é a necessidade urgente de reforçar a proteção dos ativos computacionais da SEPOG contra as ameaças digitais em constante evolução.

6.2. Motivação/Justificativa

A aquisição de um software antivírus na SEPOG (Secretaria de Planejamento e Gestão) é de extrema importância por várias razões, especialmente no contexto da proteção de dados pessoais e sensíveis, conforme estabelecido pela LGPD (Lei Geral de Proteção de Dados). Além disso, a conformidade com as normas da CIS (Center for Internet Security), como o CONTROL 8, e as normas da ABNT (Associação Brasileira de Normas Técnicas) são fundamentais para garantir a segurança da informação.

Abaixo segue algumas razões demonstrando a importância da aquisição:

6.3. Proteção de Dados Pessoais e Sensíveis (LGPD):

A LGPD estabelece diretrizes específicas para a proteção de dados pessoais, exigindo que as organizações implementem medidas adequadas para garantir a segurança e a privacidade desses dados. Um software antivírus é uma medida fundamental para proteger os sistemas e os dados armazenados pela SEPOG contra ameaças cibernéticas, como malware, ransomware e phishing, que podem comprometer a segurança dos dados pessoais e sensíveis.

6.4. CIS CONTROL 8:

O CIS CONTROL 8 estabelece diretrizes para a gestão de vulnerabilidades e ameaças, incluindo a implementação de controles de antivírus e anti-malware. Ao adquirir um software antivírus, a SEPOG estará em conformidade com aspectos deste controle, garantindo uma abordagem proativa para proteger seus sistemas contra ameaças conhecidas e emergentes.

6.5. Normas da ABNT:

As normas da ABNT relacionadas à segurança da informação, como a NBR ISO/IEC 27001, fornecem diretrizes para estabelecer implementar, manter e melhorar um sistema de gestão de segurança da informação (SGSI). A aquisição de um software antivírus é uma medida que pode ser implementada como parte desse SGSI, ajudando a garantir a segurança dos sistemas e dos dados da SEPOG de acordo com as melhores práticas estabelecidas pela ABNT.

6.6. Prevenção de Incidentes de Segurança:

Um software antivírus eficaz é essencial para prevenir incidentes de segurança, como ataques de malware e violações de dados, que podem ter sérias consequências para a SEPOG, incluindo danos à reputação, perda de dados confidenciais e interrupção das operações. Ao investir em uma licença de antivírus robusta, a SEPOG está fortalecendo suas defesas cibernéticas e reduzindo o risco de incidentes de segurança.

Em resumo, a aquisição de um software antivírus na SEPOG é crucial para proteger os dados, garantir a conformidade com regulamentações como a LGPD e as normas da CIS e da ABNT, e prevenir incidentes de segurança que possam comprometer a integridade e a disponibilidade dos sistemas e das informações da organização.

6.7. A pretendida contratação está prevista no PCA 2024 Portaria 481 (0044244035).

PCA	PROCESSO	PORTARIA
2024	0035.001708/2023-85	481 (0044244035)

7. ESTIMATIVA DO VALOR E DA QUANTIDADE DA CONTRATAÇÃO

7.1. **Estimativa do valor**

7.1.1. A memória de cálculo para obtenção do valor para a contratação foi realizado pelo Núcleo de Contratos e Licitações - NCL/SEPOG, conforme demonstrado nas propostas (0051302145/0051032413/0051752611) e cotação no banco de preços (0047909420) perfazendo um valor total de R$211.146,00 (duzentos e onze mil, cento e quarenta e seis reais), para 36 (trinta e seis) meses.

Item	Descrição	Unid.	Quant.	Valor Unitário	Valor Total
01	Antivírus - Estação de trabalho pelo período de 36 meses	Licença	200	R$324,20	R$64.840,00
02	Licença de Antivírus para equipamento do tipo Servidor físico ou virtual pelo período de 36 meses (sendo 25 licenças por pacote)	Licença	02	R$73.153,00	R$146.306,00

7.1.2. No item 2, o produto é ofertado em pacote de 25 licenças, justificando assim o quantitativo de 2 unidades, totalizando as 50 licenças, com um valor total de R$211.146,00 (duzentos e onze mil, cento e quarenta e seis reais).

7.2. **A vantajosidade da compra de 50 licenças para servidor na opção de 36 meses, é essencial a considerar alguns pontos estratégicos:**

1. **Economia a Longo Prazo:** A aquisição para 36 meses representa uma economia em relação às renovações anuais ou bienais. Considerando que o custo total para 12 meses é R$ 48.769,00 (quarenta e oito mil, setecentos e sessenta e nove reais), a cada renovação anual o valor total ao longo de três anos seria de R$ 146.307,00 (cento e quarenta e seis mil, trezentos e sete reais). O custo para 24 meses é de R$ 97.583,00 (noventa e sete mil, quinhentos e oitenta e três reais), o que, se renovado, também resultaria em um valor superior à opção de 36 meses. Optando pela contratação direta por 36 meses ao valor de R$ 146.306,00 (cento e quarenta e seis mil, trezentos e seis reais), evita-se um aumento potencial de custos por conta de reajustes anuais.
2. **Proteção Contra Reajustes:** A contratação de licenças por um período mais longo protege o governo de possíveis reajustes de preços no mercado, que podem ocorrer por inflação, variações cambiais ou mudanças nas políticas de preços dos fornecedores.
3. **Planejamento Orçamentário:** Optar pelo contrato de 36 meses facilita o planejamento orçamentário, pois permite fixar um valor conhecido e evitar surpresas financeiras em futuros exercícios. Isso é particularmente vantajoso para a administração pública, onde a previsibilidade de despesas é crucial.
4. **Redução de Custos Operacionais e Administrativos:** A renovação de contratos anualmente ou bienalmente implica custos administrativos adicionais, incluindo tempo de análise, elaboração de documentos e processos de aprovação. Ao escolher o contrato de 36 meses, esses custos são significativamente reduzidos.
5. **Continuidade do Serviço:** A contratação por um período mais longo garante a continuidade do serviço, evitando possíveis interrupções que poderiam ocorrer durante processos de renovação ou aquisição de novas licenças.

7.3. Portanto, a escolha do contrato de 36 meses é mais vantajosa tanto do ponto de vista econômico quanto do operacional, alinhando-se com os princípios de economicidade e eficiência que norteiam a administração pública.

7.4. **Estimativa da quantidade:**

7.4.1. As quantidades levantadas são justificadas pela quantidade atual de licenças já aplicadas em servidores da SEPOG. A aquisição é necessária para manter esse quantitativo para garantir uma cobertura eficiente para as necessidades da instituição.

7.4.2. Esta estimativa reflete o compromisso da SEPOG em assegurar a continuidade operacional, a proteção eficaz contra ameaças cibernéticas e a adaptação às crescentes demandas tecnológicas, reafirmando o comprometimento com a segurança e eficiência em sua infraestrutura computacional.

Item	Descrição	Unid.	Quant.
01	Antivírus - Estação de trabalho pelo período de 36 meses	Licença	200
02	Licença de Antivírus para equipamento do tipo Servidor físico ou virtual pelo período de 36 meses	Licença	50

8. DA PLANILHA DE COMPOSIÇÃO DE CUSTOS E FORMAÇÃO DE PREÇOS

8.1. Justifica-se não utilizar a planilha de Composição de Custos e Formação de Preços no processo de contratação do Antivírus pelas seguintes razões:

1. Natureza do Produto:

O Antivírus é um serviço de aquisição de licenças que possui preços fixos e pré-determinados, diferentemente de serviços ou produtos que requerem uma análise detalhada de insumos, mão-de-obra e outros componentes variáveis.

2. Simplificação do Processo:

Utilizar uma planilha de Composição de Custos para um produto com preço fixo e já consolidado no mercado adiciona uma complexidade desnecessária ao processo de contratação. O foco deve ser na avaliação de conformidade com as especificações técnicas e de serviço, bem como na garantia de suporte e manutenção oferecidos.

3. Do pagamento:

O modelo de contrato possui o pagamento em *upfront* (pagamento único antecipado), o fornecimento do *software* antivírus é caracterizado como um serviço padronizado e contínuo, essencial para a operação dos sistemas estruturantes de tecnologia da informação. Neste caso poderia ser pago mensalmente, anualmente ou no inicio do contrato sendo este ultimo economicamente mais vantajoso para administração. Dada essa natureza, a utilização de uma planilha detalhada de custos com itens, insumos, serviços, custos unitários, verbas e reflexos se torna redundante e desnecessária.

4. Da possibilidade de prorrogação do contrato:

O contrato de fornecimento de software antivírus tem a possibilidade de ser prorrogado conforme a legislação vigente, podendo alcançar uma vigência máxima de 15 anos, conforme o Artigo 114, da Lei nº 14.133 de 01 de Abril de 2021. Isso deve ser levado em consideração para uma melhor negociação de preço, já que a continuidade e a estabilidade do serviço ao longo do tempo podem proporcionar condições comerciais mais vantajosas.

5. Transparência e Comparabilidade:

No caso de soluções SaaS (Software as a Service) como o Antivírus, a comparabilidade entre propostas se dá através de funcionalidades, suporte e condições de serviço adicionais, e não através da decomposição de custos. Todos os licitantes oferecem o mesmo produto com o mesmo preço base, o que já garante uma transparência intrínseca ao processo.

6. Eficiência Administrativa:

A não utilização de uma planilha de Composição de Custos para o Antivírus torna o processo mais ágil e eficiente. A administração pode se concentrar na avaliação de outros critérios importantes, como a adequação da solução às necessidades da organização, a confiabilidade do fornecedor, as condições de pagamento e os termos de serviço.

7. Conformidade com Práticas de Mercado:

O mercado de software segue práticas de comercialização diferenciadas, onde os preços são amplamente divulgados e padronizados. A exigência de uma planilha detalhada pode não estar alinhada com estas práticas e pode até dificultar a atração de fornecedores qualificados que já operam sob um modelo de preço fixo e transparente.

Portanto, ao simplificar a composição de custos e focar na eficiência do processo de contratação, é possível assegurar que a administração pública obtenha um serviço de alta qualidade, mantendo a transparência e o controle necessário, sem sobrecarregar o processo com detalhamentos excessivos que não agregam valor significativo à contratação de um produto já amplamente padronizado e de mercado.

9. REQUISITOS DA CONTRATAÇÃO

9.1. **Necessidade de Negócio**

ID	DESCRIÇÃO DA NECESSIDADE DE NEGÓCIO	PROPOSTAS
1	Ampliar a disponibilidade dos serviços de TI;	Garantir a continuidade operacional por meio da renovação, aproveitando a estrutura já existente do antivírus para uma implementação eficiente
2	Proteção contra malware nas estações de trabalho.	Reforçar a defesa contra malware, utilizando o conhecimento adquirido com o antivírus, otimizando sua configuração para melhor performance
3	Proteção contra malware nos servidores.	Fortalecer a segurança dos servidores aproveitando a experiência adquirida com o antivírus, maximizando sua eficácia na proteção.
4	Filtragem de conteúdos maliciosos.	Aprimorar a capacidade de filtragem, utilizando a experiência acumulada para otimizar a identificação e bloqueio de conteúdos maliciosos.
5	Bloqueio de sites suspeitos.	Implementar recursos avançados para identificar e bloquear acessos a sites suspeitos, aproveitando a base de conhecimento.
6	Restrição ao acesso de dispositivos infectados	Reforçar medidas de segurança para restringir o acesso de dispositivos externos, como pendrives e cartões de memória.
7	Prevenção de fraudes em movimentações financeiras.	Aprimorar as funcionalidades antifraudes para proteger as movimentações financeiras, aproveitando o conhecimento acumulado.
8	Proteção contra vazamento de informações e perda de dados.	Reforçar as camadas de proteção visando evitar vazamentos de informações sensíveis e perda de dados.
9	Suporte técnico e atualização por 36 meses.	Garantir suporte técnico contínuo e atualizações regulares da base de dados ao longo de 36 meses.

9.2. **Necessidade Tecnológica**

ID	DESCRIÇÃO DA NECESSIDADE TECNOLÓGICA	PROPOSTAS
1	Console de Gerenciamento (Centralizado).	Aprimorar o console de gerenciamento centralizado para proporcionar uma interface mais intuitiva e eficiente
2	Gerenciamento por Grupos (Integração com AD).	Reforçar a integração com o Active Directory (AD) para um gerenciamento mais eficaz e segmentado por grupos de usuários
3	Anti-Malware/Anti-Virus	Manter e aprimorar as capacidades antivírus e antimalware para garantir uma proteção abrangente contra ameaças digitais
4	Anti-Ransomware.	Reforçar as defesas contra ransomware, incorporando tecnologias avançadas para prevenir e combater ataques deste tipo de malware
5	IPS host	Implementar um Sistema de Prevenção de Intrusões (IPS) no nível do host para detectar e bloquear atividades maliciosas em tempo real
6	IDS host	Introduzir um Sistema de Detecção de Intrusões (IDS) no nível do host para identificar padrões de comportamento suspeitos nas estações
7	Firewall host	Fortalecer as funcionalidades do firewall no nível do host para controlar o tráfego e impedir acessos não autorizados aos dispositivos
8	Filtro de conteúdo Web (Classificação de Site)	Aprimorar o filtro de conteúdo web para uma classificação mais precisa de sites, fortalecendo a segurança contra ameaças online
9	Suporte a Windows e Linux	Garantir pleno suporte para ambientes Windows e Linux, assegurando uma proteção consistente em todas as plataformas utilizadas pela SEPOG

10	Proteção para licença de email (Microsoft Exchange)	Reforçar a proteção contra ameaças em soluções de e-mail, especialmente no ambiente Microsoft Exchange, para prevenir ataques direcionados
11	Proteção para licença de Diretório (AD)	Intensificar a proteção para soluções de diretório, como o Active Directory, para mitigar possíveis ameaças que visam comprometer a infraestrutura centra
12	Gerenciamento de vulnerabilidades e correções	Implementar um sistema eficaz de gerenciamento de vulnerabilidades, permitindo a aplicação rápida de correções para reduzir exposições a ameaças
13	Integração com soluções de SIEM	Aperfeiçoar a integração com soluções de Segurança de Informações e Gerenciamento de Eventos (SIEM) para uma resposta coordenada a incidentes
14	Controle de Dispositivos (USB)	Reforçar o controle sobre dispositivos USB, garantindo restrições e monitoramento efetivo para prevenir potenciais ameaças externas
15	Proteção proativa contra ameaças desconhecidas	Incorporar tecnologias proativas para identificação e bloqueio instantâneo de ameaças desconhecidas, elevando a resiliência contra ataques
16	Monitorar o comportamento dos aplicativos	Aprimorar a capacidade de monitoramento do comportamento dos aplicativos, identificando atividades suspeitas em tempo rea
17	Interromper atividades prejudiciais em tempo real	Implementar mecanismos para interromper instantaneamente atividades potencialmente prejudiciais, garantindo uma resposta rápida a ameaças
18	Sensores para coleta de dados comportamentais	Utilizar sensores para coletar dados comportamentais dos dispositivos endpoint, permitindo uma análise abrangente para identificação de potenciais ataques
19	Monitorar pastas protegidas contra gravação não autorizada	Reforçar a monitorização de pastas protegidas, impedindo gravações não autorizadas para evitar perda ou comprometimento de dados sensíveis.

9.3. **Demais requisitos necessários e suficientes à escolha da solução de TIC**

Nº	Necessidades	Descrição
1	Lei Geral de Proteção de Dados Pessoais	Ser adequada a Lei Geral de Proteção de Dados

9.4. **Requisitos de Implantação**

Os serviços deverão ser entregues no e-mail suporte@sepog.ro.gov.br com os certificados e os procedimentos necessários para sua ativação, a empresa deve dar total suporte no idioma português durante todo o processo de ativação.

10. JUSTIFICATIVA DE PARCELAMENTO OU NÃO DO OBJETO

Durante o Estudo Técnico Preliminar (0051127927), ao avaliar a vantajosidade econômica em confronto com as características técnicas necessárias, decidiu-se fracionar o objeto em dois itens: **Item 01:** uma licença corporativa de antivírus para as estações de trabalho e **Item 02:** licença de antivírus mais robusta para os sistemas críticos da SEPOG, do tipo servidor físico ou virtual.

Esse fracionamento foi realizado para garantir a melhor proteção possível, considerando as diferentes necessidades e níveis de criticidade dos sistemas envolvidos.

Uniformidade do software antivírus:

A uniformidade do software antivírus é essencial para assegurar uma proteção eficaz contra ameaças cibernéticas. Dividir ainda mais as licenças entre diferentes fornecedores comprometeria essa uniformidade, criando potenciais conflitos de compatibilidade e gerenciamento que poderiam reduzir a eficácia da segurança implementada.

Gerenciamento Centralizado:

Um único ponto focal de gerenciamento é crucial para a administração eficiente das políticas de segurança, atualizações e monitoramento de eventos. A utilização de consoles de gerenciamento distintas para diferentes soluções de antivírus resultaria em complexidade administrativa, aumento da carga de trabalho e potenciais falhas na gestão da segurança.

Integração e Compatibilidade:

Assegurar a integração e compatibilidade de diferentes sistemas de antivírus é uma tarefa complexa que pode introduzir vulnerabilidades na infraestrutura de TI. A segmentação atual de software antivírus para estações de trabalho e outra para sistemas críticos, já considera essas questões, e uma divisão adicional não seria viável.

Eficiência e Efetividade:

A contratação de software antivírus para estações de trabalho e uma licença robusta para sistemas críticos assegura a eficiência e efetividade na proteção cibernética. Isso facilita o suporte técnico, a implementação de atualizações e a manutenção contínua dos sistemas de segurança.

Licenças para Estação de Trabalho e Servidores:

A segmentação realizada, diferenciando licenças para estações de trabalho e para servidores, atende às necessidades técnicas específicas de cada ambiente. Essa divisão já representa o máximo nível de segmentação viável, garantindo a proteção adequada e a gestão eficiente dos sistemas.

Impossibilidade de Segmentação Adicional:

Segmentar ainda mais as licenças não é possível, pois isso fragmentaria a segurança, tornando-a menos eficaz e mais difícil de administrar. Manter a segmentação atual é crucial para garantir a integridade e a eficácia da proteção cibernética oferecida.

Portanto, o parcelamento do objeto foi cuidadosamente considerado durante o Estudo Técnico Preliminar (0051127927). A decisão de dividir as licenças em duas partes, uma para estações de trabalho e outra para sistemas críticos, ou seja, licenças para equipamento do tipo Servidor físico ou virtual, foi tomada para assegurar a melhor proteção e gestão possíveis. Qualquer segmentação adicional comprometeria a uniformidade e a eficiência das licenças, tornando-a inviável para a administração pública. Portanto, a segmentação atual deve ser mantida para garantir a proteção integral dos sistemas e dados institucionais.

11. APLICAÇÃO DO ART. 8º DO DECRETO ESTADUAL 21.675/2017 – COTA ME/EPP

A não aplicação de cota para Microempresas (ME) e Empresas de Pequeno Porte (EPP) na contratação de software antivírus pode ser justificada pelas particularidades técnicas e operacionais envolvidas, tais como:

Uniformidade do Antivírus:

O uso de software antivírus exige uniformidade para garantir a eficácia na proteção contra ameaças cibernéticas. Ter duas empresas diferentes operando simultaneamente pode criar conflitos de compatibilidade e gerenciamento, resultando em uma potencial redução na eficácia da proteção oferecida.

Gerenciamento Centralizado:

Um software antivírus geralmente inclui uma console de gerenciamento centralizado que permite a administração de políticas de segurança, atualizações e monitoramento de eventos de segurança. A utilização de duas empresas diferentes pode complicar a gestão, aumentar a carga administrativa e criar pontos de falha, comprometendo a segurança da infraestrutura de TI.

Integração e Compatibilidade:

A integração de diferentes sistemas de antivírus pode ser complexa e suscetível a problemas de compatibilidade. Isso pode levar a lacunas na proteção e dificultar a resposta rápida a incidentes de segurança, algo crucial em um ambiente de TI.

Eficiência e Efetividade:

A contratação de software antivírus, fornecido por um único fornecedor, assegura a eficiência e a efetividade na gestão da segurança cibernética. Isso facilita o suporte técnico, a implementação de atualizações e a manutenção contínua do sistema.

12. VANTAGENS E BENEFÍCIOS A SEREM ALCANÇADOS

12.1. **Segurança Aprimorada**: A implementação de software antivírus atualizada e mais eficaz garantirá uma proteção mais robusta contra as ameaças cibernéticas, reduzindo o risco de comprometimento da infraestrutura e dos dados da SEPOG.

12.2. **Continuidade dos Serviços**: Ao proteger os ativos computacionais contra vírus e malwares, a SEPOG pode manter a continuidade dos serviços essenciais oferecidos à população, evitando interrupções indesejadas devido a incidentes de segurança.

12.3. **Proteção de Dados Sensíveis**: O software antivírus de proteção contribuirá para a preservação da integridade, confidencialidade e disponibilidade das informações sensíveis gerenciadas pela SEPOG, garantindo sua segurança contra acessos não autorizados.

12.4. **Redução de Riscos e Custos**: Ao mitigar o risco de ataques cibernéticos e possíveis consequências, como perda de dados ou danos à reputação da instituição, a SEPOG pode evitar custos associados à recuperação de incidentes de segurança e possíveis multas por não conformidade com regulamentações.

12.5. **Conformidade com Normas e Regulamentações**: A implementação de software antivírus de proteção atualizada pode ajudar a SEPOG a manter a conformidade com as regulamentações de segurança de dados e privacidade, mitigando potenciais penalidades por não cumprimento.

12.6. **Aumento da Produtividade**: Ao reduzir o tempo gasto em lidar com incidentes de segurança e manter a infraestrutura de TI operando de forma segura, os funcionários da SEPOG podem se concentrar mais em suas tarefas principais, aumentando a produtividade geral da instituição.

12.7. **Proteção Contra Ameaças Cibernéticas**

- **Descrição:** Antivírus ajudam a detectar e neutralizar uma ampla gama de ameaças, incluindo vírus, malwares, ransomwares e trojans.
- **Benefício:** Reduz o risco de infecções que podem comprometer dados e sistemas críticos.

12.8. **Segurança dos Dados**

- **Descrição:** Protege dados sensíveis e confidenciais contra acessos não autorizados e violações.
- **Benefício:** Garante a privacidade e a integridade das informações pessoais e institucionais.

12.9. **Manutenção da Integridade dos Sistemas**

- **Descrição:** Previne a corrupção de dados e a interferência em operações normais dos sistemas.
- **Benefício:** Assegura que os sistemas funcionem corretamente e que os dados permaneçam precisos e confiáveis.

12.10. **Prevenção de Interrupções de Serviço**

- **Descrição:** Evita que ataques cibernéticos causem interrupções nos serviços e sistemas da SEPOG.
- **Benefício:** Mantém a continuidade dos serviços públicos, evitando downtime e garantindo que os cidadãos possam acessar serviços essenciais sem interrupções.

12.11. **Redução de Custos com Recuperação**

- **Descrição:** Minimiza os custos associados à recuperação de dados e sistemas após um ataque cibernético.
- **Benefício:** Economiza recursos públicos e reduz o tempo necessário para a recuperação completa de sistemas comprometidos.

12.12. **Cumprimento de Normas e Regulamentações**

- **Descrição:** Ajuda a SEPOG a cumprir com exigências legais e regulamentares, como a Lei Geral de Proteção de Dados (LGPD).
- **Benefício:** Evita penalidades legais e mantém a conformidade com normas de segurança da informação.

12.13. **Aumento da Confiança dos Usuários**

- **Descrição:** Demonstrar um compromisso com a segurança cibernética aumenta a confiança dos cidadãos e dos servidores nos sistemas e serviços da SEPOG.
- **Benefício:** Fortalece a reputação da SEPOG como uma entidade responsável e confiável.

12.14. **Monitoramento e Relatórios**

- **Descrição:** Antivírus modernos oferecem ferramentas de monitoramento contínuo e relatórios detalhados sobre a segurança dos sistemas.
- **Benefício:** Fornece insights valiosos para aprimorar continuamente a estratégia de segurança cibernética da SEPOG.

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

13.1. **Da Forma de Entrega**

13.1.1. A entrega da licença de uso do software será realizado via endereço eletrônico e-mail: suporte@sepog.ro.gov.br.

13.2. **Do Prazo**

13.2.1. O prazo de entrega dos serviços deverá ser de até 15 (quinze) dias, contados da data de assinatura do Contrato, estabelecido pela Secretaria de Estado de Planejamento, Orçamento e Gestão - SEPOG/RO.

13.3. **Das Condições de Recebimento**

13.3.1. O recebimento provisório ou definitivo não exclui a responsabilidade civil pela solidez e segurança durante a prestação do serviço, nem ético profissional pela perfeita execução do contrato, dentro dos limites estabelecidos pela Lei ou instrumento contratual.

13.3.2. A critério exclusivo da Comissão de Recebimento, poderão ser realizados testes nas licenças de uso do software de forma a verificar a compatibilidade dos mesmos com as especificações constantes do Termo de Referência.

13.3.3. Sendo satisfatórias as verificações acima, lavrar-se-á um Termo de Recebimento Definitivo.

13.3.4. Caso insatisfatório, lavrar-se-á um Termo de Recusa e Devolução, no qual se consignarão as desconformidades com as especificações, onde a Contratada terá o prazo de 05 (cinco) dias úteis para se manifestar a respeito das desconformidades. Findado o prazo para manifestação, a Contratada deverá substituir o objeto dentro do prazo de 05 (cinco) dias úteis.

13.3.5. Caso a substituição não ocorra no prazo mencionado no item 13.3.4, a Contratada incorrerá em atraso na entrega, estará sujeita à aplicação das sanções previstas no Termo de Referência.

13.3.6. Todos os custos de substituição da licença, caso rejeitada, ocorrerão exclusivamente as expensas da Contratada.

13.3.7. O recebimento, provisório ou definitivo, não exclui a responsabilidade da Contratada pelo perfeito desempenho do serviço fornecido, cabendo-lhe sanar qualquer irregularidade detectada quando da utilização do mesmo.

13.3.8. Todas as despesas com taxas, impostos, encargos incidentes, deverão ser inclusos no preço da proposta e em hipótese alguma poderão ser cobrado em separado quando da emissão de Nota Fiscal/Fatura.

13.3.9. À Contratada caberá sanar as irregularidades apontadas no recebimento provisório/Termo de Recusa, submetendo a etapa impugnada à nova verificação, ficando sobrestado o pagamento até a execução das correções necessárias, sem prejuízo da aplicação das sanções cabíveis.

13.4. **Da Comissão de Recebimento:**

13.5. A comissão de recebimento provisório e definitivo realizará o relatório técnico para posterior emissão de recebimento definitivo, onde será designado os fiscais e gestor de contrato, por meio de Portaria devidamente publicada, após a elaboração do contrato.

13.5.1. É de competência da comissão de recebimento provisório e definitivo:

I – Verificar questões físicas do objeto/serviço adquirido para constatar a integridade conforme estipulado em Termo de Referência.

II – Verificar a conformidade com a quantidade e especificações constantes do Termo de Referência.

13.5.2. **O Recebimento dos Serviços**

13.5.2.1. A licença será recebida conforme disposição do artigo 140, inciso I da Lei 14.133/21:

13.5.3. **Do prazo de recebimento provisório e definitivo:**

a) Provisoriamente, até **2 (dois) dias úteis**, para posterior verificação da entrega das licenças, com as especificações deste termo de referência, mediante emissão de Termo de Recebimento Provisório.

b) Definitivamente, até **5 (cinco) dias úteis**, contados a partir da assinatura do Termo de Recebimento Provisório e após a verificação da compatibilidade das especificações do serviço entregue mediante a emissão de Termo de Recebimento Definitivo devidamente assinado pela comissão.

13.6. **Parâmetros e elementos descritivos:**

13.6.1. A ausência dos parâmetros e elementos descritivos como glossário de termos específicos de TIC, justificativa da métrica utilizada, arquitetura tecnológica, nível mínimo de serviço (NMS), transferência de conhecimento, documentação da licença, medição de demandas e considerações sobre contagem de pontos de função, pode ser justificada devido à natureza da compra, que se trata de um serviço de fornecimento de subscrição de licença pelo período de 36 meses.

13.6.2. Nesse contexto, a compra da subscrição de licença do Antivírus como um serviço por um período de tempo específico implica na aquisição de licenças que inclui acesso aos serviços online, atualizações de software e outros benefícios durante esse período. Como tal, a licença Antivírus adquirida dessa maneira geralmente já incorpora todos os elementos técnicos, de suporte e de documentação necessários para o uso efetivo da licença durante o período contratado.

13.6.3. Portanto, uma vez que a licença adquirida como serviço de subscrição já inclui todos esses elementos essenciais, não há necessidade de exigir a apresentação de parâmetros e elementos descritivos no processo licitatório. Exigir esses elementos adicionais poderia, de fato, complicar e prejudicar o processo licitatório, uma vez que a compra da subscrição de licença de Antivírus está pronta para uso e não requer customizações adicionais ou avaliações técnicas detalhadas.

13.7. **Critérios e prazos de medição e de Pagamento**

13.7.1. Será firmado Contrato com vigência de 36 (trinta e seis) meses com pagamento *upfront* (pagamento único antecipado), por ser um contrato com previsão de operação continuada de sistemas estruturantes de tecnologia da informação, podendo ser prorrogado conforme a lei estabelece com a possibilidade de vigência máxima de 15 (quinze) anos conforme Artigo 114 da Lei nº 14.133 de 01 de Abril de 2021, o que deve ser levado em consideração na proposta para um melhor preço.

14. DA DOTAÇÃO ORÇAMENTÁRIA

Descrição sucinta dos itens	Quantidade	Un. de medida	Prog.	Ação	Elemento de Desp.	Fonte	Servidor indicado
Software - Antivírus	250	Licenças	1015	2064	33.90.40	1500	Comissão TI

14.1. Cumpre informar que, considerando as fontes orçamentárias não decorrerem de recursos provenientes da União, não se vislumbrou a necessidade de publicação no Diário oficial da União - DOU.

15. CONDIÇÕES DO PAGAMENTO (LEI 14.133/21, ART.141, INCISO III)

15.1. O pagamento decorrente de contratações públicas será feito após a habilitação para pagamento, no prazo máximo de 15 (quinze) dias úteis, conforme artigo 190 do Decreto Estadual 28.874/24, no valor total, contados a partir da apresentação formal da respectiva documentação, respeitada a ordem cronológica das exigibilidades, depois da liquidação da despesa:

a) Nota fiscal;

b) Termo de Recebimento Definitivo;

c) Certidão Regularidade perante a Fazenda Federal (conforme PGFN/RFB Nº 1751, de 02/10/2014);

d) Certidão Regularidade perante a Fazenda Estadual;

e) Certidão de Regularidade perante a Fazenda Municipal;

f) Certificado de Regularidade do FGTS;

g) Certidão de Regularidade perante a Justiça do Trabalho – CNDT (Lei Federal nº 12.440/2011, de 07/07/2011);

h) Certidão Negativa referente ao Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual - CAGEFIMP.

15.2. No que se refere a exigência constante nas alíneas "c" a "g" serão aceitas certidões positivas com efeito negativas.

15.3. As Notas Fiscais/Faturas devem conter no corpo da Nota a descrição do objeto/serviços, o número do empenho e o número da Conta Bancária da CONTRATADA, para depósito do pagamento.

15.4. Após a aprovação da comissão, será realizado o pagamento correspondente a 03 (três) anos de licença, ou seja 36 (trinta e seis) meses.

15.5. O pagamento será efetuado através de Ordem Bancária - OB e depósito em conta corrente, indicada pela Contratada.

15.6. A Nota Fiscal deverá ser emitida em nome da **SECRETARIA DE ESTADO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO - SEPOG, CNPJ: 04.798.328/0001-56** – Endereço: Av. Farquar, 2986, Bairro Pedrinhas – CEP 76801-470 – Porto Velho/RO - Palácio Rio Madeira, Edifício Rio Cautário, prédio curvo a esquerda, 6º andar.

15.7. Na hipótese da Nota Fiscal/Fatura apresentar erros ou dúvidas quanto à exatidão dos valores, a CONTRATANTE poderá pagar apenas a parcela não controvertida no prazo fixado para pagamento, ressalvado o direito da CONTRATADA de reapresentar Nota Fiscal, para cobrança da parte controvertida com as devidas justificativas, neste caso, a CONTRATANTE terá o prazo de 05 (cinco) dias úteis, a partir do recebimento, para efetuar uma análise e o respectivo pagamento no mesmo prazo estipulado.

15.8. Na 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:

$$I = \frac{TX/100}{365}$$

EM = I x N x VP, 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.

15.9. Expedida a Nota de Empenho, o recebimento de seu objeto ficará condicionado a observância da norma contida no art. 140, inciso II, alíneas **a** e **b.**

15.10. O **Estado de Rondônia**, pessoa jurídica de direito público interno, é responsável tributário por substituição, uma vez que é o tomador do serviço, estando **obrigado a reter e recolher o ISSQN**, inclusive multa e acréscimos legais ao município de Porto Velho, independentemente de ter sido efetuada sua retenção na fonte em outro município (art. 264, inciso II, Lei complementar municipal nº 878, de 17 de dezembro de 2021).

15.11. Os serviços provenientes deste Termo de Referências deverão estar em conformidade ao item 1.07 da Lista de Serviços da Lei Complementar nº. 116 de 31 de julho de 2003 e suas alterações.

15.12. Dentro do prazo de vigência do contrato e mediante solicitação formal da CONTRATADA, o preço contratado poderá sofrer reajuste somente após o interregno dos 36 (trinta e seis) meses, aplicando-se o Índice de Custos de Tecnologia da Informação - ICTI (IPEA) ou outro índice oficial que vier a substituí-lo.

15.13. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

15.14. No caso de atraso ou não divulgação do índice de reajustamento, a CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

15.15. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

15.16. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

15.17. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

15.18. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

15.19. O reajuste será realizado por apostilamento.

16. CONDIÇÕES DE AQUISIÇÃO E PAGAMENTO SEMELHANTES ÀS DO SETOR PRIVADO E CONDIÇÕES DE EXECUÇÃO E PAGAMENTO, DAS GARANTIAS EXIGIDAS E OFERTADAS E DAS CONDIÇÕES DE RECEBIMENTO (ART. 40, 14.133/21)

16.1. Em atenção ao Art. 40, I da Lei 14.133/2021, consta a indicação neste Termo de Referência das condições de pagamento, bem como os prazos para adimplemento, vejamos:

Condições de Execução: Item 13.

Condições de pagamento: item 15 e subitens

Da Garantia da Contratação: subitem 4.4

Garantia prestado pelo fornecedor: subitem 26.13

Condições de recebimento do objeto: item 13 e subitens

16.2. As condições de aquisição e o pagamento do objeto deste Termo de Referência, atende a previsão do Art. 40, na Lei nº 14.133/21, c/c o art. 45, inciso III, do Decreto Estadual nº 28.874, de 2024, sendo semelhantes às do setor privado, conforme demonstrado nos itens 14.1.1 e 14.1.2 do Estudo Técnico Preliminar (0051127927):

1. **Proteção de Antivírus para Estação de Trabalho**

ITEM	EMPRESA	PROPOSTA	UNID.	QUANT.	MÊS		
					12	24	36
01	Solor SCANSOURCE BRASIL DISTRIBUIDORA DE TECNOLOGIAS LTDA. CNPJ 05.607.657/0008-01	(0051103889) KASPERSKY	Licença	200	R$30.958,00	R$43.728,00	R$63.912,00
02	M3 Comércio Software LTDA CNPJ: 20.040.746/0001-36	(0051032413) BITDEFENDER	Licença	200	R$54.000,00	R$78.000,00	R$102.000,00
03	PARTNERONE COMERCIO E SERVICOS EM INFORM- ATICA LTDA CNPJ: 11.439.893/0001-92	(0051302145) KASPERSKY	Licença	200	R$ 25.900,00	R$41.440,00	R$64.840,00

2. **Proteção para Servidores Físicos ou Virtuais**

ITEM	EMPRESA	PROPOSTA	UNID.	QUANT.	MÊS		
					12	24	36
01	SOLUÇÃO 3: Solução de Proteção para Servidores Físicos ou Virtuais	(0051752611) FORTINET	Pacote 25 Licença	2	R$ 48.769,00	R$ 97.583,00	R$ 146.306,00

17. DO PAGAMENTO ANTECIPADO (ART. 145 DA LEI Nº 14.133/2021)

17.1. A presente contratação se enquadra nos casos excepcionais do Art. 145, § 1º da Lei Federal nº 14.133/2021, que permite o pagamento antecipado quando propiciar sensível economia de recursos para a Administração, conforme demonstrado no Estudo Técnico Preliminar e detalhado abaixo:

Objeto da Contratação: Aquisição de licença de Antivírus para Estação de Trabalho e Licença de Antivírus para equipamento do tipo Servidor físico ou virtual.

Forma de Pagamento: Opção por pagamento integral do serviço.

Justificativa do Pagamento Antecipado: Economia de recursos e economia nos atos processuais.

18. DA SUBCONTRATAÇÃO, CESSÃO E/OU TRANSFERÊNCIA

18.1. É vedada a subcontratação, cessão ou transferência total ou parcial do serviço pela Contratada à outra empresa.

18.2. A vedação à subcontratação, cessão e/ou transferência neste projeto é essencial, não apenas para manter a alta qualidade e segurança na disponibilização dos domínios da SEPOG, mas também devido às especificidades do mercado

19. DA PARTICIPAÇÃO DE EMPRESAS REUNIDAS SOB A FORMA DE CONSÓRCIO

A participação de empresas reunidas sob a forma de consórcio na aquisição de software de Tecnologia da Informação e Comunicação (TIC) -Antivírus**,** é vedada devido a diversas considerações técnicas, econômicas e legais. Primeiramente, as licenças são essenciais para a proteção contra ameaças cibernéticas e nos ativos do Data Center, entre outras funcionalidades essenciais para as atividades administrativas da Secretaria. A contratação dessas licenças por múltiplas entidades, como seria o caso em um consórcio, poderia dificultar a integração entre os softwares.

Além disso, do ponto de vista econômico, a aquisição prevê duzentos e cinquenta licenças, o que torna a execução do projeto por várias empresas, como seria o caso em um consórcio, economicamente inviável. A complexidade e os custos adicionais associados à coordenação entre as empresas do consórcio não se justificam para um objeto de escopo relativamente limitado.

Legalmente, conforme o art. 15 da Lei Federal Nº 14.133/21, a formação de consórcios é mais adequada para objetos de grande complexidade ou de elevado valor, onde empresas individualmente não seriam capazes de atender aos requisitos mínimos de habilitação exigidos no edital. No caso em questão, o escopo e a natureza do projeto não se enquadram nesses critérios, tornando a participação de consórcios desnecessária e até contraproducente.

Portanto, a restrição à participação de consórcios neste certame não prejudica a competitividade, uma vez que a natureza do objeto não demanda a capacidade combinada de múltiplas empresas. Esta decisão visa assegurar a eficiência, a segurança e a viabilidade econômica, alinhando-se com as melhores práticas de gestão de riscos e conformidade legal.

20. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

20.1. **Da Forma de Seleção e critério de Julgamento da proposta**

O fornecedor será selecionado por meio de licitação PREGÃO ELETRÔNICO, CUJO CRITÉRIO DE JULGAMENTO SERÁ O DE MENOR PREÇO POR ITEM, em conformidade com a Lei Federal n. 14.133/2021, com adoção do critério de julgamento em que a proposta mais vantajosa para a Administração é a de menor preço por item.

20.2. **Da Validade da Proposta**

20.2.1. As propostas terão validade mínima de 90 (noventa) dias, a contar da data de homologação do certame.

20.2.2. Decorridos 90 dias da data homologação do certame sem a convocação para a contratação, ficam os licitantes liberados dos compromissos assumidos.

20.3. **Do Regime de execução**

20.3.1. Não se aplica por não se tratar de obras e serviços de engenharia.

20.4. **Do Modo de Disputa**

20.4.1. Aberto.

20.5. **Da aplicação da margem de preferência**

20.5.1. Não será aplicada margem de preferência na presente contratação.

20.6. **Da apresentação de Amostra**

20.6.1. Não se aplica.

21. EXIGÊNCIAS PARA HABILITAÇÃO

21.1. **Habilitação Jurídica**

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

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

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

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

21.1.5. 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;

21.1.6. No caso de **cooperativa:** Visando garantir a regularidade, a qualidade e a segurança dos serviços prestados pela Administração Pública, citamos alguns dos principais motivos para a **vedação** à participação de cooperativas neste pregão:

a) Controle e responsabilização: Ao vedar a participação de cooperativas, a Administração Pública busca evitar a dificuldade de controle e responsabilização pelos serviços prestados. Cooperativas são compostas por membros associados, e a rotatividade de cooperados pode dificultar a estabilidade e a continuidade dos serviços, tornando complexa a definição de responsabilidades em caso de falhas ou problemas na execução do contrato.

b) Segurança jurídica: A vedação evita situações ambíguas e potenciais questionamentos legais, uma vez que as cooperativas têm uma natureza peculiar e estão sujeitas a diferentes normas em comparação a outras formas de organização empresarial. Ao permitir a participação de cooperativas, poderia haver conflitos de interpretação sobre os direitos e deveres contratuais, afetando a segurança jurídica das contratações.

Diante do exposto, fica **vedado** a participação de empresa em forma de cooperativas.

21.1.7. 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.

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

21.2. **Qualificação econômico financeiro**

21.2.1. Para fins de qualificação econômico-financeira, as empresas interessadas em participar do certame, deverão apresentar os documentos relacionados a seguir, em conformidade com o artigo 69, da Lei 14.133/2021.

21.2.2. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, ou o Balanço de Abertura, caso a licitante tenha sido constituída em menos de um ano, devidamente autenticado ou registrado no órgão competente, para que o(a) pregoeiro(a) possa aferir se esta possui Patrimônio Líquido (licitantes constituídos há mais de um ano) ou Capital Social (licitantes constituídos há menos de um ano), de 3% (três por cento) do valor estimado do item que o licitante estiver participando.

21.2.3. 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).

21.2.4. 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).

21.2.5. O Balanço Patrimonial é necessário em função do caso não se enquadrar no Art. 70, III da Lei nº 14.133/21.

21.2.6. Certidão Negativa de Feitos sobre Falência nos termos da Lei 11.101/2005, expedida pelo distribuidor da sede da licitante, nos **últimos 90 (noventa)** dias caso não conste o prazo de validade.

21.2.7. A exigência dos documentos de qualificação econômica e financeira constantes do item 21.2, são indispensáveis à garantia do cumprimento das obrigações do objeto deste Termo de Referência.

21.3. **Da Qualificação Técnica**

21.3.1. Para fins de qualificação técnica, as empresas interessadas em participar do certame, deverão apresentar Atestado de Capacidade Técnica, (declaração ou certidão) fornecido (s) por pessoa jurídica de direito público ou privado, comprovando o fornecimento em contrato pertinente e compatível com o objeto da licitação, em conformidade com o artigo 67, §§ 1º e 2º, da Lei 14.133/2021.

21.3.2. Considerando o quantitativo de aquisição para o item 1 do item 4.3 do TR, as empresas deverão apresentar atestado de capacidade técnica que evidencie que o licitante já forneceu serviço assemelhados com o item, no percentual de 20% (vinte por cento).

21.3.3. Considerando o valor da aquisição para o item 2 do item 4.3 do TR, as empresas deverão apresentar atestado de capacidade técnica que evidencie que o licitante já forneceu serviço assemelhados com o item, no percentual de 20% (vinte por cento).

21.3.4. Justifica-se os percentuais expressos nos itens acima, pois é necessário compreender o contexto de exigência de qualificação técnica, conforme previsto na Lei 14.133/2021, e a importância de garantir a idoneidade e a capacidade das empresas licitantes. A definição de percentuais, como os 20% mencionados, serve como um critério objetivo para avaliar a experiência prévia da empresa e sua capacidade de atender a demanda da contratação. O percentual de 20% é estabelecido para assegurar que a empresa participante tenha um histórico comprovado de fornecimento ou execução de serviços semelhantes ao objeto da licitação em escala proporcional. Isso significa que o licitante deve demonstrar que já executou, em algum momento, serviços equivalentes a pelo menos 20% daquilo que está sendo solicitado na licitação.

21.3.4.1. Dessa forma, o percentual de 20% para a comprovação de qualificação técnica está em conformidade com o princípio da razoabilidade e da isonomia, ao mesmo tempo que assegura a participação de empresas com experiência mínima comprovada e capacidade técnica compatível com o objeto da licitação.

21.3.5. 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 unidade.

21.3.6. Na ausência dos dados indicados, antecipa-se a diligência prevista na lei federal nº 14.133/2021, para que sejam encaminhados em conjunto os documentos comprobatórios de atendimentos, quais sejam cópias de contratos, notas de empenho, acompanhados de editais de licitação, dentre outros. Caso não sejam encaminhados, o pregoeiro os solicitará no decorrer do certame para certificar a veracidade das informações e atendimento da finalidade do atestado.

21.3.7. A exigência dos documentos de qualificação técnica constantes do item 21.3, são indispensáveis à garantia do cumprimento das obrigações do objeto deste Termo de Referência.

22. RELATIVOS À REGULARIDADE FISCAL, SOCIAL E TRABALHISTA

22.1. **Regularidade Fiscal**

22.1.1. 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;

22.1.2. 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;

22.1.3. 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;

22.1.4. 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

22.1.5. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

22.1.6. 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.

22.2. **Do cumprimento ao disposto no inciso XXXIII do art. 7º da Constituição Federal**

22.2.1. O licitante deverá apresentar declaração, relativa ao cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal:

> Art. 7º São direitos dos trabalhadores urbanos e rurais, além de outros que visem à melhoria de sua condição social:
>
> XXXIII - proibição de trabalho noturno, perigoso ou insalubre a menores de dezoito e de qualquer trabalho a menores de dezesseis anos, salvo na condição de aprendiz, a partir de quatorze anos;

22.3. **Do cumprimento da Instrução Normativa nº 72/2023 (Imposto de Renda Retido na Fonte)**

22.3.1. A obrigação de retenção do Imposto de Renda alcançará todos os contratos vigentes, relações de compras e pagamentos efetuados por órgãos da Administração Pública Direta do estado de Rondônia, autarquias e fundações públicas e, ainda, por empresas estatais dependentes.

22.3.2. Para que se formalize as hipóteses de isenção e imunidade tributária, o representante legal da Pessoa Jurídica contratada deverá apresentar, no momento da celebração do contrato, ajuste ou instrumento congênere, bem como no momento de eventuais prorrogações, Declaração ao estado de Rondônia, conforme os seguintes modelos:

- Declaração de Instituições Inscritas no Simples Nacional;
- Declaração de Instituições de Educação e Assistência Social e CEBAS;
- Declaração de Instituições de Caráter Filantrópico, Recreativo, Cultural, Científico e Associações Civis e CEBAS;

22.4. **Do cumprimento do disposto no inciso XVII do art. 92º da Lei de Licitações e Contratos Administrativos nº14.133/2021.**

22.4.1. O licitante deverá apresentar declaração, relativa ao cumprimento do disposto no inciso XVII do art. 92 da Lei nº14.133/21 para reserva de cargos prevista em lei, para pessoa com deficiência:

> Art. 92. São necessárias em todo contrato cláusulas que estabeleçam:
>
> XVII - a obrigação de o contratado cumprir as exigências de reserva de cargos prevista em lei, bem como em outras normas específicas, para pessoa com deficiência, para reabilitado da Previdência Social e para aprendiz;

22.5. **Do cumprimento do disposto no inciso VI do art. 67 a Lei de Licitações e Contratos Administrativos nº14.133/2021.**

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

23. PARTICIPAÇÃO DE PESSOAS FÍSICAS

23.1. Cumpre apontar que conforme o Estudo Técnico Preliminar (0051127927), não se vislumbrou a possibilidade de exclusão de pessoas físicas, conforme previsto no art. 34, XIV do Decreto nº 28.874/2024.

23.2. No caso do licitante ser pessoa física deverá apresentar a documentação a seguir conforme previsto na INSTRUÇÃO NORMATIVA SEGES/ME Nº 116, DE 21 DE DEZEMBRO DE 2021:

> I - certidões ou atestados de qualificação técnica, expedidos por pessoas jurídicas de direito público ou privado, que comprovem ter as pessoas físicas fornecido os materiais ou prestado os serviços compatíveis com o objeto da licitação, conforme item 18.9 deste Termo de Referência;
>
> II - apresentação pelo adjudicatário dos seguintes documentos:
>
> a) prova de regularidade perante a Fazenda federal, estadual e/ou municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;
>
> b) prova de regularidade perante a Seguridade Social e trabalhista;
>
> c) certidão negativa de insolvência civil;
>
> d) declaração de que atende os requisitos do edital ou do aviso de contratação direta;
>
> e) declaração de inexistência de fato impeditivo para licitar ou contratar com a Administração Pública.
>
> III - exigência de a pessoa física, ao ofertar seu lance ou proposta, acrescentar o percentual de 20% (vinte por cento) do valor de comercialização a título de contribuição patronal à Seguridade Social, para fins de melhor avaliação das condições da contratação pela Administração.
>
> IV - exigência do cadastramento da pessoa física no Sistema de Registro Cadastral Unificado (Sicaf).
>
> Parágrafo único. O valor de que trata o inciso III deverá ser subtraído do valor da proposta final do ajudicatário e recolhido, pela Administração, ao Instituto Nacional do Seguro Social (INSS).

24. DAS OBRIGAÇÕES

24.1. **Da Contratante**

24.1.1. Efetuar o pagamento à CONTRATADA de acordo com as condições de preços e prazos estabelecidos neste Termo de Referência;

24.1.2. Aplicar à CONTRATADA as penalidades regulamentares e contratuais cabíveis devendo, caso seja necessário, aplicar à mesma as penalidades legais cabíveis;

24.1.3. Caso a comissão ateste que o serviço não estejam dentro das especificações constantes do presente Termo de Referência, a CONTRATADA ficará sujeita às sanções.

24.1.4. Oferecer todas as informações necessárias para que a contratada possa fazer a entrega das licenças dentro das especificações técnicas recomendadas, suas quantidades e periodicidade solicitadas.

24.1.5. Fornecer à Contratada, todos os esclarecimentos necessários sobre a entrega das licenças e demais informações que estes venham a solicitar;

24.1.6. Acompanhar, fiscalizar, conferir e avaliar o serviço deste termo de referência, através de representantes designados pela SEPOG;

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

24.2. **Da Contratada/Fornecedor**

24.2.1. Além daquelas determinadas por leis, decretos, regulamentos e demais dispositivos legais, nas obrigações da futura Contratada, também se incluem os dispositivos a seguir:

24.2.2. Aceitar nas mesmas condições contratuais os acréscimos ou supressões que se fizerem necessário, decorrentes de modificações de quantitativos ou projetos ou especificações, até o limite de 25% (vinte e cinco por cento) do valor contratual atualizado, de acordo com o art. 125, da Lei n°. 14.133/2021.

24.2.3. No caso de vícios ou de quaisquer outras irregularidades constatadas, a Administração fornecerá à Contratada, relatório concernente a essas ocorrências, expondo seus motivos, a fim de que as mesmas sejam corrigidas, no prazo máximo de 30 (trinta) dias, de acordo com o artigo 18, parágrafo 1° da Lei n° 8.078/1990 (Código de Defesa do Consumidor).

24.2.4. Além das demais obrigações exigidas em Lei a empresa deverá:

24.2.4.1. Responsabilizar-se integralmente pelas licenças contratadas, nos termos da legislação vigente;

24.2.4.2. Entregar as licenças nas especificações contidas neste Termo de Referência;

24.2.4.3. Entregar as licenças na forma e prazo estipulado;

24.2.4.4. Entregar as licenças nas quantidades indicadas neste TR;

24.2.4.5. Responsabilizar-se por todos os ônus, encargos, perdas e danos quando for constatado que tenham sido ocasionados em decorrência do fornecimento do serviço;

24.2.4.6. Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas e todos os tributos incidentes, sem qualquer ônus à CONTRATANTE,

24.2.4.7. Prestar à CONTRATANTE qualquer informação sobre o serviço a ser adquirido, sobre tudo qualquer dificuldade encontrada;

24.2.4.8. Manter, durante toda a execução do contrato, em compatibilidade com as obrigações por ele assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

24.2.4.9. A contratada deverá substituir, às suas expensas os serviços rejeitados.

24.2.4.10. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

24.2.4.11. Realizar todo o suporte e intermediação com o fabricante no idioma português Brasil.

25. SANÇÕES

25.1. Além daquelas determinadas por leis, decretos, regulamentos e demais dispositivos legais, a CONTRATADA estará sujeita as sanções definidas neste Termo de Referência.

25.2. A contratada que, sem justa causa, atrasar ou não cumprir as obrigações assumidas ou infringir preceitos legais, aplicar-se-ão as penalidades prescritas nos art. 155 ao art. 163 da Lei nº 14.133/2021, assim como as descritas no Decreto Estadual nº 28.874 de 25 de janeiro de 2024, garantindo a prévia defesa, sem prejuízo das responsabilidades civil e criminal. Dentre as penalidades, tem-se:

I - advertência;

II - multa moratória;

III - multa contratual;

IV - impedimento de licitar e contratar com o Estado de Rondônia, com o descredenciamento do Cadastro de Fornecedores do Estado de Rondônia, pelo prazo de até 3 (três) anos; e

V - 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.

25.3. As licitantes e contratadas serão responsabilizadas 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 n. 12.846, de 1º de agosto de 2013;

XIII - se recusar a Receber empenho;

XIV - não apresentar situação regular na ocasião dos recebimentos/realização serviços;

XV - Recusar-se a executar as determinações feitas pela FISCALIZAÇÃO, sem motivo justificado;

XVI - Destruir ou danificar documentos por culpa ou dolo de seus agentes;

XVII - Deixar de efetuar o pagamento de seguros, encargos fiscais e sociais, assim como quaisquer despesas diretas e/ou indiretas relacionadas à execução deste contrato;

XVIII - Deixar de cumprir quaisquer dos itens do Termo de Referência e seus anexos, mesmo que não previstos na tabela do item 25.11.

25.4. Na aplicação das sanções serão considerados:

I - a natureza e a gravidade da infração cometida;

II - as peculiaridades do caso concreto;

III - as circunstâncias agravantes ou atenuantes;

IV - os danos que dela provierem para a Administração Pública;

25.5. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

25.6. Sem prejuízo das sanções cominadas no art. 156, I, III e IV, da Lei nº 14.133/21, pela inexecução total ou parcial deste Termo de Referência, a Contratante poderá, garantida a prévia e ampla defesa, aplicar à Contratada multa, sobre a parcela inadimplida da presente contratação.

25.7. A multa será calculada na forma do termo de referência ou documento equivalente, não poderá ser inferior a 0,5% (cinco décimos por cento) nem superior a 30% (trinta por cento) do valor do contrato licitado ou celebrado e será aplicada ao responsável por qualquer das infrações administrativas previstas no item 19.3 e nos termos do art. 155 ao art. 163 da Lei nº 14.133/2021 e será calculada com base no quadro SANÇÕES - **item 25.11.**

25.8. A advertência deverá ser aplicada quando não se justificar a imposição de penalidade mais grave e 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.

25.9. A sanção de impedimento de licitar e contratar será aplicada ao responsável pelas infrações administrativas previstas no item 19.3 incisos: II, III, IV, V, VI, e VII, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta do ente federativo, que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos.

25.10. A sanção declaração de inidoneidade para licitar ou contratar será aplicada ao responsável pelas infrações administrativas previstas no item 25.11 inciso: VIII ao XVIII, bem como pelas infrações administrativas previstas nos incisos II, III, IV, V, VI e VII do Art. 155 da Lei 14.133/21 que justifiquem a imposição de penalidade mais grave que a sanção referida no § 4º do artigo 156 da Lei 14.133, e impedirá o responsável de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos.

25.11. Para efeito de aplicação de multas, às infrações são atribuídos 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:

SANÇÕES		
ITEM	**DESCRIÇÃO DA INFRAÇÃO**	**PENALIDADE PECUNIÁRIA - MULTA ***
I	dar causa à inexecução parcial do contrato com a entrega incompleta dos materiais/serviços ou deixar de providenciar recomposição complementar;	Multa de 1,6% por dia, por ocorrência.
II	dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;	Multa de 4,0%, por ocorrência.
III	dar causa à inexecução total do contrato;	Multa de 10%
IV	deixar de entregar a documentação exigida para o certame;	Multa de 4% sobre o valor contratado
V	não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;	Multa de 0,5% por dia, por item e por ocorrência.
VI	não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;	Multa de 1,0% por dia, por item e por ocorrência.
VII	ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;	Multa de 1,6 % por dia.
VIII	apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;	Multa de 1,0% por dia, por ocorrência.
IX	fraudar a licitação ou praticar ato fraudulento na execução do contrato;	Multa de 1,0% por dia, por ocorrência.
X	comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;	Multa de 3,0% por dia, por ocorrência.
XI	praticar atos ilícitos com vistas a frustrar os objetivos da licitação;	Multa de 1% sobre o valor contratado
XII	praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013;	Multa de 10% sobre o valor contratado
XIII	se recusar a Receber empenho	multa de até 10% sobre o valor total adjudicado.
XIV	não apresentar situação regular na ocasião dos recebimentos/realização serviços	multa de até 5% sobre o valor total adjudicado, por ocorrência;
XV	Recusar-se a executar as determinações feitas pela FISCALIZAÇÃO, sem motivo justificado;	1,6% por dia
XVI	Destruir ou danificar documentos por culpa ou dolo de seus agentes;	Multa de 4% sobre o valor contratado por ocorrência.
XVII	Deixar de efetuar o pagamento de seguros, encargos fiscais e sociais, assim como quaisquer despesas diretas e/ou indiretas relacionadas à execução deste contrato;	1,0% por dia, por dia e por ocorrência;
XVIII	Deixar de cumprir quaisquer dos itens do Termo de Referência e seus anexos, mesmo que não previstos nesta tabela de multas.	3,0% por dia, por ocorrência

*** Incidente sobre a Parte Inadimplida**

25.12. Após 16º (décimo sexto) dia da falta de entrega do objeto, será considerada inexecução total da contratação, o que ensejará a rescisão contratual.

25.13. 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.

25.14. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será cobrada judicialmente.

25.15. As sanções previstas não poderão ser relevadas, salvo se 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.

25.16. A sanção de advertência e a imposição de multa até o limite de 5% (cinco por cento) do valor contratado poderá ser aplicada diretamente pelo servidor ou comissão responsável pela fiscalização, assim como a constituição em mora do contratado em caso de inexecução do contrato, nos termos do Parágrafo Único do art. 185 do Decreto Estadual nº 28.874 de 25 de janeiro de 2024.

25.17. A aplicação das sanções previstas nos incisos III e IV do caput do art. 156 da Lei n. 14.133, de 2021, cumuladas ou não com multa, deverá ser precedida de processo administrativo, a ser conduzido por comissão integrada, no mínimo, por dois servidores públicos estáveis, respeitando os termos do art. 186 do Decreto Estadual nº 28.874 de 25 de janeiro de 2024.

25.18. Os atos previstos como infrações administrativas na Lei 14.133/21 ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 1º de agosto de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, por meio de processo administrativo de responsabilização - PAR, observado o rito procedimental específico nos termos do art. 187 do Decreto Estadual nº 28.874 de 25 de janeiro de 2024.

25.19. A sanção será obrigatoriamente registrada no Sistema de Cadastramento Unificado de Fornecedores – SICAF, bem como em sistemas Estaduais.

25.20. 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:

25.21. tenham sofrido condenações definitivas por praticarem, por meio dolosos, fraude fiscal no recolhimento de tributos;

25.22. tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

25.23. demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

25.24. Na hipótese de apresentar documentação inverossímil ou de cometer fraude, o licitante poderá sofrer sem prejuízo da comunicação do ocorrido ao Ministério Público, quaisquer das sanções previstas, que poderão ser aplicadas cumulativamente.

25.25. Nenhuma sanção será aplicada sem o devido processo administrativo, que **assegurará o contraditório e a ampla defesa ao fornecedor/adjudicatário**, observando-se o procedimento previsto na Lei nº 14.133, de 2021.

26. DO INSTRUMENTO CONTRATUAL

26.1. A formalização da contratação se dará através de Contrato Administrativo, conforme disposto no Art. 92 e 95 da Lei nº 14.133/21.

26.2. Administração convocará o interessado para assinatura do contrato, no prazo de até 10 (dez) dias úteis, contado da data da ciência ao chamamento, firmar o instrumento nas condições estabelecidas no respectivo Termo de Referência, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas no art. 155 da Lei n.º 14.133/21.

26.3. A convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela parte Contratada durante o seu transcurso e desde que ocorra motivo **justificado** e aceito pela Administração.

26.4. É facultado à Administração, quando o convocado não assinar o termo de contrato ou não aceitar o instrumento equivalente no prazo e condições estabelecidos, convocar as empresas remanescentes, na ordem de classificação, para a celebração do contrato nas condições propostas, prevista no artigo 90, parágrafo 2° da Lei 14.133/21.

26.5. O contrato terá vigência de 36 (trinta e seis) meses, a contar da assinatura do contrato, podendo ser prorrogado nos termos do art. 107 da Lei nº 14.133/2021, desde que a autoridade competente ateste que as condições e os preços permanecem vantajosos para a Administração, permitindo inclusive a negociação com o contratado.

26.6. A recusa injustificada do adjudicatário em assinar o contrato ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades legalmente estabelecidas e à imediata perda da garantia de proposta em favor do órgão ou entidade licitante estabelecidas na Lei. 14.133/21.

26.7. Toda e qualquer modificação, redução ou acréscimo nas disposições do Contrato será formalizada através de Termo Aditivo, exceto as previstas no artigo 136 da Lei 14.133/93.

26.8. É obrigação do contratado durante toda execução do serviço prestado ter compatibilidade com as obrigações por ele assumidas, além de todas as condições de habilitação e qualificação exigidas na licitação.

26.9. Para critério de reajuste, deverão retratar a variação efetiva do custo de produção, admitida a adoção de índices específicos ou setoriais (Item 15.11), desde a data prevista para apresentação da proposta, ou do orçamento a que essa proposta se referir, até a data do adimplemento de cada parcela.

26.10. **Do reajuste**

26.10.1. Dentro do prazo de vigência do contrato e mediante solicitação formal da CONTRATADA, o preço contratado poderá sofrer reajuste após o interregno de 36 (trinta e seis) meses, aplicando-se o Índice de Custos de Tecnologia da Informação - ICTI (IPEA) ou outro índice oficial que vier a substituí-lo exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

26.10.2. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

26.10.3. No caso de atraso ou não divulgação do índice de reajustamento, a CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

26.10.4. Fica a CONTRATADA obrigada a apresentar a memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer.

26.10.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

26.10.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor.

26.10.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

26.10.8. O reajuste será realizado por apostilamento.

26.11. **Dos acréscimos e Supressão Contratual**

26.11.1. A Contratada deverá aceitar, nas mesmas condições contratuais, acréscimos ou supressões de até 25% (vinte e cinco por cento) do valor inicial atualizado do contrato, nos termos do art. 125, da Lei 14.133/2021 e aqueles determinados no Decreto Estadual nº 28.874 de 25 de janeiro de 2024.

26.12. **Da Rescisão Contratual**

26.12.1. Os casos de rescisão de contrato serão aqueles regidos na Lei nº 14.133 de 2021 e no Decreto Estadual nº 28.874 de 25 de janeiro de 2024.

26.12.2. A inexecução contratual ensejará a extinção do instrumento contratual e/ou o cancelamento da ata de registro de preços, nos termos do Título III, Capítulo VIII, da Lei n. 14.133/2021, nos seguintes modos:

a) Determinada por ato unilateral e escrito da Administração, exceto no caso de descumprimento decorrente de sua própria conduta;

b) Consensual, por acordo entre as partes, por conciliação, por mediação ou por comitê de resolução de disputas, desde que haja interesse da Administração;

c) Determinada por decisão arbitral, em decorrência de cláusula compromissória ou compromisso arbitral, ou por decisão judicial.

26.12.3. O descumprimento, por parte da vencedora da licitação, de suas obrigações legais e/ou contratuais assegura ao Contratante o direito de extinguir o instrumento contratual e de cancelar a ata de registro de preços a qualquer tempo, independentemente de aviso, interpelação judicial e/ou extrajudicial.

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

26.13. **Garantia da Contratual**

26.13.1. No presente caso, não haverá exigência da garantia da contratação nos moldes do artigo 96 e seguintes da lei nº 14.133/2021, pois conforme previsão no dispositivo sua exigência constitui uma faculdade da administração, que deve ser analisada, em cada caso, os riscos que a contratação pode trazer, ou seja, está relacionada a complexidade do objeto/serviço, vulto da contratação e aos potenciais riscos oriundo da execução do contrato.

26.13.2. Assim, a equipe de planejamento ao elaborar o Estudo Técnico Preliminar - ETP e validar a viabilidade da contratação, analisou os riscos associados à contratação, e em função de não existir histórico ou situação de risco relacionada à exigência de garantia, foi identificado pela equipe técnica a dispensabilidade de sua exigência, pois representaria um ônus desnecessário a ser suportado pelo contratado.

27. DO ACOMPANHAMENTO E FISCALIZAÇÃO

27.1. A fiscalização do contrato será realizado por comissão designada pela administração pública, que irá fiscalizar a execução do contrato, nos termos do art. 117, da Lei 14.133/21, anotando em registro próprio todas as ocorrências relacionados a execução do contrato.

27.2. Os esclarecimentos solicitados pela fiscalização deverão ser prestados imediatamente, salvo se depender de modificação de cálculo ou teste, hipótese em que será fixado um prazo de acordo com a complexidade do caso;

27.3. O exercício da fiscalização pela CONTRATANTE, não excluirá ou reduzirá a responsabilidade da CONTRATADA.

27.4. O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade do objeto/serviço, de forma a assegurar o perfeito cumprimento do objeto, devendo ser exercidos por um ou mais representantes da Contratante, especialmente designados, na forma dos art 117 e 140 da Lei 14.133 de Abril de 2021.

27.5. O representante da Contratante deverá ter a experiência necessária para o acompanhamento e controle do serviço e do contrato.

27.6. A verificação da adequação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

27.7. A fiscalização será feita por uma comissão especialmente nomeada para este fim pela **Secretaria de Estado do Planejamento, Orçamento e Gestão**, através de portaria a ser publicada no diário oficial do Estado.

27.8. O fiscal do contrato será auxiliado pelos órgãos de assessoramento jurídico e de controle interno da Administração, que deverão dirimir dúvidas e subsidiá-lo com informações relevantes para prevenir riscos na execução contratual, conforme § 3º, da Lei 14.133/21.

27.9. **Gestor do Contrato**

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

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

28. DA ADOÇÃO DE CONCILIAÇÃO, MEDIAÇÃO, COMITÊ DE RESOLUÇÃO DE DISPUTAS E ARBITRAGEM PARA A SOLUÇÃO DE LITÍGIO

Conforme o caput do art. 151 da Lei 14.133/21, é facultada à Administração utilizar os meios alternativos de prevenção e resolução de controvérsias em suas contratações, por outro lado, o parágrafo único exige que tais meios sejam aplicados às controvérsias relacionadas a direitos patrimoniais disponíveis.

Dessa forma, caso necessário, será adotado os meios alternativos de resolução de controvérsias, tendo em vista que o objeto a ser licitado possui valor econômico e pode ser comercializado ou transacionado livremente por seus titulares, obtendo assim uma maior celeridade na solução dos conflitos no âmbito administrativo, evitando o custo e a morosidade do Poder Judiciário.

29. DA PROPRIEDADE INTELECTUAL - ARTIGO 42 DO DECRETO ESTADUAL 28.874/2024

29.1. Considerando que a aquisição do software antivírus pela SEPOG ocorre por meio de subscrição, ou seja, a compra de um direito de uso temporário por 36 meses, trata-se de um software de prateleira amplamente distribuído no mercado, o qual não envolve desenvolvimento personalizado ou exclusivo para a SEPOG. Por esse motivo, não há transferência de direitos autorais ou propriedade intelectual sobre o produto.

29.2. A ausência de cláusula específica sobre propriedade intelectual se justifica pela natureza do contrato, que se limita ao uso da solução por um período determinado, sem qualquer cessão ou transferência de propriedade do software. Os direitos sobre o software permanecem com o fornecedor, sendo a SEPOG apenas licenciada a utilizar o produto dentro dos limites estabelecidos no contrato.

29.3. Além disso, não há necessidade de cláusulas específicas de propriedade intelectual quando o produto em questão é software comercial pronto para uso comercial, pois os direitos autorais e a propriedade intelectual já estão claramente regulamentados nas políticas de licença padrão do fabricante. A SEPOG adquire apenas o direito de utilizar a solução durante o prazo contratado, sem envolvimento em questões de propriedade intelectual.

29.4. Portanto, a inclusão de cláusulas sobre propriedade intelectual seria redundante e desnecessária neste contexto, pois não altera o escopo do contrato de subscrição do software.

30. DA PROTEÇÃO DE DADOS PESSOAIS - LEI N 13.709/2018 - LGPD E DA LEI FEDERAL Nº 12.527/2011 DE ACESSO A INFORMAÇÃO - LAI

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 13.709, estabelece uma série de princípios e requisitos relacionados à segurança dos dados pessoais. O respeito à segurança dos dados é de extrema importância por várias razões:

- Proteção dos Direitos Individuais: A LGPD visa proteger os direitos e liberdades dos titulares dos dados pessoais. Isso significa que as informações pessoais de indivíduos devem ser tratadas de forma a evitar acessos não autorizados, prevenindo assim a violação de seus direitos à privacidade e à proteção de dados.
- Prevenção à Fraude e à Segurança do Titular: A lei permite o tratamento de dados sensíveis quando necessário para garantir a prevenção à fraude e a segurança dos titulares. Isso é fundamental para proteger as pessoas contra crimes e atividades fraudulentas.
- Pesquisas em Saúde Pública: A LGPD reconhece a importância das pesquisas em saúde pública, mas exige que esses dados sejam tratados em ambiente controlado e seguro, garantindo a confidencialidade e a segurança das informações dos indivíduos envolvidos.
- Responsabilidade: A lei estabelece a responsabilidade dos controladores e operadores de dados pessoais em garantir a segurança da informação. Qualquer violação de segurança que resulte em danos aos titulares de dados é de responsabilidade do controlador ou operador.
- Relatório de Impacto à Proteção de Dados: A autoridade nacional de proteção de dados pode exigir que as organizações elaborem relatórios de impacto à proteção de dados, incluindo a descrição das medidas de segurança adotadas. Isso incentiva as empresas a investirem em segurança da informação.
- Obrigações Permanentes: A LGPD estabelece que a obrigação de garantir a segurança dos dados pessoais continua mesmo após o término do tratamento dos dados. Isso significa que as organizações devem manter a segurança das informações mesmo após sua utilização inicial.

Em resumo, a LGPD enfatiza a importância da segurança dos dados pessoais como um elemento essencial para a proteção dos direitos individuais, a prevenção de fraudes, a pesquisa em saúde pública e a responsabilidade das organizações. Adotar medidas de segurança adequadas não apenas ajuda a cumprir a lei, mas também constrói a confiança dos titulares de dados e protege a reputação das organizações.

31. DOS CRITÉRIOS DE SUSTENTABILIDADE

A contratação de licenças de software, em sua essência, não gera impacto ambiental significativo devido à sua natureza predominantemente virtual e intangível. Tais sistemas, alinhados ao paradigma da digitalização, operam primordialmente em ambientes digitais, onde a manipulação de dados e o processamento de informações ocorrem sem a necessidade de recursos materiais tangíveis.

Este fenômeno é corroborado pela abstração inerente à produção de conteúdo audiovisual por meio de softwares, onde a criação, edição e renderização de elementos visuais e sonoros são realizados mediante algoritmos computacionais, prescindindo de materiais Isicos que possam resultar em resíduos ou degradação ambiental. Ademais, a natureza itera/va e virtual dos processos criativos e de pós-produção envolvidos nestes softwares favorece a minimização do consumo de recursos naturais e energia.

Além disso, a substituição gradual de processos analógicos por soluções digitais tem contribuído para a redução do consumo de papel, tinta, solventes e outros materiais tradicionalmente associados à produção e distribuição de mídia audiovisual, promovendo, assim, uma pegada ambiental mais leve e sustentável.

Portanto, a contratação de licença de softwares não apenas atesta uma abordagem tecnológica avançada e eficiente, mas também se destaca como uma prática que converge harmoniosamente com os imperativos contemporâneos de conservação e preservação ambiental.

32. **DAS CONDIÇÕES GERAIS**

32.1. As omissões, dúvidas e casos não previstos neste instrumento serão resolvidos e decididos aplicando-se a Lei Federal nº 14.133/21 e suas alterações.

32.2. Ocorrendo fato novo decorrente caso fortuito ou força maior, nos termos previstos na legislação vigente, que obste o cumprimento pela contratada dos prazos e demais obrigações aqui estatuídas a mesma ficará isenta das multas e penalidade pertinentes.

32.3. As partes contratantes elegem o foro de Porto Velho/RO como competente para dirimir quaisquer questões oriunda do contrato, inclusive os casos omissos que não puderem ser resolvidos pela via administrativa.

33. **ANEXOS:**

33.1. Anexo I - **ESPECIFICAÇÕES TÉCNICAS (0051097159).**

Elaboração:

JEANE KARINE GONÇALVES COLARES

Assessora SEPOG-NCLCC

Revisão:

PASCALINI CARVALHO CHAGAS

Coordenadora Administrativo e Financeiro - SEPOG

APROVO:

ESTEFANE FERREIRA ESTEVAM MARINHO

Diretora Executiva da Secretaria de Estado do Planejamento, Orçamento e Gestão - SEPOG

Delegação de Competência da Portaria nº 210 de 02 de maio de 2024

Documento assinado eletronicamente por **Estefane Ferreira Estevam Marinho**, **Diretor(a) Executivo(a)**, em 18/03/2025, às 11:24, 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 **PASCALINI CARVALHO CHAGAS**, **Coordenador(a)**, em 18/03/2025, às 11:39, 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 **Jeane Karine Gonçalves Colares**, **Assessor(a)**, em 19/03/2025, às 15:55, 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 **0058149249** e o código CRC **879E81CD**.

Governo do Estado de
RONDÔNIA

GOVERNO DO ESTADO DE RONDÔNIA
Secretaria de Estado do Planejamento, Orçamento e Gestão - SEPOG

ESTUDO TÉCNICO PRELIMINAR

1. INTRODUÇÃO

O Estudo Técnico Preliminar – ETP é o documento constitutivo da primeira etapa do planejamento de uma contratação, que tem por objetivo demonstrar o interesse público envolvido e a sua melhor solução. Ele serve de base ao Termo de Referência a ser elaborado, caso se conclua pela viabilidade da contratação.

O ETP tem por objetivo identificar e analisar os cenários para o atendimento de demanda registrada no Documento de Formalização da Demanda – DFD, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar a tomada de decisão e o prosseguimento do respectivo processo de contratação.

2. MODELO DE REFERÊNCIA

O modelo padrão utilizado foi o Estudo Técnico Preliminar (ETP) (atualizado em 06/04/2023) do governo federal, disponível em: https://www.gov.br/governodigital/pt-br/contratacoes/templates-e-listas-de-verificacao. Para adequar a realidade da SEPOG e a este objeto foram feitos os seguintes ajustes:

- Acrescentado item 23 Critérios de Sustentabilidade;
- Acrescentado item 24 Riscos;
- Item responsável foi acrescentado a comissão de elaboração ETP;

3. FUNDAMENTAÇÃO LEGAL

O presente Estudo Técnico Preliminar foi elaborado em atendimento aos regulamentos legais a seguir:

a) Constituição Federal, art. 37, caput;
b) Lei Federal nº 14.133/21 (Nova Lei de Licitações);
c) Decreto nº 28.874, DE 25 DE JANEIRO DE 2024 (Regulamenta a Lei nº 14.133/2021);
d) Instrução Normativa SEFIN nº 72/2023 (Manual de Imposto de Renda Retido na Fonte);
e) Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
f) Lei nº 12.527/2021 (Lei de Acesso à Informação); e
g) Instrução Normativa SGD/ME nº 94 de 23 de dezembro de 2022.

4. INFORMAÇÕES BÁSICAS

Processo: nº 0035.003501/2023-45
Categoria: Contratação de TIC - Serviço

5. DESCRIÇÃO DA NECESSIDADE

O presente estudo visa avaliar a viabilidade funcional, negocial e técnica da aquisição de proteção corporativa contra vírus, *malware* e *trojans.* Esta iniciativa de adquirir softwares de Tecnologia da Informação e Comunicação (TIC) está alinhada com os objetivos estratégicos da SEPOG, ao prover defesa contra ameaças digitais aos dispositivos em uso na Secretaria de Estado do Planejamento, Orçamento e Gestão (SEPOG), como computadores, notebooks e servidores. O crescente risco de ataques cibernéticos representa um desafio significativo para a segurança das organizações, evidenciando a necessidade urgente de um software antivírus eficaz. No contexto específico da SEPOG, o antivírus desempenha um papel crucial na proteção de seu ambiente computacional. Renovar ou substituir o antivírus torna-se crucial para assegurar a continuidade dos serviços prestados pela SEPOG, bem como a segurança dos serviços públicos e a eficaz prestação de informações. O antivírus enfrenta uma ampla gama de ameaças, desde objetos maliciosos até sequestradores de navegadores, Ransomware, keyloggers, entre outros.

A proteção contra ameaças virtuais, como URLs infectadas, spam, fraude, ataques de *phishing* e ameaças persistentes avançadas (APTs), é essencial. A exposição da infraestrutura tecnológica da SEPOG à internet aumenta a vulnerabilidade, tornando a aquisição das licenças uma medida essencial para garantir a proteção contra a rápida propagação de vírus e malwares. A continuidade do suporte e das atualizações do antivírus é vital para manter a eficácia do software na proteção dos ativos computacionais. Destaca-se ainda a importância do antivírus na proteção contra o aumento exponencial de riscos associados ao crescente número de equipamentos e soluções digitais. A aquisição de uma nova solução é apresentada como uma necessidade iminente, alinhada com o Planejamento de Contratação Anual (PCA) e o Plano Plurianual (PPA) da SEPOG.

A adoção de uma nova solução para atender o servidor de TI, bem como a contratação para atender os usuários, é justificada pela necessidade crítica de proteger os ativos computacionais da SEPOG contra constantes ameaças cibernéticas. Essa medida garante a continuidade dos serviços públicos e a segurança das informações.

5.1. DO PROBLEMA

O antivírus desempenha um papel necessário na proteção contra vírus, malware e trojans, essencial para garantir a continuidade dos serviços e a segurança das informações. O problema central é a necessidade urgente de reforçar a proteção dos ativos computacionais da SEPOG contra as ameaças digitais em constante evolução.

5.2. MOTIVAÇÃO/JUSTIFICATIVA

A aquisição de software antivírus na SEPOG (Secretaria de Planejamento e Gestão) é de extrema importância por várias razões, especialmente no contexto da proteção de dados pessoais e sensíveis, conforme estabelecido pela LGPD (Lei Geral de Proteção de Dados). Além disso, a conformidade com as normas da CIS (*Center for Internet Security*), como o CONTROL 8, e as normas da ABNT (Associação Brasileira de Normas Técnicas) são fundamentais para garantir a segurança da informação. Aqui estão algumas razões para a importância dessa aquisição:

5.2.1. Proteção de Dados Pessoais e Sensíveis (LGPD):

A LGPD estabelece diretrizes específicas para a proteção de dados pessoais, exigindo que as organizações implementem medidas adequadas para garantir a segurança e a privacidade desses dados. Um software antivírus é uma medida fundamental para proteger os sistemas e os dados armazenados pela SEPOG contra ameaças cibernéticas, como malware, ransomware e phishing, que podem comprometer a segurança dos dados pessoais e sensíveis.

5.2.2. CIS CONTROL 8:

O CIS CONTROL 8 estabelece diretrizes para a gestão de vulnerabilidades e ameaças, incluindo a implementação de controles de antivírus e anti-malware. Ao adquirir um software antivírus, a SEPOG estará em conformidade com aspectos deste controle, garantindo uma abordagem proativa para proteger seus sistemas contra ameaças conhecidas e emergentes.

5.3. Normas da ABNT:

As normas da ABNT relacionadas à segurança da informação, como a NBR ISO/IEC 27001, fornecem diretrizes para estabelecer implementar, manter e melhorar um sistema de gestão de segurança da informação (SGSI). A aquisição de um software antivírus é uma medida que pode ser implementada como parte desse SGSI, ajudando a garantir a segurança dos sistemas e dos dados da SEPOG de acordo com as melhores práticas estabelecidas pela ABNT.

5.4. Prevenção de Incidentes de Segurança:

Um software antivírus eficaz é essencial para prevenir incidentes de segurança, como ataques de malware e violações de dados, que podem ter sérias consequências para a SEPOG, incluindo danos à reputação, perda de dados confidenciais e interrupção das operações. Ao investir em uma solução de antivírus robusta, a SEPOG está fortalecendo suas defesas cibernéticas e reduzindo o risco de incidentes de segurança.

Em resumo, a aquisição de um software antivírus na SEPOG é crucial para proteger os dados, garantir a conformidade com regulamentações como a LGPD e as normas da CIS e da ABNT, e prevenir incidentes de segurança que possam comprometer a integridade e a disponibilidade dos sistemas e das informações da organização.

5.4.1. INTERESSE PÚBLICO

Aspecto	Descrição	Interesse Público
Proteção de Dados Sensíveis	Proteção contra acessos não autorizados e vazamentos de dados.	Proteção da privacidade e segurança das informações pessoais.
Continuidade de Serviços	Manter a disponibilidade e funcionamento dos sistemas.	Garantir que os serviços públicos estejam sempre disponíveis para os cidadãos.
Integridade dos Sistemas	Garantia de que os dados e operações não sejam corrompidos ou alterados por malwares.	Assegurar a confiabilidade e precisão das informações geradas e mantidas pela SEPOG.
Conformidade Legal	Cumprimento de legislações como a LGPD.	Evitar sanções e penalidades legais.
Eficiência Operacional	Prevenção de perda de produtividade e custos elevados com recuperação de sistemas.	Promover a eficiência e economia na administração pública.
Confiança e Credibilidade	Manter a confiança dos cidadãos e servidores na capacidade de proteção de informações.	Fortalecer a credibilidade da SEPOG como uma entidade segura e confiável.

5.5. **ALINHAMENTO COM OS INSTRUMENTOS DE PLANEJAMENTO ORGANIZACIONAL**

A pretendida contratação está prevista no PCA 2024, devidamente publicado no DIOF/RO n°212, na data de 10/11/2023.

	Descrição
PCA 2024 - SEPOG	**Portaria n° 481 de 08 de novembro de 2023 (**0046974964**)**

5.6. **NATUREZA DO OBJETO**

Os bens/serviços a serem adquiridos enquadram-se na classificação de bens comuns, nos termos do art. 6°, XIII da Lei 14.133/2021, uma vez que detêm especificações técnicas conhecidas e usualmente utilizadas no mercado de TIC. Desse modo, nos termos do art. 20 da Lei 14.133/2021, os elementos do planejamento da contratação reafirmam que os bens/serviços descritos neste Estudo não possuem características de bem de luxo.

6. ÁREA REQUISITANTE

Identificação da Área Requisitante	Nome do Responsável
ASTIC	**MARCELO MATOS LIMA**

7. NECESSIDADE DE NEGÓCIO

ID	DESCRIÇÃO DA NECESSIDADE DE NEGÓCIO	PROPOSTAS
1	Ampliar a disponibilidade dos serviços de TI;	Garantir a continuidade operacional por meio da aquisição, aproveitando a estrutura já existente do antivírus para uma implementação eficiente
2	Proteção contra malware nas estações de trabalho.	Reforçar a defesa contra malware, utilizando o conhecimento adquirido com o antivírus, otimizando sua configuração para melhor performance
3	Proteção contra malware nos servidores.	Fortalecer a segurança dos servidores aproveitando a experiência adquirida com o antivírus, maximizando sua eficácia na proteção.
4	Filtragem de conteúdos maliciosos.	Aprimorar a capacidade de filtragem, utilizando a experiência acumulada para otimizar a identificação e bloqueio de conteúdos maliciosos.
5	Bloqueio de sites suspeitos.	Implementar recursos avançados para identificar e bloquear acessos a sites suspeitos, aproveitando a base de conhecimento.
6	Restrição ao acesso de dispositivos infectados	Reforçar medidas de segurança para restringir o acesso de dispositivos externos, como pendrives e cartões de memória.
7	Prevenção de fraudes em movimentações financeiras.	Aprimorar as funcionalidades antifraudes para proteger as movimentações financeiras, aproveitando o conhecimento acumulado.
8	Proteção contra vazamento de informações e perda de dados.	Reforçar as camadas de proteção visando evitar vazamentos de informações sensíveis e perda de dados.
9	Suporte técnico e atualização por 36 meses.	Garantir suporte técnico contínuo e atualizações regulares da base de dados ao longo de 36 meses.

8. NECESSIDADE TECNOLÓGICA

ID	DESCRIÇÃO DA NECESSIDADE TECNOLÓGICA	PROPOSTAS
1	Console de Gerenciamento (Centralizado).	Aprimorar o console de gerenciamento centralizado para proporcionar uma interface mais intuitiva e eficiente
2	Gerenciamento por Grupos (Integração com AD).	Reforçar a integração com o Active Directory (AD) para um gerenciamento mais eficaz e segmentado por grupos de usuários
3	Anti-Malware/Anti-Virus	Manter e aprimorar as capacidades antivírus e antimalware para garantir uma proteção abrangente contra ameaças digitais
4	Anti-Ransomware.	Reforçar as defesas contra ransomware, incorporando tecnologias avançadas para prevenir e combater ataques deste tipo de malware
5	IPS host	Implementar um Sistema de Prevenção de Intrusões (IPS) no nível do host para detectar e bloquear atividades maliciosas em tempo real
6	IDS host	Introduzir um Sistema de Detecção de Intrusões (IDS) no nível do host para identificar padrões de comportamento suspeitos nas estações
7	Firewall host	Fortalecer as funcionalidades do firewall no nível do host para controlar o tráfego e impedir acessos não autorizados aos dispositivos
8	Filtro de conteúdo Web (Classificação de Site)	Aprimorar o filtro de conteúdo web para uma classificação mais precisa de sites, fortalecendo a segurança contra ameaças online
9	Suporte a Windows e Linux	Garantir pleno suporte para ambientes Windows e Linux, assegurando uma proteção consistente em todas as plataformas utilizadas pela SEPOG
10	Proteção para licença de email (Microsoft Exchange)	Reforçar a proteção contra ameaças em soluções de e-mail, especialmente no ambiente Microsoft Exchange, para prevenir ataques direcionados
11	Proteção para licença de Diretório (AD)	Intensificar a proteção para soluções de diretório, como o Active Directory, para mitigar possíveis ameaças que visam comprometer a infraestrutura centra
12	Gerenciamento de vulnerabilidades e correções	Implementar um sistema eficaz de gerenciamento de vulnerabilidades, permitindo a aplicação rápida de correções para reduzir exposições a ameaças
13	Integração com soluções de SIEM	Aperfeiçoar a integração com soluções de Segurança de Informações e Gerenciamento de Eventos (SIEM) para uma resposta coordenada a incidentes
14	Controle de Dispositivos (USB)	Reforçar o controle sobre dispositivos USB, garantindo restrições e monitoramento efetivo para prevenir potenciais ameaças externas
15	Proteção proativa contra ameaças desconhecidas	Incorporar tecnologias proativas para identificação e bloqueio instantâneo de ameaças desconhecidas, elevando a resiliência contra ataques
16	Monitorar o comportamento dos aplicativos	Aprimorar a capacidade de monitoramento do comportamento dos aplicativos, identificando atividades suspeitas em tempo rea
17	Interromper atividades prejudiciais em tempo real	Implementar mecanismos para interromper instantaneamente atividades potencialmente prejudiciais, garantindo uma resposta rápida a ameaças
18	Sensores para coleta de dados comportamentais	Utilizar sensores para coletar dados comportamentais dos dispositivos endpoint, permitindo uma análise abrangente para identificação de potenciais ataques
19	Monitorar pastas protegidas contra gravação não autorizada	Reforçar a monitorização de pastas protegidas, impedindo gravações não autorizadas para evitar perda ou comprometimento de dados sensíveis.

9. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

Nº	Necessidades	Descrição
1	Lei Geral de Proteção de Dados Pessoais	Ser adequada a Lei Geral de Proteção de Dados

10. ESTIMATIVA DA DEMANDA

As quantidades levantadas levaram em consideração o quantitativo atual de funcionários que a SEPOG dispõe.

De igual modo, o quantitativo de Licenças para fins do servidor TI foi retirado da necessidade constante no Documento de Oficialização de Demanda 5 (0048979555).

Desse modo, o quantitativo de ambas as licenças, para atender as necessidades da Secretaria, estão presentes no Documento de Oficialização de Demanda 5 (0048979555), conforme a seguir:

DESCRIÇÃO	UND.	QUANTIDADE
Antivírus para Usuários	Licenças	200
Licença de Antivírus para equipamento do tipo Servidor	Licenças	50

Esta estimativa reflete o compromisso da SEPOG em assegurar a continuidade operacional, a proteção eficaz contra ameaças cibernéticas e a adaptação às crescentes demandas tecnológicas, reafirmando o comprometimento com a segurança e eficiência em sua infraestrutura computacional.

11. LEVANTAMENTO DE MERCADO

11.1. **Necessidades similares em outros órgãos ou entidades da Administração Pública e as soluções adotadas:**

a) Governo do Estado de Rondônia:

UNIDADE	PROCESSO	ESTUDO TÉCNICO PRELIMINAR	OBJETIVO	QTD	PERÍODO	VALOR
IDARON	0015.076396/2022-11	ETP SEI nº 0029300750 RENOVAÇÃO KASPERSKY	Renovar Kaspersky	1.200	36 MESES	R$ 252.996,00
SEFIN	0030.065871/2022-35	Estudo Técnico - Atualizado (0024032913)	Renovar Kaspersky	900	36 MESES	R$ 141.696,00

DER	0009.068736/2022-19	Não tem	Renovar Kaspersky	500	36 MESES	R$ 61.720,00
SEOSP	069.000418/2023-27	Estudo Técnico Preliminar 2 (0038653409)	Licitou kaspersky	300	36 MESES	R$ 47.232,00

b) Outros órgãos:

UASG	Processo	Objeto	Cenário 1	Cenário 2	Cenário 3	Solução apontada	QTD de licença	Período	Valor Estimado
158718	23479.000082/2021-12	Renovação Kaspersky	Renovar Kaspersky	Não Explorado	Não Explorado	Renovar Kaspersky	1000	36 meses	R$82.020,00
158151	23147.001950/2020-30	Solução de Antivirus	Renovação de licenciamento da solução atual de antivírus	Implantar solução de antivírus Gratuita	Contratação de Nova Solução de antivírus	Contratação de Nova Solução de antivírus considerando que renovar era inviável devido a 8 anos sem renovação	1310	36 meses	R$213.818,20
154810	23501.000118.2021-25	Solução de Software Antivírus	Armadito-av	Bitdefender GravityZone Advanced Business Security	ClamAV	-	450	12 meses	R$35.388,00
154040	23106.017186/2021-96	solução corporativa de antivírus	Trend Micro – Período 48 meses. Valor Unitário: R$133,50	Kaspersky – Período 48 meses. Valor Unitário: R$125,60	Kaspersky Endpoint Security for Business Advanced – Período 36 meses. Valor Unitário: R$98,18	-	4000	36 meses	R$256.000,00
240128	01204.000092/2023-07	kASPERSKY	Renovar Kaspersky	-	-	-	170	36 meses	R$29.826,50

11.2. **Estudo Técnico de Outros Órgãos:**

a) Tribunal de Justiça do Amazonas:

Item	Descrição	Unid.	Qnt. Total	Preço (R$)	
				Unit.	Total
1	SERVIÇO DE LICENÇAS DE SOFTWARE, Caracteristica(s): especializado em licença de uso de software versão equivalente superior, com suporte e atualizações por 36 meses, características adicional(is): conforme Termo de Referência	Unidades	4.000	R$322,00	R$1.288.00,00
2	(ID 511957) SERVIÇO DE CAPACITAÇÃO ADICIONAL, Característica(s): especializado em treinamento na área de solução de antivírus kaspersky para até 05 (cinco) pessoas, Características Adicional(is): Conforme Projeto Básico/Termo de Referência.	Unidades	1	R$95.000,00	R$95.000,00
3	(ID 511955) SERVIÇO DE CONSULTORIA, Característica(s): especializado em instalação e configuração da solução de proteção para até 4.999 (quatro mil, novecentos e noventa e nove) Endpoints, Características Adicional(is): Conforme Projeto Básico/Termo de Referência.	Unidades	1	R$38.000,00	R$38.000,00
4	(ID 515283) SERVIÇO DE CONSULTORIA, Característica(s): especializado em consultoria e suporte técnico por 36 meses na solução de preteção de Endpoints Kaspersky, Características Adicional(is): Conforme Projeto Básico/Termo de Referência.	Unidades	120	R$12.000,00	R$1.444.000,00
				Valor Estimado Total	**R$2.861.000,00**

Fonte: https://www.tjam.jus.br/index.php/publicacoes-documentos/resolucoes-publicacoes-doc/Divisoes-Setores-e-Varas.415/setor-de- desenvolvimento/governanca/gestao/plano-de-contratacoes-e-aquisicoes/2023-15/antivirus/31888-antivirus-etp-pdf/file

11.3. Em seu ETP, o TJ-AM não explorou outras opções utilizando um ETP simplificado e direcionando para o produto Antivírus Kaspersky pelo período de 36 meses, catser 369285. Declarando:

> "Considerando todo o exposto acima, esta Secretaria de Tecnologia da Informação e Comunicação declara que aquisição de uma Solução de Proteção de Endpoints da fabricante Kaspersky se faz necessária e é viável, dada a necessidade de manter o padrão de proteção atualmente utilizado neste tribunal e reforçar a segurança digital do ambiente da rede corporativa do TJAM".

11.4. **b) Tribunal de Justiça do Maranhão:**

Fonte: https://www.tjma.jus.br/financas/downacordo.php?acordo=pe_0008/2023&tpAcordo=L&anodoc=2023&nrTermo=pm

11.5. O TJ-MA explorou a opção de substituir e renovar por versão superior, sua conclusão foi técnica:

> Instalar uma nova plataforma de antivírus de outro fabricante necessitaria de grandes esforços na sua execução, tendo em vista o tempo necessário para o estudo de elaboração dos artefatos para contratação de uma nova solução, o tempo e gasto necessários para a equipe técnica dominar a nova solução, bem como o tempo e custo de adaptação e treinamento dos usuários na nova solução e por fim, o tempo e a complexidade de implantação da nova solução nos servidores e endpoints;

11.6. Atualmente, o TJ-MA possui licenças perpétuas do software antivírus Kaspersky Endpoint Security for Business SELECT, adquiridas por meio do Processo nº 16418/2019 - TJ-MA.

11.7. **As alternativas do Mercado:**

11.7.1. Ao demonstrar a intenção de compra, através do PCA (ID:0046974964) e de publicação no site da SEPOG (ID:0043655401), tivemos as seguintes fabricantes dentre as cotações apresentadas:

11.7.2. **Empresa Clear:**

- Solução de Proteção para Servidores Físicos ou Virtuais;

11.7.3. **Empresa Partnerone e Solor:**

- Solução de Proteção para Estação de Trabalho;

11.7.4. **Empresa Bitdefender**

- Solução de Proteção para Estação de Trabalho.

11.7.5. **A existência de softwares disponíveis conforme descrito na Portaria STI/MP nº 46, de 28 de setembro de 2016, e suas atualizações;**

- O Software Público Brasileiro é um tipo específico de software livre que atende às necessidades de modernização da administração pública. Há no portal 69 (sessenta e nove) sistemas, no entanto, não foram identificados softwares que possam atender às necessidades dos setores demandantes.

11.8. **As políticas, os modelos e os padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico - ePing, Modelo de Acessibilidade em Governo Eletrônico - eMag, Padrões Web em Governo Eletrônico - ePwg, padrões de Design System de governo, Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil, quando aplicáveis:**

- Este tópico foi detalhado através da tabela "Quadro de requisitos " nos itens 7 e 8.

11.9. **Das necessidades de adequação do ambiente do órgão ou entidade para viabilizar a execução contratual (exemplo: mobiliário, instalação elétrica, espaço adequado para prestação do serviço, etc):**

- Infraestrutura tecnológica: Não há necessidade de adequação da infraestrutura tecnológica da SEPOG.
- Infraestrutura elétrica: Não se aplica.
- Logística de implantação: Não se aplica.
- Espaço físico: Não se aplica.
- Mobiliário: Não se aplica.
- Impacto ambiental**:** Não se aplica

11.10. **Dos diferentes modelos de prestação do serviço:**

- **Licenciamento de Software**: Esta é a forma tradicional de fornecimento, onde a organização adquire licenças de software para instalar nos dispositivos de sua rede. As licenças podem ser adquiridas com base no número de usuários, dispositivos ou assinaturas anuais**;**
- **Software como Serviço (SaaS)**: Muitas empresas oferecem soluções de antivírus baseadas em nuvem, onde o software é hospedado remotamente e acessado pela organização por meio de assinaturas de serviço. Essas soluções geralmente são escaláveis e oferecem atualizações automáticas**;**
- **Appliance de Segurança**: Algumas empresas oferecem dispositivos físicos que incluem software antivírus pré-instalado. Esses appliances podem ser implantados na rede da organização para proteger o tráfego de entrada e saída. A SEPOG já usa essa solução e a demanda pretendida vem para somar com essa defesa atuando diretamente na ultima instancia o equipamento do usuário**;**
- **Integração com Plataformas de Segurança Maior**: Alguns fornecedores de soluções de segurança mais abrangentes incluem funcionalidades de antivírus em seus produtos. Isso pode incluir firewalls de próxima geração, soluções de detecção e resposta de endpoints (EDR) e sistemas de prevenção de intrusões (IPS), entre outros;
- **Gratuitos e de Código Aberto**: Existem também soluções de antivírus gratuitas e de código aberto disponíveis, embora nem sempre ofereçam o mesmo nível de funcionalidade ou suporte que as soluções comerciais.

11.11. **Os diferentes tipos de soluções em termos de especificação, composição ou características dos serviços integrantes**:

Empresa	Produto/Solução	Tipo de Solução
Symantec (Norton)	Norton Antivirus, Norton 360, Norton Internet Security	Licenciamento de Software, SaaS
McAfee	McAfee Total Protection, McAfee LiveSafe	Licenciamento de Software, SaaS
Kaspersky Lab	Kaspersky Anti-Virus, Kaspersky Internet Security	Licenciamento de Software, SaaS
Bitdefender	Bitdefender Antivirus Plus, Bitdefender Total Security	Licenciamento de Software, SaaS
Avast	Avast Free Antivirus, Avast Premium Security	Licenciamento de Software, SaaS
Trend Micro	Trend Micro Antivirus, Trend Micro Maximum Security	Licenciamento de Software, SaaS
Sophos	Sophos Home, Sophos Intercept X	Licenciamento de Software, SaaS, Appliance
ESET	ESET NOD32 Antivirus, ESET Internet Security	Licenciamento de Software, SaaS
Fortinet	Fortinet APP	Licenciamento de Software, SaaS

11.11.1. Contudo, nem todas as empresas demonstraram o interesse em apresentar uma proposta e especificações, algumas até iniciaram o procedimento e pararam de responder, abaixo estão as principais soluções levantadas:

Empresa	Antivírus Corporativo	EDR	XDR
Symantec (Norton)	Symantec Endpoint Protection	Symantec Endpoint Detection and Response	Symantec Extended Detection and Response
McAfee	McAfee Endpoint Security	McAfee MVISION EDR	McAfee MVISION XDR
Kaspersky Lab	Kaspersky Endpoint Security	Kaspersky EDR	Kaspersky XDR
Bitdefender	Bitdefender GravityZone	Bitdefender EDR	Bitdefender XDR
Avast	Avast Business Antivirus	Avast Business EDR	Avast Business XDR
Trend Micro	Trend Micro Apex One	Trend Micro XDR	Trend Micro XDR
Sophos	Sophos Intercept X	Sophos EDR	Sophos XDR
ESET	ESET Endpoint Security	ESET Enterprise Inspector	ESET Enterprise Inspector + EDR
Fortinet	FortiClient	FortiEDR	FortiXDR

11.12. **Da possibilidade de aquisição na forma de contratação como serviço:**

11.12.1. Neste modelo as proposta se confundem no mercado, sendo a única diferença a hospedagem do servidor de administração na nuvem ou em hosts virtuais disponibilizado pela contratante.

- Cessão Temporária de Direitos sobre Locação de Software;
- Software como Serviço (SaaS);

11.12.2. Em todas as formas de contratação a diferença encontra-se na forma de pagamento, que pode ser: mensal, semestral, anual ou 36 (trinta e seis) meses.

11.13. **Da ampliação ou substituição da solução implantada:**

- O processo anterior não foi firmado contrato, inviabilizando a renovação.

11.14. **Das diferentes métricas de prestação do serviço e de pagamento**.

11.14.1. Quando falarmos de governo as principais forma de pagamento são:

- **Pagamento Mensal**: Modelo pouco utilizado.
- **Pagamento Anual**: Este é o modelo mais utilizado no mercado, inclusive pelo Governo.
- **Pagamento por 36 meses**: Este é o modelo padrão utilizado no Governo. Ao observar o mercado podemos verificar uma diminuição de preço ao optarmos por um pagamento antecipado, no caso de anual podendo variar de 10% a 20% de desconto e em 36 meses de 30% a 50%.

11.15. **Possíveis Soluções:**

11.15.1. Com base nos levantamentos do item 10 e seus subitens as seguintes soluções foram levantadas:

ID	DESCRIÇÃO DA SOLUÇÃO (OU CENÁRIO)
1	Solução de Proteção com Tecnologia XDR
2	Solução de Proteção com Tecnologia de VPN ZTNA
3	Solução de Proteção para Servidores Físicos ou Virtuais
4	Solução de Proteção Open source.
5	Solução de Proteção para Estação de Trabalho

12. ANÁLISE COMPARATIVA DAS SOLUÇÕES

12.1. **Solução 1 - Solução de Proteção com Tecnologia XDR**

Esta solução oferece uma abordagem avançada de detecção e resposta estendida (XDR) para a segurança cibernética. O Intercept X Advanced with XDR da Sophos integra recursos de proteção de endpoint (EPP), detecção e resposta de endpoint (EDR) e análise de nuvem para fornecer uma proteção abrangente contra ameaças. No entanto, seu custo é mais elevado, e por incluir recursos adicionais, é necessário um treinamento para os servidores, o que pode tornar a implementação mais onerosa para a Administração.

Esta solução não tem integração com o ambiente Fortinet da SEPOG, onerando a equipe e dificultando a análise em diversos equipamentos, tendo ainda uma proteção insuficiente para os servidores, pois não fornece a robustez necessária contra ransomware e outras ameaças críticas aos servidores.

PONTOS POSITIVOS	PONTOS NEGATIVOS

Integração de várias camadas de segurança.	**Custos mais elevados:** Pode ser mais caro em comparação com soluções tradicionais de antivírus
Análise avançada de ameaças.	**Capacitação:** Pode exigir recursos adicionais de treinamento e gerenciamento.
Detecção e resposta em tempo **real.**	**Incompatibilidade:** Esta solução não tem integração com o ambiente Fortinet da SEPOG, onerando a equipe e dificultando a análise em diversos equipamentos.
Capacidade de correlacionar dados de segurança em toda a infraestrutura.	

12.2. **Solução 2 - Solução de Proteção com Tecnologia de VPN ZTNA**

ZTNA (Zero Trust Network Access) é uma abordagem moderna para a segurança de rede que segue o princípio de "nunca confie, sempre verifique". Em vez de permitir acesso irrestrito a uma rede após a autenticação, como uma VPN tradicional, o ZTNA verifica continuamente a identidade e o contexto de cada usuário ou dispositivo, garantindo que apenas os usuários autorizados tenham acesso aos recursos específicos que precisam.

VPN Fortinet com ZTNA: A Fortinet, conhecida por suas soluções de segurança, integrou a tecnologia ZTNA em suas VPNs para melhorar a segurança e o gerenciamento de acesso. No entanto, tal solução pode exigir um redesenho da arquitetura de rede existente e requer uma infraestrutura de rede compatível. A seguir, demonstramos seus pontos positivos e negativos:

PONTOS POSITIVOS	PONTOS NEGATIVOS
Maior controle acesso à rede.	Requer uma infraestrutura de rede compatível.
Capacidade de implementar políticas de segurança granulares.	Pode exigir um redesenho da arquitetura de rede existente.
Redução de superfície de ataque.	Pode ser mais complexo de implantar e gerenciar.

12.3. **Solução 3 - Solução de Proteção para Servidores Físicos ou Virtuais**

Os ambientes de TI das organizações foram transformados pela mudança para a nuvem e pelas respostas à pandemia da COVID-19. Ao mesmo tempo, os agentes de ameaças cibernéticas tornaram-se mais sofisticados e profissionais, levando a ataques de maior impacto e mais dispendiosos.

Com o trabalho remoto se tornando comum, o endpoint tornou-se a primeira linha de defesa para os programas de segurança cibernética de muitas organizações. Isso significa que esses endpoints são alvo de ataques sofisticados e exigem soluções avançadas de segurança para protegê-los.

As soluções ATP (Advanced Threat Protection) e EDR (Endpoint Detection and Response) são projetadas para fornecer essa proteção avançada. Elas usam uma variedade de soluções de segurança de última geração para identificar ataques cibernéticos no início de seus ciclos de vida, permitindo quebrar a cadeia de ataque e prevenir o ataque antes que ele possa causar danos significativos a um endpoint.

Solução Fortinet de Prevenção Avançada de Ameaças: Esta solução utiliza uma abordagem de proteção avançada de endpoint com a tecnologia de prevenção avançada de ameaças da Fortinet. Ela visa proteger os dispositivos contra uma ampla gama de ameaças conhecidas e desconhecidas, incluindo malware, ransomware e ataques de dia zero.

A segurança do endpoint visa proteger a infraestrutura de TI em geral, protegendo os endpoints como gateways para ela. Como tal, ele protege contra malware e outras ameaças externas. Além de oferecer à equipe de segurança de TI um portal de gerenciamento central, que os ajuda a controlar todos os endpoints e manter a visibilidade. Também permite monitorar áreas problemáticas e movimentação suspeita de tráfego de dados, por meio do gerenciamento centralizado, pode também proteger os terminais de forças de trabalho remotas. A segurança do endpoint pode restringir quais dispositivos podem ou não se conectar aos seus endpoints. Assim, poderá impedir que um USB com uma carga útil de malware malicioso seja instalado em certas portas USB sem permissão. Finalmente, a segurança de endpoint oferece uma infinidade de recursos, sendo tal solução indicada para atender a demanda de Solução de Proteção para servidores.

PONTOS POSITIVOS	PONTOS NEGATIVOS
Detecção proativa de ameaças.	Pode exigir uma curva de aprendizado para administradores de TI
Proteção em tempo real contra ameaças avançadas.	Pode aumentar a carga de processamento nos dispositivos protegidos.
Integração com outros produtos de segurança da Fortinet.	-

Embora a Solução 3 possa apresentar um custo elevado, sua capacidade de resposta imediata e sua abordagem proativa oferecem uma proteção abrangente e essencial para garantir a integridade e a segurança contínua dos sistemas e serviços hospedados nos servidores virtuais ou físicos da SEPOG.

12.4. **Solução 4 - Solução de Proteção Open source:**

Esta solução envolve a implementação de uma solução de antivírus baseada em software de código aberto. Existem várias opções disponíveis, como ClamAV e AVG Antivirus, que oferecem proteção contra ameaças conhecidas. Embora seja uma solução de antivírus gratuita podendo ser atraentes em termos de custo inicial, elas geralmente não oferecem o nível de proteção, suporte e recursos avançados necessários para garantir a segurança eficaz de uma rede corporativa, sendo tal solução não indicada para demanda.

PONTOS POSITIVOS	PONTOS NEGATIVOS
Custo zero de licenciamento	Recursos limitados em comparação com soluções comerciais, suporte.
Transparência do código fonte.	Não oferecem nível de proteção suficiente.
-	Carente de recursos avançados.

12.5. **Solução 5 - Solução de Proteção para Estação de Trabalho:**

O antivírus corporativo é um software de proteção contra ameaças cibernéticas, desenvolvido com mais recursos e robustez do que as soluções voltadas para dispositivos pessoais. Essas ferramentas incluem pacotes de serviços exclusivos para empresas, capacitando-as a lidar com grandes volumes de dados e diversas variedades de ciber ataques.

O objetivo central do antivírus corporativo é detectar e remover ameaças, prevenir o acesso a sites suspeitos para evitar roubos de informações e invasões, e proteger todos os tipos de dispositivos conectados na infraestrutura empresarial, como notebooks, desktops, servidores e dispositivos móveis. Adicionalmente, oferece recursos extras como gestão de sistemas, rastreamento, identificação de vulnerabilidades e correções de falhas.

Conforme apresentado no item 11.11, inúmeras marcas oferecem soluções de antivírus corporativo, incluindo Symantec, McAfee, Bitdefender, Avast, entre outros, sendo tal demanda indicada para atender as Estações de Trabalho da Secretaria de Estado do Planejamento, Orçamento e Gestão - SEPOG.

Atualmente, a SEPOG utiliza a licença do Kaspersky, cuja garantia de atualização expirou no dia 30 de abril de 2024. Após essa data, as licenças deixaram de receber novas versões da solução e atualizações de bases de dados (lista de vírus e vacinas), expondo a SEPOG a novas vulnerabilidades na rede corporativa e à entrada de malwares como vírus e worms, comprometendo a integridade e disponibilidade dos dispositivos computacionais.

PONTOS POSITIVOS	PONTOS NEGATIVOS
Confiabilidade Comprovada: Muitos fornecedores de antivírus corporativo têm um histórico sólido de proteção contra ameaças.	Recursos de Detecção de Ameaças: Algumas soluções podem ser menos avançadas em comparação com as mais recentes no mercado.
Interface de Usuário Intuitiva: Facilita a gestão e operação da solução.	Preocupações com Privacidade de Dados: Certos fornecedores podem ter questões relacionadas à privacidade e origem da empresa.

Ampla Cobertura de Ameaças: Protege contra uma vasta gama de ciberataques.	-

Portanto, considerando a inviabilidade administrativa de não possuir contrato vigente e a expiração da licença anterior, este cenário recomenda que a SEPOG escolha uma nova solução de antivírus corporativo por meio de uma licitação com ampla participação, permitindo que qualquer fabricante possa apresentar sua proposta, com o objetivo de alcançarmos a melhor proposta. Esta abordagem garante maior competitividade e a possibilidade de encontrar soluções mais inovadoras e adaptadas às necessidades da SEPOG.

12.6. **TABELA COMPARATIVA DAS SOLUÇÕES**

Quadro de Requisitos

Requisito	ID Solução	Sim	Não	Não se aplica
A solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1	x		
	2	x		
	3	x		
	4	x		
	5	x		
A Solução está disponível no Portal do Software Público Brasileiro?	1		x	
	2		x	
	3		x	
	4		x	
	5		x	
A Solução é um software livre ou software público?	1		x	
	2		x	
	3		x	
	4		x	
	5	x		
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MAG?	1		x	
	2		x	
	3		x	
	4		x	
	5			x
Design System de governo, Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil	1		x	
	2		x	
	3		x	
	4		x	
	5			x
Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil	1		x	
	2		x	
	3		x	
	4		x	
	5			x

12.6.1. **Requisitos da necessidade de negócio:**

N°	Necessidade de Negócio	1	2	3	4	5
1	Ampliar a disponibilidade dos serviços de TI	x	x	x	x	x
2	Proteção contra malware nas estações de trabalho	x	x	x	x	x
3	Proteção contra malware nos servidores	x	x	x	x	x
4	Filtragem de conteúdos maliciosos	x	x	x	x	x
5	Bloqueio de sites suspeitos	x	x	x	x	x
6	Restrição ao acesso de dispositivos infectados	x	x	x	x	x
7	Prevenção de fraudes em movimentações financeiras	x	x	x	x	x
8	Proteção contra vazamento de informações e perda de dados	x	x	x	x	x
9	Suporte técnico e atualização por 36 meses	x	x	x	x	x

12.6.2. **Dentre os principais *players* de mercado fizemos um comparativo para auxiliar no ETP:**

Antivírus	Principais Recursos	Plataformas Suportadas	Preço	Suporte Técnico
Symantec Endpoint Protection	Proteção avançada contra malware; Firewall; Controle de aplicações	Windows, macOS, Linux	Variável, depende do número de licenças e recursos adicionais	Sim, oferecido por telefone, email e chat
McAfee Total Protection	Proteção contra ameaças em tempo real; Firewal; Proteção de navegação na web	Windows, macOS, Android, iOS	Variável, depende do número de licenças e recursos adicionais	Sim, oferecido por telefone, email e chat
Kaspersky Endpoint Security	Proteção avançada contra malware;- Controle de aplicativos e dispositivos;- Criptografia de dados	Windows, macOS, Linux	Variável, depende do número de licenças e recursos adicionais	Sim, oferecido por telefone, email e chat
Bitdefender GravityZone Business Security	Proteção multicamadas contra malware;- Controle de dispositivos;- Proteção de email	Windows, macOS, Android, iOS	Variável, depende do número de licenças e recursos adicionais	Sim, oferecido por telefone, email e chat
Trend Micro Apex One	Proteção contra ransomware;- Controle de aplicações;- Proteção de e-mail	Windows, macOS, Linux	Variável, depende do número de licenças e recursos adicionais	Sim, oferecido por telefone, email e chat

12.7. **COMPARAÇÃO ENTRE AS SOLUÇÕES:**

Critérios	Solução 1 - XDR	Solução 2 - ZTNA	Solução 3 - Servidores	Solução 4 - Open Source	Solução 5 - Estações de Trabalho
Integração de várias camadas de segurança	Sim	Não	Sim	Não	Sim
Análise avançada de ameaças	Sim	Não	Sim	Não	Sim
Detecção e resposta em tempo real	Sim	Não	Sim	Não	Sim
Maior controle de acesso à rede	Não	Sim	Sim	Não	Não
Redução da superfície de ataque	Não	Sim	Sim	Não	Sim
Confiabilidade comprovada	Sim	Sim	Sim	Não	Sim
Interface de usuário intuitiva	Sim	Não	Sim	Não	Sim
Recursos de detecção de ameaças	Sim	Sim	Sim	Não	Sim
Suporte técnico e atualização	Sim	Sim	Sim	Não	Sim

Critérios	Solução 1 - XDR	Solução 2 - ZTNA	Solução 3 - Servidores	Solução 4 - Open Source	Solução 5 - Estações de Trabalho
Proteção de Servidores Fisicos e Virtuais	Sim	Sim	Sim	Não	Não
Compatibilidade e Integração com Amitente Fortinet	Não	Sim	Sim	Não	Não
Complexidade de implementação e gerenciamento	Alta	Alta	Média	Baixa	Baixa

Considerando a necessidade de proteger 250 equipamentos, incluindo 50 servidores Virtuais ou físico, a SEPOG deve optar por uma solução que ofereça uma proteção abrangente, suporte técnico confiável, e que seja viável economicamente. A recomendação é realizar uma licitação com ampla participação de fornecedores, garantindo competitividade e a possibilidade da melhor contratação diante das necessidades específicas da SEPOG.

Portanto, as melhores soluções levantadas foram:

Solução 3 - **Solução de Proteção para Servidores Físicos ou Virtuais;**

Solução 5 - Proteção para Estações de Trabalho.

13. REGISTRO DAS SOLUÇÕES CONSIDERADAS INVÍAVEIS

ID	DESCRIÇÃO DA SOLUÇÃO (OU CENÁRIO)
1	**Solução de Proteção com Tecnologia XDR**

A solução oferece uma abordagem avançada de detecção e resposta estendida (XDR) para a segurança cibernética, integrando recursos de proteção de endpoint (EPP), detecção e resposta de endpoint (EDR), e análise de nuvem.

Motivos da Inviabilidade:

- **Custos Elevados:** A solução apresenta um custo significativamente mais alto comparado a outras opções disponíveis no mercado.
- **Necessidade de Treinamento Adicional:** Requer capacitação específica para os servidores, o que aumenta o custo e a complexidade da implementação.
- **Infraestrutura Necessária:** Pode demandar ajustes na infraestrutura existente, gerando despesas e complexidade adicional.
- **Incompatibilidade:** Não tem integração com o ambiente Fortinet da SEPOG, onerando a equipe e dificultando a análise em diversos equipamentos.
- **Proteção Insuficiente para Servidores:** Embora ofereça uma abordagem avançada, pode não fornecer a robustez necessária contra ransomware e outras ameaças críticas aos servidores.

2	**Solução de Proteção com Tecnologia de VPN ZTNA**

ZTNA (Zero Trust Network Access) é uma tecnologia moderna de segurança de rede que verifica continuamente a identidade e o contexto de cada usuário ou dispositivo, garantindo acesso apenas aos recursos específicos necessários.

Motivos da Inviabilidade:

- **Infraestrutura Compatível:** Exige uma infraestrutura de rede que suporte a tecnologia ZTNA.
- **Redesenho de Rede:** A implementação pode necessitar de um redesenho completo da arquitetura de rede existente.
- **Complexidade de Gestão:** A solução é mais complexa de implantar e gerenciar, o que pode ser oneroso e demandar recursos adicionais.
- **Conflito com Solução Já Existente:** A SEPOG já possui uma solução de VPN, contudo, a atual solução não fornece os recursos de proteção necessários.
- **Inadequada para Topologia de Rede Atual:** A tecnologia ZTNA pode não se integrar bem com a configuração de rede existente na SEPOG.
- **Alto Custo para Proteção dos Usuários:** O investimento necessário pode ser desproporcional aos benefícios em termos de proteção individual dos usuários.

4	**Solução de Proteção Open source.**

Esta solução envolve a implementação de um antivírus baseado em software de código aberto, como ClamAV e AVG Antivirus, que oferece proteção contra ameaças conhecidas.

Motivos da Inviabilidade:

- **Recursos Limitados:** As soluções de código aberto geralmente não oferecem o mesmo nível de proteção e funcionalidades avançadas comparado às soluções comerciais.
- **Nível de Proteção Insuficiente:** Não atendem às necessidades de segurança da SEPOG para uma rede corporativa.
- **Falta de Suporte Especializado:** A ausência de suporte técnico robusto e atualização contínua limita a eficácia da solução.
- **Atualização em Tempo Real:** Falta de atualizações constantes e em tempo real, essenciais para combater ameaças como ransomware.
- **Proteção Insuficiente para Servidores:** Não fornece a robustez necessária para um ambiente que requer proteção avançada contra ransomware e outras ameaças graves.
- **Limitações de Recursos:** As soluções gratuitas geralmente oferecem recursos básicos de proteção contra malware, muitas vezes não sendo tão abrangentes ou avançadas quanto as soluções pagas.
- **Falta de Recursos de Gerenciamento Centralizado:** Para empresas com várias estações de trabalho ou dispositivos, é essencial ter recursos de gerenciamento centralizado para facilitar a implementação, monitoramento e gerenciamento da segurança.
- **Questões de Conformidade e Regulamentação:** Em certos setores, como saúde, financeiro e governamental, pode haver requisitos específicos de conformidade e regulamentação que exigem o uso de soluções de segurança robustas e certificadas.

14. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

O Custo Total de Propriedade, do inglês *Total Cost of Ownership* – TCO, é um método utilizado para calcular o custo global de um produto ou serviço ao longo de seu ciclo de vida, considerando custos diretos e indiretos. É importante calcular o TCO para ter uma visão mais precisa e abrangente do custo de uma solução, permitindo a comparação entre diferentes soluções e a identificação de oportunidades de redução de custos. Ressalta-se que, mesmo nos casos em que for **identificada uma única solução viável**, deve-se realizar a análise TCO daquela solução a fim de subsidiar a tomada de decisão, pois essa análise poderá prover a dimensão de todos os custos inerentes à sua implantação.

No cálculo do TCO são considerados os custos diretos e indiretos associados à solução, incluindo custos de aquisição, manutenção, suporte técnico, atualizações, treinamento, substituição, entre outros. O ciclo de vida da solução é o período que compreende desde a aquisição ou implementação da solução até o final de sua vida útil, incluindo prorrogações contratuais planejadas. Para se estimar os valores dos componentes de custos relacionados à aquisição de recursos ou prestação de serviços, pode-se utilizar os mecanismos de pesquisa já previstos na Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, ou adotar mecanismos de estimativa específicos, assegurando-se que tais mecanismos estejam descritos no documento ou nos autos do processo. Para se estimar os valores de outras componentes de custos (a exemplo de depreciação, risco de downtime, risco de falhas de segurança, custos administrativos, etc.) pode-se adotar valores constantes de estudos especializados, adequando-os ao caso concreto, ou adotar mecanismos de estimativa específicos, assegurando-se a devido registro e descrição no documento ou nos autos do processo.

14.0.1. SOLUÇÕES CONSIDERADAS INVIÁVEIS

14.0.2. **SOLUÇÃO 1: Solução de Proteção com Tecnologia XDR e,**

14.0.3. **SOLUÇÃO 2: Solução de Proteção com Tecnologia de VPN ZTNA**

Considerando ambas as soluções não atenderem tecnicamente as necessidades desta secretária, tendo em vista a Solução 1 ser incompatível com o ambiente Fortinet da Sepog, não possuir uma solução suficiente para servidores e demandar uma infraestrutura necessária, gerando complexidade adicional e a Solução 2 por ser mais complexa de implantar e gerenciar, podendo ter ainda conflito com a solução VPN já existente na Sepog, dentre outro motivos apresentados no item 13 deste Estudo Técnico Preliminar, não há o que se falar em análise comparativa de custos (TCO), sendo tais soluções desclassificadas tecnicamente.

14.1. SOLUÇÕES CONSIDERADAS VIÁVEIS

14.1.1. **Solução 5 - Solução de Proteção para Estação de Trabalho**

ITEM	EMPRESA	PROPOSTA	UNID.	QUANT.	MÊS

					12	24	36
01	Solor SCANSOURCE BRASIL DISTRIBUIDORA DE TECNOLOGIAS LTDA. CNPJ 05.607.657/0008-01	KASPERSKY 0051365720	Licença	200	R$36.420,00	R$58.304,00	R$91.304,00
02	M3 Comércio Software LTDA CNPJ: 20.040.746/0001-36	BITDEFENDER 0051032413	Licença	200	R$54.000,00	R$78.000,00	R$102.000,00
03	**PARTNERONE COMERCIO E SERVICOS EM INFORM- ATICA LTDA CNPJ: 11.439.893/0001-92**	**(0051302145) KASPERSKY**	**Licença**	**200**	**R$ 25.900,00**	**R$41.440,00**	**R$64.840,00**

14.1.2. **Solução 3 - Solução de Proteção para Servidores Físicos ou Virtuais**

ITEM	EMPRESA	PROPOSTA	UNID.	QUANT.	MÊS		
					12	24	36
01	**SOLUÇÃO 3: Solução de Proteção para Servidores Físicos ou Virtuais**	**(0051752611) FORTINET**	**Pacote 25 Licença**	**2**	**R$48.769,00**	**R$97.583,00**	**R$146.306,00**

14.2. **COMPARATIVO DE VALORES**

Durante a fase de coleta de informação, a equipe da ASTIC iniciou a avaliação de alguns sistemas para proteger seus dados, tanto para atender a LGPD, quanto para proteger os ativos "INFORMAÇÃO E DADOS", dentre os possíveis fornecedores se destacaram as marcas KASPERSKY, BITDEFENDER e FORTINET, com a tabela abaixo é possível constatar que a aquisição da solução coorporativa é financeiramente mais vantajosa.

Na tabela abaixo temos o comparativo entre as diversas formas de serviço para Solução de Proteção para Estação de Trabalho:

ITEM	SOLUÇÃO	PROPOSTA	UNID.	QUANT.	MÊS		
					12	24	36
01	SOLUÇÃO 5: Solução de Proteção para Estação de Trabalho	(0051365720) KASPERSKY	Licença	200	R$36.420,00	R$58.304,00	R$91.304,00
02	SOLUÇÃO 5: Solução de Proteção para Estação de Trabalho	(0051032413) BITDEFENDER	Licença	200	R$54.000,00	78.000,00	102.000,00
03	**SOLUÇÃO 5: Solução de Proteção para Estação de Trabalho**	**(0051302145) KASPERSKY EDR**	**Licença**	**200**	**R$25.900,00**	**R$41.440,00**	**R$ 64.840,00**

14.2.1. Ao analisar a proposta podemos observar os valores pelo período de 12 (doze) meses até 36 (trinta e seis) meses de contrato, a tabela abaixo detalha (apenas no valor da licença), o investimento a longo prazo:

CONTRATO	12	24	36	TOTAL A LONGO PRAZO	ECONOMIA
ANUAL	R$25.900,00	R$25.900,00	R$25.900,00	R$77.700,00	0
2 ANOS	R$41.440,00		R$41.440,00	R$82.880,00	0
3 ANOS	R$64.840,00			R$64.840,00	R$18.040,00

14.2.2. Desta forma, podemos afirmar que havendo previsão e orçamento, ao longo prazo é mais vantajoso optar pelo modelo de 36 meses de contrato, cuja a economia nesse período seria em torno de R$18.040,00 (dezoito mil, oitocentos e quarenta reais) para os cofres públicos.

14.3. Na tabela abaixo temos o comparativo entre os valores de 12 meses a 36 meses de serviço para Solução de Proteção para Servidores Físicos e Virtuais:

ITEM	SOLUÇÃO	PROPOSTA	UNID.	QUANT.	MÊS		
					12	24	36
04	SOLUÇÃO 3: Solução de Proteção para Servidores Físicos ou Virtuais	(0051752611) FORTINET	Pacote 25 Licença	2	R$48.769,00	R$97.583,00	R$146.306,00

14.3.1. Ao analisar a proposta podemos observar os valores pelo período de 12 (doze) meses até 36 (trinta e seis) meses de contrato, a tabela abaixo detalha (apenas no valor da licença), o investimento a longo prazo:

CONTRATO	12	24	36	TOTAL A LONGO PRAZO	ECONOMIA
ANUAL	R$48.769,00	R$48.769,00	R$48.769,00	R$146.307,00	0
2 ANOS	R$97.583,00		R$97.583,00	R$195.166,00	0
3 ANOS	R$146.306,00			R$146.306,00	R$1,00

14.3.2. **A vantajosidade da compra de 50 licenças para servidor na opção de 36 meses, é essencial a considerar alguns pontos estratégicos:**

1. **Economia a Longo Prazo:** A aquisição para 36 meses representa uma economia em relação às renovações anuais ou bienais. Considerando que o custo total para 12 meses é R$ 48.769,00 (quarenta e oito mil, setecentos e sessenta e nove reais), a cada renovação anual o valor total ao longo de três anos seria de R$ 146.307,00 (cento e quarenta e seis mil, trezentos e sete reais). O custo para 24 meses é de R$ 97.583,00 (noventa e sete mil, quinhentos e oitenta e três reais), o que, se renovado, também resultaria em um valor superior à opção de 36 meses. Optando pela contratação direta por 36 meses ao valor de R$ 146.306,00 (cento e quarenta e seis mil, trezentos e seis reais), evita-se um aumento potencial de custos por conta de reajustes anuais.
2. **Proteção Contra Reajustes:** A contratação de licenças por um período mais longo protege o governo de possíveis reajustes de preços no mercado, que podem ocorrer por inflação, variações cambiais ou mudanças nas políticas de preços dos fornecedores.
3. **Planejamento Orçamentário:** Optar pelo contrato de 36 meses facilita o planejamento orçamentário, pois permite fixar um valor conhecido e evitar surpresas financeiras em futuros exercícios. Isso é particularmente vantajoso para a administração pública, onde a previsibilidade de despesas é crucial.
4. **Redução de Custos Operacionais e Administrativos:** A renovação de contratos anualmente ou bienalmente implica custos administrativos adicionais, incluindo tempo de análise, elaboração de documentos e processos de aprovação. Ao escolher o contrato de 36 meses, esses custos são significativamente reduzidos.
5. **Continuidade do Serviço:** A contratação por um período mais longo garante a continuidade do serviço, evitando possíveis interrupções que poderiam ocorrer durante processos de renovação ou aquisição de novas licenças.

14.3.3. Portanto, a escolha do contrato de 36 meses é mais vantajosa tanto do ponto de vista econômico quanto do operacional, alinhando-se com os princípios de economicidade e eficiência que norteiam a administração pública.

14.4. **VALOR DA LICENÇA ESTAÇÃO VS SERVIDOR VITUAL OU FÍSICO**

ITEM	SOLUÇÃO	PROPOSTA	VALOR UNITÁRIO (1 LICENÇA 36 MESES)
01	SOLUÇÃO 5: Solução de Proteção para Estação de Trabalho	(0051103889) KASPERSKY	R$319,56
01	SOLUÇÃO 5: Solução de Proteção para Estação de Trabalho	(0051032413) BITDEFENDER	R$510,00
01	SOLUÇÃO 5: Solução de Proteção para Estação de Trabalho	(0051302145) KASPERSKY EDR	R$324,20
02	SOLUÇÃO 3: Solução de Proteção para Servidores Físicos ou Virtuais	(0051752611) FORTINET	R$ 2.926,12

A razão pela qual é necessário investir financeiramente mais em licença para antivírus de servidor virtuais ou físico do que em licença para estação de trabalho envolve vários fatores relacionados à complexidade e criticidade da proteção necessária para servidores em comparação com estações de trabalho.

Abaixo segue alguns pontos chave que explicam e demonstram essa diferença de custo:

1. **Maior Risco e Criticidade**:

- Servidores geralmente hospedam aplicativos críticos, armazenam dados sensíveis e servem como ponto central de operações de rede. Portanto, eles são alvos mais atraentes para ataques cibernéticos.
- Uma falha de segurança em um servidor pode ter impactos mais severos, incluindo a perda de dados críticos, interrupções no serviço e violações de segurança que afetam toda a organização.

2. Funcionalidades Adicionais:

- As soluções de antivírus para servidores geralmente incluem funcionalidades adicionais que não são necessárias em estações de trabalho, como controle de aplicações, segurança de rede, proteção contra intrusões e monitoramento em tempo real de alto desempenho.
- Elas também podem oferecer proteção especializada para ambientes de virtualização e servidores em nuvem.

3. Desempenho e Escalabilidade:

- As soluções de proteção para servidores são otimizadas para lidar com cargas de trabalho pesadas e múltiplas conexões simultâneas, o que requer uma arquitetura mais robusta e eficiente.
- Eles precisam ser capazes de funcionar sem comprometer o desempenho do servidor, o que exige um software mais sofisticado e poderoso.

4. Suporte e Manutenção:

- As licenças de antivírus para servidores geralmente incluem níveis mais altos de suporte técnico e manutenção, o que pode incluir suporte 24/7, atualizações frequentes e assistência especializada para resolução de problemas complexos.
- O custo do suporte técnico para servidores tende a ser mais elevado devido à necessidade de intervenções rápidas e soluções customizadas.

5. Compliance e Regulações:

- Servidores frequentemente devem cumprir normas e regulamentos de segurança mais rigorosos, o que implica em requisitos adicionais de segurança e conformidade.
- Isso inclui auditorias de segurança, relatórios detalhados e a capacidade de atender a padrões específicos, como PCI DSS, HIPAA, GDPR, entre outros.

Por fim, cabe destacar que a licença para antivírus de servidor virtual ou físico, será para proteger o hardware em nuvem e o hardware físico, respectivamente.

14.4.1. **DA ESCOLHA**

Ao pensar em um servidor virtuais ou físicos, temos o que segue:

Fator	Solução Antivírus Gratuita	Solução Antivírus Paga
Proteção contra Malware	Geralmente oferece proteção básica contra malware, com atualizações menos frequentes e abrangentes	Oferece proteção avançada contra malware, com atualizações regulares e automáticas para proteção contínua
Suporte Técnico	Geralmente oferece suporte técnico limitado ou inexistente	Oferece suporte técnico dedicado e especializado, ajudando a resolver problemas de segurança de forma rápida e eficaz
Atualizações de Segurança	As atualizações de software podem ser menos frequentes ou abrangentes, aumentando o risco de exposição a ameaças cibernéticas	Oferece atualizações regulares e automáticas de software, garantindo proteção contínua contra as últimas ameaças
Recursos e Funcionalidades	Pode carecer de recursos avançados e personalizáveis, deixando a rede corporativa mais vulnerável a ameaças sofisticadas	Oferece uma ampla gama de recursos e funcionalidades avançadas, essenciais para proteger eficazmente a rede corporativa
Conformidade com Regulamentações	Pode não atender aos requisitos específicos de conformidade e regulamentação em setores regulamentados, como saúde, financeiro e governamental	Geralmente está em conformidade com as regulamentações de segurança de dados e privacidade, ajudando a evitar multas e penalidades por não conformidade
Risco de Tempos de Inatividade	Pode haver maior risco de tempos de inatividade devido a problemas de segurança não resolvidos ou dificuldades na resolução de problemas sem suporte técnico dedicado	Menor risco de tempos de inatividade devido a problemas de segurança, com suporte técnico dedicado disponível para resolver problemas de forma rápida e eficaz
Custo de Recuperação de Incidentes de Segurança	Pode resultar em custos indiretos mais elevados associados à recuperação de incidentes de segurança devido à falta de suporte técnico e atualizações de segurança inadequadas	Custos de recuperação de incidentes de segurança potencialmente menores, graças ao suporte técnico dedicado e atualizações regulares de segurança

Essa tabela destaca as diferenças significativas no nível de risco e exposição entre o uso de soluções antivírus gratuitas e pagas.

Embora as soluções gratuitas possam parecer atraentes em termos de custo inicial, elas vêm geralmente com riscos adicionais relacionados à proteção, suporte técnico e conformidade com regulamentações, que podem resultar em custos indiretos mais elevados a longo prazo. Por outro lado, as soluções pagas oferecem proteção mais abrangente, suporte técnico dedicado e atualizações regulares de segurança, o que pode ajudar a mitigar esses riscos e reduzir o TCO geral.

Para avaliarmos melhor o impacto na escolha precisamos comparar os riscos de segurança entre soluções antivírus desktop (usuários) e soluções para um servidor TI, focando em aspectos como proteção contra *malware*, suporte técnico, atualizações de segurança, recursos e funcionalidades, conformidade com regulamentações, risco de tempo de inatividade e custo de recuperação de incidentes.

Categoria	Solução Antivírus Desktop	Solução Antivírus Servidor	Observações
Proteção contra Malware	Baixa	Alta	As soluções para servidores geralmente oferecem proteção mais robusta e abrangente contra malwares, incluindo ransomware e ataques direcionados.
Suporte Técnico	Limitado ou inexistente	Dedicado e especializado	O suporte técnico dedicado para soluções de servidor garante ajuda rápida e eficaz na resolução de problemas de segurança.
Atualizações de Segurança	Menos frequentes ou abrangentes	Regulares e automáticas	As atualizações frequentes garantem que os servidores estejam protegidos contra as últimas ameaças.
Recursos e Funcionalidades	Básicos	Avançados e personalizáveis	As soluções para servidores oferecem recursos como firewalls, controle de acesso e criptografia, além de proteção contra malware.
Conformidade com Regulamentações	Pode não atender a requisitos específicos	Geralmente em conformidade com regulamentações de segurança de dados e privacidade	A conformidade com a LGPD e outras regulamentações é crucial para evitar multas e sanções.
Risco de Tempo de Inatividade	Alto	Baixo	A indisponibilidade dos servidores pode ter um impacto significativo nas operações da organização.
Custo de Recuperação de Incidentes de Segurança	Elevado	Potencialmente menor	As soluções para servidores podem ajudar a reduzir os custos de recuperação de incidentes de segurança.

Considerando o objetivo da escolha de uma solução de antivírus ideal para atender as necessidades específicas da SEPOG, para a solução de um servidor virtuais ou físicos oferecem um nível de proteção e confiabilidade superior, mas podem ter um custo mais elevado. É importante avaliar os riscos e benefícios de cada opção antes de tomar uma decisão.

Conforme exposto, para este TCO, o mais viável é separar a compra em Estações de Trabalho (usuários) e em Servidores e virtuais ou físicos.

Há um grande número de fornecedores no mercado nacional que oferecem bens e serviços prontos para aquisição, sem necessidade de customizações ou adaptações. Essa ampla oferta elimina a necessidade de uma comparação detalhada entre fornecedores, pois qualquer empresa que atenda à solicitação pode participar do processo de fornecimento.

14.4.1.1. **Da análise:**

Após uma análise pormenorizada das soluções de antivírus disponíveis, considerando robustez, segurança, viabilidade e custos, recomendamos que seja separado em dois itens, conforme a seguir:

Item 1: Estações de Trabalho (usuários) sendo necessário 200 (duzentas) licenças.

- Foco em soluções com bom custo-benefício e alta escalabilidade.
- Considerar a integração com a infraestrutura de TI existente.
- Priorizar soluções que ofereçam proteção contra as principais ameaças cibernéticas.
- Para este item considerando requisitos de qualidade, segurança e economicidade, **a solução 5 é a mais viável**.

Item 2: Licença de Antivírus para equipamento do tipo Servidor - 50 (cinquenta) licenças.

- Priorizar soluções com alto nível de segurança e robustez.
- Considerar recursos avançados de proteção, como firewalls de aplicativos web (WAF) e criptografia de dados.
- Avaliar a capacidade de integração com soluções de backup e recuperação de desastres.
- Para este item, a economia de recurso frente ao possível dano as informações inverte a prioridade para uma solução mais robusta e ativa, **a qual seria a solução 3**.

Benefícios da Licitação sem Direcionamento no item 1:

- Maior competitividade entre fornecedores, resultando em custos mais baixos.
- Possibilidade de encontrar soluções mais inovadoras e customizadas para as necessidades da SEPOG.
- Abertura para novas tecnologias e abordagens de segurança.

Benefícios da Licitação com Direcionamento no item 2:

- Maior segurança e integração de solução nos ativos importantes que operam 24x7.

14.4.1.2. **Conclusão:**

A decisão de implementar a solução 3 (Solução de Proteção para Servidores Físicos ou Virtuais) nos ativos do Data Center da SEPOG foi baseada na necessidade de garantir uma proteção eficaz para um ambiente crítico e altamente ativo. Ao contrário das soluções corporativas convencionais, que tendem a ser reativas e lidam com ameaças após a ocorrência de uma ação do usuário, os servidores de TI hospedam serviços essenciais, sistemas vitais e operam continuamente. Diante disso, é fundamental contar com uma proteção mais robusta e proativa, capaz de detectar e responder imediatamente a qualquer anomalia ou ameaça em tempo real. Embora a solução 3 (Solução de Proteção para Servidores Físicos ou Virtuais) possa, aparentemente, apresentar um custo mais elevado, sua capacidade de resposta imediata e sua abordagem proativa oferecem uma proteção abrangente e essencial para garantir a integridade e a segurança contínua dos sistemas e serviços hospedados nos servidores da SEPOG.

Por fim, a recomendação da Solução 5 para as estações de trabalho baseia-se no fato de que o antivírus corporativo é um software de proteção contra ameaças cibernéticas, desenvolvido com mais recursos e robustez do que as soluções voltadas para dispositivos pessoais. Antivírus para usuários finais são mais simples, focando na defesa contra sites maliciosos, spam e outras ameaças comuns. Já as soluções corporativas incluem pacotes de serviços exclusivos para empresas, capacitando-as a lidar com grandes volumes de dados e diversas variedades de ciberataques.

15. LEVANTAMENTO DE PREÇO

15.1. A memória de cálculo para obtenção de valores para a contratação foi realizado pelo Núcleo de Contratos e Licitações - NCL/SEPOG, na qual foi enviado e-mail's para empresas interessadas, conforme cotações apresentadas no item 14.1, ainda, houve publicação no site SEPOG e pesquisa no Banco de Preços (0047909420), demonstrado de acordo com o Quadro Comparativo (0051371227), no qual chegou-se aos referidos valores:

15.2. Conforme informações abaixo, registra-se a estimativa do valor da Contratação de TIC:

Item	Descrição	Unid.	Quant.	Valor Unitário	Valor Total
01	Antivírus - Estação de trabalho pelo período de 36 meses	Licença	200	R$210,00	R$42.000,00
02	Licença de Antivírus para equipamento do tipo Servidor pelo período de 36 meses (sendo 25 licenças por pacote)	Pacote	02	R$73.153,00	R$146.306,00

15.3. No item 2, o produto é ofertado em pacote de 25 licenças, justificando assim o quantitativo de 2 unidades.

16. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

16.1. **ITEM 1: SOLUÇÃO DE ANTIVÍRUS COORPORATIVA PARA ESTAÇÃO DE TRABALHO (USUÁRIOS):**

2. Licenciamento:

- Licenciamento válido por 36 meses;
- Inclui manutenções corretivas e atualizações sem custos adicionais para a SEPOG durante o ciclo de vida do software indicado pelo fabricante;
- Idioma deve ser em português.

2. Compatibilidade:

- Compatível com os seguintes sistemas operacionais;
- Microsoft Windows Server 2008 R2;
- Microsoft Windows Server 2016;
- Microsoft Windows Server 2019;
- Microsoft Windows Server 2022;
- Microsoft Windows 7 (todas as edições, 32 e 64 bits);
- Microsoft Windows 8.1 (todas as edições, 32 e 64 bits);
- Microsoft Windows 10 (todas as edições, 32 e 64 bits).
- Microsoft Windows 11 (todas as edições, 32 e 64 bits).

3. Características:

- Possuir console de gerenciamento baseada no modelo cliente/servidor acessada WEB, todo o custo de instalação é por conta da contratada exceto sistemas operacional
- Deve permitir atribuição de perfis para os administradores da solução;
- Expirada sua validade o produto deverá permanecer funcional contra códigos maliciosos utilizando das definições até o momento da expiração da licença;,
- Possuir ferramenta de remoção de soluções antivírus próprio ou de outros fabricantes;
- Capacidade de instalar e desinstalar remotamente a solução de antivírus, com integração ao Active Directory, incluindo descobrimento de máquinas com ou sem agente;
- A console deve permitir visualizar o número total de licenças gerenciadas;
- A console deve ter a capacidade de gerar relatórios em HTML ou PDF, visualizar eventos e gerenciar políticas;
- Capacidade de atualizar os pacotes de instalação com as últimas vacinas;
- Capacidade de desinstalar remotamente qualquer software da ferramenta nas máquinas cliente;
- Capacidade de definir diferentes políticas de configuração para grupos de estações;
- Capacidade de fornecer informações básicas sobre os computadores: se o antivírus está instalado, iniciado, atualizado, última conexão com o servidor administrativo, tempo desde a última atualização das vacinas, sistema operacional etc; Capacidade de enviar e-mail em caso de determinados eventos, como ocorrência de vírus etc;
- Capacidade de escolher quais módulos serão instalados em cada cliente ou grupo de clientes;
- Capacidade de adicionar aplicativos a uma lista de "aplicativos confiáveis";
- Capacidade de agendar varreduras nos clientes;
- Capacidade de acesso remoto nos clientes;
- Prover segurança para estações de trabalho, sejam físicas ou em ambiente virtualizado;
- Possuir console de gerenciamento que permita realizar configurações do antivírus, antispyware, firewall, detecção de intrusão, controle de dispositivos e controle de aplicações;
- O produto deverá ter a capacidade de remoção do software de antivírus já instalado e ser instalado de forma remota pela console de gerenciamento;
- As licenças não deve fazer distinção de servidor (Windows Server, File Serve, Linuz) e estação de trabalho.

- As licenças do antivírus deverá ser a última versão do mercado.

16.2. **ITEM 2: LICENÇA DE ANTIVÍRUS PARA EQUIPAMENTO DO TIPO SERVIDOR FÍSICO OU VIRTUAL POR 36 MESES:**

- SOLUÇÃO DE DETEÇÃO E RESPOSTA

1. Características gerais

- A solução deve conter políticas de segurança e playbooks básicos pré-definidos, sem que haja a necessidade de criação manual;
- A solução deve possuir integração nativa com soluções de controle de acesso;
- A solução deve possuir integração nativa com soluções de SIEM (Security Information and Event Management);
- A solução deve possuir integração nativa com soluções de firewall;
- A solução deve permitir o isolamento de um dispositivo através da integração de um NAC de acordo com a categoria do evento detectado;
- A solução deve permitir adicionar endereços IP maliciosos detectados em um ou mais firewalls remotos integrados;
- A solução deve exigir que uma senha seja desabilitada por aplicativo de terceiros;
- A solução deve permitir a configuração de perfis nas informações coletadas para a função de pesquisa de ameaças;
- A solução deve permitir exclusões de informações que não serão coletadas na função de pesquisa de ameaças;
- A solução deve ser certificada pela Microsoft como uma solução de antivírus e ser capaz de se integrar com o Windows Security Center;
- A solução deve entregar informações geradas pelos serviços de inteligência na nuvem para a tomada de decisão sobre um evento detectado;
- A solução deve permitir que os serviços em nuvem recategorizem uma classificação de evento;
- A solução deve permitir que os administradores desabilitem as notificações para um evento de descoberta;
- A solução deve permitir que as funções de filtragem da web sejam realizadas bloqueando o acesso a páginas da web categorizadas como maliciosas;
- A solução deve identificar e prevenir tentativas de elevação de privilégios;
- A solução deve bloquear ataques de ransomware conhecidos;
- A solução deve ter a capacidade de descobrir dispositivos IOT não gerenciados na rede;
- A solução deve ter a capacidade de detectar dispositivos não gerenciados e protegidos pela solução com sistemas operacionais Linux e Windows.

2. Características da Console de Administração

- A console de gerenciamento deve permitir a integração com o “Active Directory” para garantir o cumprimento dos requisitos da política de senhas da organização;
- A console de gerenciamento deve permitir o uso de autenticação de dois fatores (2FA);
- A console de gerenciamento deve permitir a integração com SAML para autenticação de usuários;
- A console de gerenciamento deve permitir o uso de funções granulares para administradores;
- A console de gerenciamento deve permitir o gerenciamento por meio de API;
- A console de gerenciamento deve permitir a visualização dos eventos registrados nos dispositivos que requeiram atenção;
- A console de gerenciamento deve permitir a visualização do estado dos agentes instalados;
- A console de gerenciamento deve permitir a desinstalação remota do agente instalado nos dispositivos;
- A console de gerenciamento deve permitir a desativação/ativação remota do agente instalado nos dispositivos;
- A console de gerenciamento deve permitir a criação de relatórios executivos contendo um resumo que descreva os eventos de segurança e o status do sistema;
- A console de gerenciamento deve permitir a criação de grupos organizacionais de dispositivos nos quais cada grupo possa ter regras de proteção independentes dos demais;
- A console de gerenciamento deve permitir a exportação dos logs locais gerados pelos agentes;
- A console de gerenciamento deve permitir a criação de relatórios de inventário dos agentes contendo informações como: Endereço IP, Nome do Host, Sistema Operacional, Endereço MAC, Versão do Agente, Status do Agente;
- A console de gerenciamento deve ter visibilidade dos eventos gerados pelos dispositivos ou eventos de acordo com o processo executado;
- A console de gerenciamento deve permitir a integração de um SMTP externo para envio de alertas por e-mail;
- A console de gerenciamento deve permitir auditorias de alterações feitas por administradores/operadores. Essas auditorias também devem poder ser exportadas em formato CSV.

3. características do agente de proteção

- A solução deve ser compatível com os seguintes sistemas operacionais:
- Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 e 2022;
- RedHat Enterprise Linux e CentOS 6.8 ou superior, 7.2 ou superior, 8 ou superior e 9 ou superior;
- Ubuntu Server 16.04, 18.04, 20.04 e 22.04;
- Oracle Linux 6.10, 7.7 ou superior e 8.2 ou superior.
- A solução deve ser compatível com ambientes de Virtual Desktop Infrastructure (VDI) em VMware Horizons 6 e 7 e Citrix XenDesktop 7;
- A solução deve ter um consumo máximo de 350 MB de memória RAM;
- A solução deve ter um consumo médio de menos de 2% do uso da CPU;
- A solução deve ter a capacidade de atualizar o agente sem interação do usuário e sem exigir uma reinicialização;
- A solução deve ter proteção “anti-violação” no agente;
- A solução deve funcionar sem depender de assinaturas hash locais conhecidas para a detecção de arquivos maliciosos;
- A solução deve ser capaz de registrar em tempo real informações do processo e informações adicionais;
- A solução deve ter a opção de definir uma senha para desinstalar o agente;
- A solução deve ser capaz de gerar um instalador para Windows pré-configurado. Esta configuração deve permitir a instalação sem a necessidade de interação ou configuração por parte do usuário;
- O agente deve ser capaz de funcionar através de um proxy.

4. funcionalidades de detecção de malware

- A solução deve ser capaz de funcionar no modo “offline” sem que o agente esteja conectado à rede corporativa;
- A solução deve ser capaz de detectar, eliminar e retornar ao seu valor inicial as alterações feitas por processos maliciosos no registro do Windows;
- A solução deve ser capaz de detectar conexões de rede a partir do dispositivo;
- A solução deve ser capaz de incorporar inteligência de ameaças ao esquema de detecção;
- A solução deve ser capaz de incorporar as técnicas do MITRE ATT&CK no esquema de detecção e mostrar quais dessas técnicas foram utilizadas;
- A solução deve ter a capacidade de pesquisar ameaças em Sistema Operacional Windows usando indicadores de comprometimento (IOC), como: nome, hash e ações relacionadas a arquivos (Criação, Exclusão, Renomear);
- A solução deve ter a capacidade de pesquisar ameaças em Sistema Operacional Windows usando indicadores de comprometimento (IOC), como ações relacionadas a processos (Terminação de Processo, Criação de Processo, Carregamento de Executáveis)
- A solução deve ter a capacidade de pesquisar ameaças em Sistema Operacional Windows usando indicadores de comprometimento (IOC), como ações relacionadas ao uso da rede (Socket Connect, Socket Close, Socket Brind);
- A solução deve ter a capacidade de pesquisar ameaças em Sistema Operacional Windows usando indicadores de comprometimento (IOC), como ações relacionadas log de eventos;
- A solução deve ter a capacidade de pesquisar ameaças em Sistema Operacional Windows usando indicadores de comprometimento (IOC), como ações relacionadas ao registro do Sistema Operacional (criação de chave, exclusão de chave, conjunto de valores);
- A solução deve ter a capacidade de realizar consultas para filtrar as informações disponíveis para pesquisa de ameaças;
- A solução deve ter capacidade de armazenar pesquisas realizadas para serem reutilizadas no futuro;

- A solução deve ter a capacidade de agendar pesquisas armazenadas;
- A solução deve identificar atividades maliciosas conhecidas;
- A solução deve ter a capacidade de receber atualizações diárias de inteligência;
- A solução deve ter a capacidade de classificar os eventos detectados em diferentes categorias.

5. funcionalidades de prevenção de malware

- A solução deve ter a capacidade de prevenir a execução de arquivos maliciosos;
- A solução deve incorporar mecanismo de proteção baseado no kernel do sistema operacional, com capacidade de “Aprendizado de Máquina” (Machine Learning);
- A solução deve ter a capacidade de controlar dispositivos USB;
- A solução deve ter a capacidade de criar exceções para dispositivos USB com base no nome do dispositivo;
- A solução deve ter a capacidade de criar exceções para dispositivos USB com base no fornecedor do dispositivo;
- A solução deve ter a capacidade de criar exceções para dispositivos USB com base no número de série do dispositivo;
- A solução deve ter a capacidade de criar exceções para dispositivos USB com base em uma combinação de: nome do dispositivo, fornecedor, número de série;
- A solução deve ser capaz de bloquear o tráfego malicioso de exfiltração de dados;
- A solução deve ser capaz de bloquear tráfego de comunicação malicioso para C&C (Comando e Controle);
- A solução deve ser capaz de impedir violações de segurança e tentativas de ransomware em tempo real;
- A solução deve ser capaz de evitar a criptografia causada por ransomware e modificação de arquivos ou registro de dispositivos. Caso isso ocorra, a solução deverá restaurar os arquivos afetados/modificados para o seu estado original em tempo real;
- A solução deve permitir que as políticas nela contidas sejam modificadas permitindo vários estados tais como: ativo, inativo ou apenas criar “logs”;
- A solução deve ser capaz de ser configurada em modo onde nenhum bloqueio é feito, mas todas as atividades maliciosas são registradas;
- A solução deve ser capaz de permitir a modificação das regras de detecção de eventos maliciosos de forma que essas regras apenas armazenem um registro ou fiquem em modo de bloqueio;
- A solução deve ser capaz de permitir verificações periódicas dos arquivos contidos nos dispositivos com o agente instalado.

6. Funcionalidades de difusão (pós-infecção)

- A solução deve permitir o isolamento automático do tráfego de rede de um dispositivo onde foi encontrada atividade causada por malware
- A solução deve permitir alterar as políticas atribuídas de um dispositivo onde foi encontrada atividade causada por malware;
- A solução deve permitir o bloqueio de atividades realizadas por arquivos maliciosos;
- A solução deve ter a capacidade de criar exceções para processos com base na localização do arquivo (caminho do arquivo);
- A solução deve ter a capacidade de criar exceções para processos com base no destino do tráfego gerado por este;
- A solução deve ter a capacidade de criar exceções para os processos baseados no usuário que o executou;
- A solução deve ter a capacidade de criar exceções manualmente para falsos positivos e evitar a ocorrência de ocorrências futuras;
- A solução deve ter a capacidade de reclassificar automaticamente a atividade como um falso positivo e evitar a ocorrência de detecções semelhantes;
- A solução deve permitir a criação de exceções de eventos com base em endereços IP, aplicações e protocolos.
- Funcionalidades de resposta a incidente
- A solução deve armazenar metadados gerados pelos dispositivos para que possam ser usados em investigações forenses;
- A solução deve permitir a integração com soluções de SIEM através de um syslog;
- A solução deve ter a capacidade de obter instantâneos ou “dumps” de memória que permitam a realização de processos forenses;
- A solução deve ter a capacidade de abrir tickets em plataformas de gerenciamento como ServiceNow e JIRA;
- A solução deve permitir a integração através de API onde tem a capacidade de entregar informações geradas em um evento como: endereço IP, nome do host, usuário, data/hora ocorrida, atividade suspeita etc.;
- A solução deve ter a capacidade de encerrar um processo com base em sua classificação;
- A solução deve ter a capacidade de excluir um arquivo com base em sua classificação;
- A solução deve ter a capacidade de restaurar as configurações de registro básicas com base na classificação de atividade predefinida;
- A solução deve ter a capacidade de isolar os dispositivos infectados da rede;
- A solução deve ter a capacidade de restringir automaticamente o acesso do dispositivo à rede de acordo com a classificação do processo detectado;
- A solução deve obter visibilidade total da cadeia de ataques e alterações maliciosas;
- A solução deve permitir a limpeza automática do dispositivo e reverter alterações maliciosas, mantendo o tempo de atividade do dispositivo;
- A solução deve permitir o envio de executáveis para análise em um sandbox, a fim de determinar se são maliciosos ou inofensivos;
- A solução deve possuir integração com Active Directory a fim de possibilitar a utilização de playbooks para resposta a incidentes de segurança;
- A solução deve fornecer vários mecanismos de proteção, incluindo o encerramento de um processo, a exclusão de um arquivo malicioso e o bloqueio de uma conexão de rede.
- Funcionalidades de controle de vulnerabilidades e comunicação.

7. A solução deve ter a capacidade de descobrir aplicativos que estão se comunicando através da rede e que representam risco para o dispositivo;

- A solução deve ter capacidade para realizar um patch virtual, através da restrição de acessos nas aplicações vulneráveis
- A solução deve permitir a redução das superfícies de ataque utilizando políticas de comunicação proativas baseadas no risco de acordo com o CVE e a qualificação ou reputação que uma aplicação possa ter;
- A solução deve ter a capacidade de impedir que aplicativos não autorizados se comuniquem pela rede;
- A solução deve ter a capacidade de criar políticas que tenham a capacidade de impedir a comunicação de aplicativos de acordo com a versão do aplicativo instalado;
- A solução deve ser capaz de detectar e identificar todas as aplicações nos dispositivos que se comunicam na rede;
- A solução deve ser capaz de fornecer informações sobre o uso de aplicativos de rede mostrando, por exemplo, quais dispositivos geram tráfego para um aplicativo e os destinos IP do tráfego gerado pelo aplicativo.
- A solução de referência adotada nesta especificação técnica se baseia no modelo FortiEDR;
- A citação de modelo se pauta da necessidade da oferta da licitantes ser totalmente integrada com os ativos FORTINET presentes em nosso ambiente, composto de diversas soluções da referida fabricante.

17. JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO

17.1. A escolha da solução antivírus paga em vez da gratuita pode ser justificada por várias razões técnicas:

- **Proteção Avançada contra Ameaças** : As soluções antivírus pagas geralmente oferecem uma proteção mais avançada contra uma ampla gama de ameaças cibernéticas. Isso inclui detecção mais precisa de malware, capacidade de identificar ameaças emergentes e proteção contra ataques sofisticados como ransomware e ataques de dia zero.
- **Atualizações Regulares e Automáticas** : As soluções antivírus pagas geralmente fornecem atualizações de segurança regulares e automáticas. Isso garante que o software esteja sempre atualizado com as últimas definições de vírus e técnicas de detecção, reduzindo o risco de exposição a novas ameaças.
- **Suporte Técnico Especializado**: As soluções antivírus pagas geralmente incluem suporte técnico dedicado e especializado. Isso é crucial em caso de problemas de segurança, pois fornece acesso a especialistas que podem ajudar a resolver rapidamente questões críticas e minimizar o tempo de inatividade.
- **Recursos Adicionais de Segurança**: Muitas soluções antivírus pagas oferecem recursos adicionais de segurança, como firewalls, proteção de navegação na web, controle de aplicativos e proteção de identidade. Esses recursos adicionais ajudam a fortalecer as defesas de segurança da rede corporativa.
- **Conformidade com Regulamentações**: Em setores regulamentados, como saúde, financeiro e governamental, a escolha de uma solução antivírus paga pode ajudar a garantir a conformidade com as regulamentações de segurança de dados e privacidade. Isso pode evitar multas e penalidades por não conformidade
- **Gestão Centralizada e Relatórios**: Muitas soluções antivírus pagas oferecem recursos avançados de gestão centralizada e relatórios. Isso permite que os administradores de TI monitorem e gerenciem facilmente a segurança da rede corporativa, identifiquem tendências de ameaças e demonstrem conformidade com regulamentações.

17.2. Em resumo, a escolha de uma solução 3 e 5 é justificada pela necessidade de uma proteção mais avançada, atualizações regulares, suporte técnico especializado, conformidade com regulamentações e recursos adicionais de segurança.

18. JUSTIFICATIVA ECONÔMICA DA ESCOLHA DA SOLUÇÃO

18.1. A escolha econômica de uma solução antivírus paga pode ser justificada considerando-se diversos fatores, incluindo a conformidade com a Lei Geral de Proteção de Dados (LGPD) e os custos totais de propriedade (TCO) a longo prazo. Aqui está uma justificativa econômica para a escolha de uma solução antivírus pago:

- **Conformidade com a LGPD**: A LGPD exige que as empresas protejam adequadamente os dados pessoais dos usuários, o que inclui implementar medidas de segurança adequadas para prevenir acessos não autorizados, vazamentos e outras violações de dados. Optar por uma solução antivírus paga pode fornecer recursos de segurança mais robustos e atualizados, ajudando a garantir a conformidade com os requisitos da LGPD e a evitar multas e penalidades associadas a violações de dados
- **Redução do Risco de Violações de Dados**: Soluções antivírus pagas geralmente oferecem proteção mais avançada contra ameaças cibernéticas, atualizações regulares de segurança e suporte técnico dedicado. Isso pode reduzir significativamente o risco de violações de dados, perda de dados e interrupções no negócio, que podem resultar em custos substanciais, incluindo multas, perda de reputação e perda de clientes.
- **Suporte Técnico Especializado**: As soluções antivírus pagas frequentemente incluem suporte técnico dedicado, que pode ajudar a resolver rapidamente problemas de segurança e minimizar o tempo de inatividade. Isso pode resultar em economias significativas de custos, especialmente em caso de incidentes de segurança que exigem uma resposta rápida e eficaz.
- **Recursos Avançados de Segurança** : As soluções antivírus pagas geralmente oferecem recursos adicionais de segurança, como firewall, proteção de navegação na web, controle de aplicativos e proteção de identidade. Esses recursos podem ajudar a fortalecer as defesas de segurança da empresa e reduzir o risco de violações de dados.
- **Custos Totais de Propriedade (TCO)** : Embora as soluções antivírus pagas possam ter um custo inicial mais alto em comparação com as soluções gratuitas, uma análise abrangente do TCO pode revelar que elas oferecem melhor valor a longo prazo. Isso se deve aos recursos adicionais, atualizações regulares, suporte técnico dedicado e redução do risco de violações de dados, que podem resultar em custos indiretos mais baixos ao longo do tempo.

18.2. Em resumo, escolher uma solução 3 e 5 pode ser uma decisão econômica inteligente, considerando os benefícios adicionais de segurança, conformidade com a LGPD, suporte técnico dedicado e custos totais de propriedade a longo prazo.

19. JUSTIFICATIVAS DE PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Durante este Estudo Técnico Preliminar, ao avaliar a vantajosidade econômica em confronto com as características técnicas necessárias, decidiu-se fracionar o objeto em dois itens:

- Licença corporativa de antivírus para as estações de trabalho e,
- Licença de antivírus Proteção para Servidores Físicos ou Virtuais.

Esse fracionamento foi realizado para garantir a melhor proteção possível, considerando as diferentes necessidades e níveis de criticidade dos sistemas envolvidos.

Uniformidade do software antivírus: A uniformidade do software antivírus é essencial para assegurar uma proteção eficaz contra ameaças cibernéticas. Dividir ainda mais as licenças entre diferentes fornecedores comprometeria essa uniformidade, criando potenciais conflitos de compatibilidade e gerenciamento que poderiam reduzir a eficácia da segurança implementada.

Gerenciamento Centralizado: Um único ponto focal de gerenciamento é crucial para a administração eficiente das políticas de segurança, atualizações e monitoramento de eventos. A utilização de consoles de gerenciamento distintas para diferentes soluções de antivírus resultaria em complexidade administrativa, aumento da carga de trabalho e potenciais falhas na gestão da segurança.

Integração e Compatibilidade:
Assegurar a integração e compatibilidade de diferentes sistemas de antivírus é uma tarefa complexa que pode introduzir vulnerabilidades na infraestrutura de TI. A segmentação atual de software antivírus para estações de trabalho e outra para sistemas críticos, já considera essas questões, e uma divisão adicional não seria viável.

Eficiência e Efetividade: A contratação de software antivírus para estações de trabalho é uma licença robusta para sistemas críticos assegura a eficiência e efetividade na proteção cibernética. Isso facilita o suporte técnico, a implementação de atualizações e a manutenção contínua dos sistemas de segurança.

Parcelamento do Objeto: O parcelamento do objeto, conforme dimensionado por este ETP, é inviável para a administração, pois comprometeria a completa integração do antivírus e a centralização do gerenciamento, suporte e garantia.

Licenças para Estação de Trabalho e Servidores TI: A segmentação realizada, diferenciando licenças para estações de trabalho e para servidores de TI, atende às necessidades técnicas específicas de cada ambiente. Essa divisão já representa o máximo nível de segmentação viável, garantindo a proteção adequada e a gestão eficiente dos sistemas.

Impossibilidade de Segmentação Adicional:

Segmentar ainda mais as licenças não é possível, pois isso fragmentaria a segurança, tornando-a menos eficaz e mais difícil de administrar. Manter a segmentação atual é crucial para garantir a integridade e a eficácia da proteção cibernética oferecida.

Portanto, o parcelamento do objeto foi cuidadosamente considerado durante o Estudo Técnico Preliminar. A decisão de dividir as licenças em duas partes, uma para estações de trabalho e outra para sistemas críticos, foi tomada para assegurar a melhor proteção e gestão possíveis. Qualquer segmentação adicional comprometeria a uniformidade e a eficiência das licenças, tornando-a inviável para a administração pública. Portanto, a segmentação atual deve ser mantida para garantir a proteção integral dos sistemas e dados institucionais.

20. RESULTADOS PRETENDIDOS

20.1. **Segurança Aprimorada**: A implementação de uma solução atualizada e mais eficaz garantirá uma proteção mais robusta contra as ameaças cibernéticas, reduzindo o risco de comprometimento da infraestrutura e dos dados da SEPOG.

20.2. **Continuidade dos Serviços**: Ao proteger os ativos computacionais contra vírus e malwares, a SEPOG pode manter a continuidade dos serviços essenciais oferecidos à população, evitando interrupções indesejadas devido a incidentes de segurança.

20.3. **Proteção de Dados Sensíveis**: A solução de proteção contribuirá para a preservação da integridade, confidencialidade e disponibilidade das informações sensíveis gerenciadas pela SEPOG, garantindo sua segurança contra acessos não autorizados.

20.4. **Redução de Riscos e Custos**: Ao mitigar o risco de ataques cibernéticos e possíveis consequências, como perda de dados ou danos à reputação da instituição, a SEPOG pode evitar custos associados à recuperação de incidentes de segurança e possíveis multas por não conformidade com regulamentações.

20.5. **Conformidade com Normas e Regulamentações**: A implementação de uma solução de proteção atualizada pode ajudar a SEPOG a manter a conformidade com as regulamentações de segurança de dados e privacidade, mitigando potenciais penalidades por não cumprimento.

20.6. **Aumento da Produtividade**: Ao reduzir o tempo gasto em lidar com incidentes de segurança e manter a infraestrutura de TI operando de forma segura, os funcionários da SEPOG podem se concentrar mais em suas tarefas principais, aumentando a produtividade geral da instituição.

20.7. **Proteção Contra Ameaças Cibernéticas**

- **Descrição:** Antivírus ajudam a detectar e neutralizar uma ampla gama de ameaças, incluindo vírus, malwares, ransomwares e trojans.
- **Benefício:** Reduz o risco de infecções que podem comprometer dados e sistemas críticos.

20.8. **Segurança dos Dados**

- **Descrição:** Protege dados sensíveis e confidenciais contra acessos não autorizados e violações.
- **Benefício:** Garante a privacidade e a integridade das informações pessoais e institucionais.

20.9. **Manutenção da Integridade dos Sistemas**

- **Descrição:** Previne a corrupção de dados e a interferência em operações normais dos sistemas.
- **Benefício:** Assegura que os sistemas funcionem corretamente e que os dados permaneçam precisos e confiáveis.

20.10. **Prevenção de Interrupções de Serviço**

- **Descrição:** Evita que ataques cibernéticos causem interrupções nos serviços e sistemas da SEPOG.
- **Benefício:** Mantém a continuidade dos serviços públicos, evitando downtime e garantindo que os cidadãos possam acessar serviços essenciais sem interrupções.

20.11. **Redução de Custos com Recuperação**

- **Descrição:** Minimiza os custos associados à recuperação de dados e sistemas após um ataque cibernético.
- **Benefício:** Economiza recursos públicos e reduz o tempo necessário para a recuperação completa de sistemas comprometidos.

20.12. **Cumprimento de Normas e Regulamentações**

- **Descrição:** Ajuda a SEPOG a cumprir com exigências legais e regulamentares, como a Lei Geral de Proteção de Dados (LGPD).
- **Benefício:** Evita penalidades legais e mantém a conformidade com normas de segurança da informação.

20.13. **Aumento da Confiança dos Usuários**

- **Descrição:** Demonstrar um compromisso com a segurança cibernética aumenta a confiança dos cidadãos e dos servidores nos sistemas e serviços da SEPOG.
- **Benefício:** Fortalece a reputação da SEPOG como uma entidade responsável e confiável.

20.14. **Monitoramento e Relatórios**

- **Descrição:** Antivírus modernos oferecem ferramentas de monitoramento contínuo e relatórios detalhados sobre a segurança dos sistemas.
- **Benefício:** Fornece insights valiosos para aprimorar continuamente a estratégia de segurança cibernética da SEPOG.

21. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

Não se faz necessário proceder com outras contratações para se atingir ao fim almejado neste processo.

22. PROVIDÊNCIAS A SEREM ADOTADAS

22.1. Elaboração de Termo de Referência;

22.2. Instrumento Convocatório;

22.3. Celebração de contrato;

22.4. Portaria designando gestores e fiscais de contrato.

23. CRITÉRIOS DE SUSTENTABILIDADE

A contratação de licenças de software, em sua essência, não gera impacto ambiental significativo devido à sua natureza predominantemente virtual e intangível. Tais sistemas, alinhados ao paradigma da digitalização, operam primordialmente em ambientes digitais, onde a manipulação de dados e o processamento de informações ocorrem sem a necessidade de recursos materiais tangíveis.

Este fenômeno é corroborado pela abstração inerente à produção de conteúdo audiovisual por meio de soLwares, onde a criação, edição e renderização de elementos visuais e sonoros são realizados mediante algoritmos computacionais, prescindindo de materiais Isicos que possam resultar em resíduos ou degradação ambiental. Ademais, a natureza itera/va e virtual dos processos criativos e de pós-produção envolvidos nestes softwares favorece a minimização do consumo de recursos naturais e energia.

Além disso, a substituição gradual de processos analógicos por soluções digitais tem contribuído para a redução do consumo de papel, tinta, solventes e outros materiais tradicionalmente associados à produção e distribuição de mídia audiovisual, promovendo, assim, uma pegada ambiental mais leve e sustentável.

Portanto, a contratação de licença de softwares não apenas atesta uma abordagem tecnológica avançada e eficiente, mas também se destaca como uma prática que converge harmoniosamente com os imperativos contemporâneos de conservação e preservação ambiental.

24. RISCOS

24.1. No sentido de ponderar e mitigar riscos implícitos no serviço ora pleiteado, nas fases de planejamento, seleção de fornecedores e gestão de contratos, foi elaborado o Mapa de Riscos que pode ser visualizado no documento (0048233556).

25. PARTICIPAÇÃO DE PESSOAS FÍSICAS

Cumpre apontar que conforme o Estudo Técnico Preliminar, não se vislumbrou a possibilidade de exclusão de pessoas físicas, conforme previsto no art. 34, XIV do Decreto nº 28.874/2024.

No caso do licitante ser pessoa física deverá apresentar a documentação conforme previsto na INSTRUÇÃO NORMATIVA SEGES/ME Nº 116, DE 21 DE DEZEMBRO DE 2021.

26. DA PROTEÇÃO DE DADOS PESSOAIS - LEI N 13.709/2018 - LGPD

26.1. A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 13.709, estabelece uma série de princípios e requisitos relacionados à segurança dos dados pessoais. O respeito à segurança dos dados é de extrema importância por várias razões:

- **Proteção dos Direitos Individuais:** A LGPD visa proteger os direitos e liberdades dos titulares dos dados pessoais. Isso significa que as informações pessoais de indivíduos devem ser tratadas de forma a evitar acessos não autorizados, prevenindo assim a violação de seus direitos à privacidade e à proteção de dados.
- **Prevenção à Fraude e à Segurança do Titular:** A lei permite o tratamento de dados sensíveis quando necessário para garantir a prevenção à fraude e a segurança dos titulares. Isso é fundamental para proteger as pessoas contra crimes e atividades fraudulentas.
- **Pesquisas em Saúde Pública:** A LGPD reconhece a importância das pesquisas em saúde pública, mas exige que esses dados sejam tratados em ambiente controlado e seguro, garantindo a confidencialidade e a segurança das informações dos indivíduos envolvidos.
- **Responsabilidade:** A lei estabelece a responsabilidade dos controladores e operadores de dados pessoais em garantir a segurança da informação. Qualquer violação de segurança que resulte em danos aos titulares de dados é de responsabilidade do controlador ou operador.
- **Relatório de Impacto à Proteção de Dados:** A autoridade nacional de proteção de dados pode exigir que as organizações elaborem relatórios de impacto à proteção de dados, incluindo a descrição das medidas de segurança adotadas. Isso incentiva as empresas a investirem em segurança da informação.
- **Obrigações Permanentes:** A LGPD estabelece que a obrigação de garantir a segurança dos dados pessoais continua mesmo após o término do tratamento dos dados. Isso significa que as organizações devem manter a segurança das informações mesmo após sua utilização inicial.

26.2. Em resumo, a LGPD enfatiza a importância da segurança dos dados pessoais como um elemento essencial para a proteção dos direitos individuais, a prevenção de fraudes, a pesquisa em saúde pública e a responsabilidade das organizações. Adotar medidas de segurança adequadas não apenas ajuda a cumprir a lei, mas também constrói a confiança dos titulares de dados e protege a reputação das organizações.

27. POSICIONAMENTO CONCLUSIVO

Com base nas análises detalhadas realizadas neste Estudo Técnico Preliminar (ETP), a equipe de planejamento recomenda a adoção das seguintes soluções para a proteção da infraestrutura de TI da SEPOG:

27.1. **Solução 3 - Proteção para Servidores Físicos ou Virtuais (50 Licenças)**

A Solução 3 foi selecionada por sua capacidade de fornecer um nível superior de segurança para os servidores da SEPOG. Esta solução oferece proteção robusta para os dados críticos armazenados e processados nos servidores da organização. A sua eficácia comprovada contra uma ampla gama de ameaças cibernéticas e sua conformidade com as regulamentações de segurança de dados fazem dela a escolha ideal para proteger os ativos de TI mais sensíveis da SEPOG.

27.2. **Solução 5 - Proteção para Estações de Trabalho (200 Licenças)**

A Solução 5 foi escolhida para proteger as estações de trabalho dos funcionários da SEPOG contra ameaças cibernéticas. Esta solução garante a segurança dos dados e sistemas utilizados nas operações diárias da organização. Sua robustez na proteção contra malware, ransomware e ataques de phishing, juntamente com suas atualizações automáticas e suporte especializado, fornecerá uma camada adicional de segurança essencial para a infraestrutura de TI da SEPOG.

27.3. **Divisão por Itens**

Durante a análise dos cenários, foi identificado que a solução ideal envolve a divisão dos itens para licitar os recursos necessários para servidores e estações de trabalho, conforme descrito a seguir:

- **Item 1 (Solução 5 - Antivírus Corporativo para Estações de Trabalho):** Aquisição de 200 licenças para implementar a Solução 5 nas estações de trabalho dos funcionários da SEPOG pelo período de 36 meses.
- **Item 2 (Solução 3 - Licença de Antivírus para Servidores Virtuais e Físicos):** Aquisição de 50 licenças para implementar a Solução 3 em servidores virtuais e físicos da SEPOG pelo período de 36 meses.

27.4. **Motivação Técnica**

- **Proteção Especializada:** A Solução 3 oferece recursos avançados de segurança projetados especificamente para servidores, garantindo uma defesa robusta contra ameaças cibernéticas direcionadas a esses sistemas críticos.
- **Ampla Cobertura:** A Solução 5 foi escolhida por sua capacidade de fornecer proteção abrangente para as estações de trabalho, abordando uma variedade de ameaças, desde malware comum até ataques mais sofisticados como phishing e ransomware.
- **Atualizações e Suporte:** Ambas as soluções garantem atualizações contínuas e suporte técnico especializado, assegurando que a infraestrutura de segurança da SEPOG esteja sempre atualizada e preparada para enfrentar novas ameaças.

27.5. **Motivação Econômica**

- **Valor de Longo Prazo:** Embora a Solução 3 possa ter um custo inicial mais alto devido à sua especialização em servidores, seu valor a longo prazo é justificado pela proteção aprimorada que oferece aos dados críticos da organização.
- **Eficiência e Produtividade:** A Solução 5 proporciona uma proteção robusta de forma econômica, garantindo a continuidade das operações e minimizando os custos associados a interrupções causadas por ameaças cibernéticas.

27.6. **Conclusão**

Com base em todas as considerações apresentadas, a equipe de planejamento recomenda enfaticamente a contratação das soluções 3 - Proteção para Servidores Físicos ou Virtuais e 5 - Proteção para Estações de Trabalho, e sugere a realização do processo licitatório na modalidade de pregão eletrônico, conforme detalhado nos itens acima.

Essas soluções são cruciais para garantir uma segurança robusta e abrangente para a SEPOG, protegendo seus dados e sistemas contra as mais recentes ameaças cibernéticas, garantindo a conformidade com as regulamentações de segurança de dados e proporcionando um retorno positivo do investimento a longo prazo.

Por fim, muito embora não seja objetivo do ETP apontar a forma de contratação da melhor solução apresentada, sugerimos pela Contratação de Licença de Antivírus para a Proteção de Servidores Físicos ou Virtuais e Proteção para Estações de Trabalho por realização de Processo Licitatório na modalidade Pregão Eletrônico, cujo critério de julgamento será o de menor preço.

28. **RESPONSÁVEIS**

Portaria nº 279 de 14 de junho de 2024 (0051100695), de Comissão de Planejamento de Contratação de bens e serviços no âmbito da Secretaria de Estado Planejamento, Orçamento e Gestão - SEPOG.

Cidade, data e hora do sistema.

Elaboração:

JEANE KARINE GONÇALVES COLARES

Assessora/SEPOG-NCLCC

Revisão:

MARCELO MATOS LIMA

Assessor responsável pela ASTIC

Portaria nº 83 de 07 de fevereiro de 2024 (0045869660)

APROVO:

ESTEFANE FERREIRA ESTEVAM MARINHO

Diretora Executiva da Secretaria de Estado do Planejamento, Orçamento e Gestão - SEPOG

Delegação de Competência da Portaria nº 210 de 02 de maio de 2024

Documento assinado eletronicamente por **Estefane Ferreira Estevam Marinho**, **Diretor(a) Executivo(a)**, em 16/08/2024, às 11:30, 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 **Jeane Karine Gonçalves Colares**, **Assessor(a)**, em 16/08/2024, às 11:49, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **Marcelo Matos Lima**, **Assessor(a)**, em 16/08/2024, às 12:31, 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 **0051127927** e o código CRC **F2503F75**.

Referência: Caso responda este(a) Estudo Técnico Preliminar, indicar expressamente o Processo nº 0035.003501/2023-45 SEI nº 0051127927

Processo - 0035.000618/2024-58							
ITEM DE VERIFICAÇÃO	**RISCOS**	**PROBABILIDADES**	**CONSEQUÊNCIAS**	**NÍVEL DE RISCO**	**AÇÕES SUGERIDAS**	**AÇÕES DE CONTINGÊNCIA**	**OBSERVAÇÕES**
1	Falha em identificar corretamente os requisitos de segurança da organização. - Escolha inadequada de critérios de seleção da solução antivírus. - Ausência de consideração sobre a conformidade com regulamentações, como a LGPD.	Rara	relevante	**Médio**	Realizar uma análise detalhada dos requisitos de segurança e envolver os stakeholders relevantes na definição dos critérios de seleção. - Consultar especialistas em segurança cibernética para garantir a conformidade com regulamentações aplicáveis	Substituir membros da equipe de planejamento que não estejam tendo rendimento e capacitar os servidores escolhidos para o planejamento.	
2	Problemas de compatibilidade da solução com a infraestrutura existente da organização. - Falhas na configuração e integração da solução, resultando em lacunas na proteção antivírus. - Resistência dos usuários finais à adoção da nova solução.	Rara	Muito relevante	**Alto**	Realizar testes de compatibilidade e integração antes da implementação em larga escala. -	Fornecer treinamento e suporte adequados aos usuários finais para garantir uma adoção suave da nova solução.	
3	Interrupções no serviço devido a falhas no sistema antivírus, resultando em possível exposição a ameaças cibernéticas. - Atualizações de segurança não aplicadas em tempo hábil, deixando a rede vulnerável a novas ameaças. - Falta de treinamento adequado para os administradores de TI na operação e manutenção da solução	frequente	Muito relevante	**Extremo**	Implementar procedimentos de backup e redundância para minimizar o impacto de possíveis interrupções no serviço. - Estabelecer um plano de gestão de patches e atualizações para garantir que as atualizações de segurança sejam aplicadas de forma rápida e eficiente. -	Oferecer treinamento contínuo aos administradores de TI para garantir que estejam atualizados com as melhores práticas de operação e manutenção da solução	

GOVERNO DO ESTADO DE RONDÔNIA
Secretaria de Estado do Planejamento, Orçamento e Gestão - SEPOG

SAMS

Órgão Requisitante: **SECRETARIA DE ESTADO DO PLANEJAMENTO, ORÇAMENTO E GESTÃO - SEPOG**

Exposição de Motivo**:** Contratação de TIC - Serviço Comum

Nº do processo: 0035.003501/2023-45

ITEM	Descrição	Unidade	Quantidade	Período - 12 meses	Período - 24 meses	Período - 36 meses
01	**Antivírus Corporativo para Estação de Trabalho -** conforme especificação técnica do Adendo ANEXO I (0051097159)	Licença	200			
02	**Licença de Antivírus para equipamento do tipo Servidor físico ou virtual por 36 meses -** conforme especificação técnica do Adendo ANEXO I (0051097159)	Pacote com 25 licenças (cada)	02			

Carimbo do CNPJ/CPF-ME:	Local:	Responsável pela cotação da Empresa:	**USO EXCLUSIVO DA ACP/GC/SEPOG**	Valor da Proposta:
	Data:	Fone:		Validade Proposta:
	Banco: Agência: C/C:	Assinatura:		Prazo de Entrega:

Elaborado:
Roberta Silva dos Santos

ESTEFANE FERREIRA ESTEVAM MARINHO

Diretora Executiva da Secretaria de Estado do Planejamento, Orçamento e Gestão - SEPOG

Delegação de Competência da Portaria nº 210 de 02 de maio de 2024

Documento assinado eletronicamente por **Estefane Ferreira Estevam Marinho**, **Diretor(a) Executivo(a)**, em 20/09/2024, 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 **0052986162** e o código CRC **97DED0ED**.

Referência: Caso responda este(a) SAMS, indicar expressamente o Processo nº 0035.003501/2023-45 SEI nº 0052986162

Governo do Estado de RONDÔNIA

Superintendência Estadual de Compras e Licitações
Coordenadoria de Pesquisa e Análise de Preços

ITEM	DESCRIÇÃO	UNID	QUANT.(A)	EMP 1	EMP 2	EMP 3	EMP 4	EMP 5	EMP 6	EMP 7	PREÇO MÍNIMO (D)	PREÇO MÉDIO (E)	PREÇO MEDIANO (F)	DESVIO PADRÃO	COEFICIENTE DE VARIAÇÃO	PARAMETRO UTILIZADO (MÍNIMO/MÉDIO)	SUBTOTAL ANUAL (12 MESES)	SUBTOTAL GERAL (24 MESES)	SUBTOTAL GERAL (36 MESES)
1	Antivírus Corporativo para Estação de Trabalho	UNIDADES	200	181,68	195,00	215,00	129,50	182,10	NC	126,33	126,33	R$ 171,60	181,89	35,96	20,95%	MÉDIO	R$ 34.320,00	R$ 68.640,00	R$ 102.960,00
2	Licença de Antivírus para equipamento do tipo Servidor físico ou virtual	PCT C/25	2	34.425,00	20.970,75	NC	NC	NC	24.384,50	37.991,50	20.970,75	R$ 29.442,94	29.404,75	8.067,73	27,40%	MEDIANA	R$ 58.809,50	R$ 117.619,00	R$ 176.428,50

VALOR TOTAL (12 MESES)	R$	93.129,50
VALOR TOTAL (24 MESES)	R$	186.259,00
VALOR TOTAL (36 MESES)	R$	279.388,50

LEGENDA: PARA O ITEM 2, VALORES UNITÁRIOS FORAM MULTIPLICADOS POR 25, PARA FORMAR O PACOTE SOLICITADO EM SAMS
NC = Não encontrado

NOTA EXPLICATIVA: PARA ITEM 2 EMP6, VER MEMÓRIA DE CÁLCULO (Página 2).

IDENTIFICAÇÃO DAS COTAÇÕES		
	EMP1	BANCO DE PREÇOS
	EMP2	BANCO DE PREÇOS
	EMP3	BANCO DE PREÇOS
	EMP4	PARTNERONE - CNPJ: 11.439.893/0001-92
	EMP5	SECURITY INFO - CNPJ: 17.866.425/0001-80
	EMP6	CLEARIT - CNPJ: 30.088.923/0001-08
	EMP7	ATA DE REGISTRO DE PREÇOS Nº01/2024 - ITI

1) NC
2) As descrições foram reduzidas neste quadro comparativo, porém se encontra completas no termo de referência.