Governo do Estado de
RONDÔNIA

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

ATA

ATA DE REGISTRO DE PREÇOS Nº xxx/202X/SUPEL_RO			
Origem:	Pregão Eletrônico nº 90236/2025		
Data da Homologação:	xx/xx/xxxx	Processo nº	0036.028242/2024-36
Órgão Participante:	XXXXX		
Órgão gerenciador:	Superintendência Estadual de Compras e Licitações - SUPEL		

1. **CLÁUSULA I – IDENTIFICAÇÃO DO(S) FORNECEDOR(S) REGISTRADO(S).**

1.1. A identificação dos detentores está inserida no anexo único desta ata.

2. **CLÁUSULA II – DO OBJETO**

2.1. O objeto da presente licitação é contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da Secretaria de Estado da Saúde - SESAU/RO, por um período de 3 (três) anos, por meio do **Sistema de Registro de Preços**, conforme condições, quantidades e exigências estabelecidas no Termo de Referência - Anexo I. conforme condições, quantidades e exigências estabelecidas no Termo de Referência - Anexo I.

3. **CLÁUSULA III – DA VALIDADE DA ATA DE REGISTRO DE PREÇOS**

3.1. A validade desta ata de registro de preços será de 1(um) ano, contados a partir da publicação no Diário Oficial do Estado, e poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso, mediante pesquisa de mercado que leve em consideração os parâmetros fixados no art. 51 do Decreto Estadual n° 28.874/2024.

4. **CLÁUSULA IV – DA UTILIZAÇÃO DESTA ATA DE REGISTRO DE PREÇOS POR ÓRGÃO NÃO PARTICIPANTE**

4.1. A adesão ao presente Registro de Preços fica condicionada ao atendimento das determinações do Estado de Rondônia após autorização expressa do órgão gerenciador – Superintendência Estadual de Compras e Licitações – SUPEL.

4.2. A adesão fica ainda condicionada às exigências dispostas no art. 124, § 1º ao § 8º do Decreto Estadual n° 28.874/2024, em consonância com o art. 86 da Lei nº 14.133, de 1º de abril de 2021.

4.3. As aquisições ou as contratações adicionais (caronas) não poderão exceder, por órgão ou entidade, 50% (cinquenta por cento) dos quantitativos dos itens registrados na ata de registro de preços, ressalvado o disposto no art. 86, § 7°, da Lei Federal n° 14.133, de 2021.

4.4. O conjunto de solicitações de adesão, independentemente do órgão ou entidade solicitante, não poderá exceder ao limite global de duas vezes o quantitativo registrado.

5. **CLÁUSULA V – DA REVISÃO E CANCELAMENTO DO REGISTRO**

5.1. Os preços registrados poderão ser revisto em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução tal como pactuado, observada a instrução processual respectiva, cabendo ao órgão gerenciador promover as negociações junto aos fornecedores, conforme disposto no art. 133 do Decreto Estadual n° 28.874 de 25 de janeiro de 2024.

5.2. Os preços registrados serão mantidos inalterados por todo o período de vigência da Ata de Registro de Preços - ARP, admitida sua revisão para majorar ou minorar os preços registrados em casos excepcionais, nas hipóteses legais e considerando os preços vigentes de mercado.

5.3. A revisão de preços precederá de requerimento: I - do detentor da ata, que deverá fazê-la antes do pedido de fornecimento e, instruindo seu pedido com documentação probatória de majoração de preço do mercado e a oneração de custos; ou II - pelo órgão participante ou órgão interessado, comprovando por meio de pesquisas de preços que há minoração do valor originalmente registrado.

5.4. Quando o preço inicialmente registrado, por motivo superveniente, tornar-se superior ao preço praticado no mercado o órgão gerenciador convocará o fornecedor visando a negociação para redução de preços e sua adequação ao praticado pelo mercado e, caso este não aceite a redução dos seus preços aos valores praticados pelo mercado será liberado dos compromissos assumidos, sem aplicação de penalidades administrativas, nos termo do art. 134, § 1º do Decreto Estadual n° 28.874/2024.

5.5. Se não houver prova efetiva da desatualização dos preços registrados e da existência de fato superveniente, o fornecedor continuará obrigado a cumprir os compromissos pelo valor registrado na ata, sob pena de cancelamento do registro de preços e de aplicação das penalidades administrativas previstas em lei e no edital, nos termos do art. 135, § 2º do Decreto Estadual n° 28.874/2024.

5.5.1. Na hipótese do cancelamento do registro de preços prevista no art. 135, § 2º do Decreto Estadual n° 28.874/2024, o órgão gerenciador poderá convocar os demais fornecedores integrantes do cadastro de reserva para que manifestem interesse em assumir o fornecimento dos bens, a execução das obras ou dos serviços, pelo preço registrado na ata.

5.6. Caso comprovada a desatualização dos preços registrados decorrente de fato superveniente que prejudique o cumprimento da ata, poderá ser efetuada a atualização do preço registrado, adequando-o aos valores praticados no mercado.

5.6.1. O órgão gerenciador, em alternativa à atualização prevista no item 5.6 desta Ata de Registro de Preços, poderá liberar o fornecedor do compromisso sem aplicação de penalidades, convocando, posteriormente, os licitantes remanescentes, na ordem de classificação, para negociação e assinatura da ata no máximo nas condições ofertadas por estes, desde que o valor seja igual ou inferior ao orçamento estimado para a contratação, inclusive quanto aos preços atualizados, nos termos do instrumento convocatório.

5.6.2. A redução do preço registrado será comunicada pelo órgão gerenciador aos órgãos que tiverem formalizado contratos com fundamento no respectivo registro, para que avaliem a necessidade de efetuar a revisão dos preços contratados.

5.7. O cancelamento do preço registrado, em conformidade com o artigo 136 do Decreto Estadual n° 28.874/2024, poderá ocorrer por fato superveniente decorrente de caso fortuito ou força maior que prejudique o cumprimento da ata, **devidamente comprovados e justificados**, por razão de interesse público ou a pedido do fornecedor.

5.7.1. O preço registrado, em atenção ao estabelecido pelo art. 136, inc. I a V do Decreto Estadual n° 28.874/2024, também poderá ser cancelado quando o fornecedor descumprir total ou parcialmente as condições previstas na Ata de Registro de Preços, não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, não aceitar reduzir o seu preço registrado na hipótese deste se tornar superior aqueles praticados no mercado ou sofrer sanção prevista na forma do Decreto Estadual n° 28.874/2024 em seu Capítulo VIII.

6. **CLÁUSULA VI - DA FORMAÇÃO DE CADASTRO RESERVA**

6.1. Em atenção ao art. 131 do Decreto Estadual n° 28.874/2024, o cadastro reserva será composto pelos demais licitantes que aceitaram cotar os bens, obras ou serviços com preços iguais aos do licitante vencedor, a ser incluído na respectiva ata na forma de anexo, respeitada a sequência da classificação do certame.

6.2. O cadastro reserva poderá ser utilizado nas hipóteses previstas no art. 131, § 1º do Decreto Estadual n° 28.874/2024.

6.3. A apresentação de novas propostas para compor o cadastro de reserva não prejudicará o resultado do certame em relação ao licitante melhor classificado.

6.4. Esta ordem de classificação dos licitantes registrados deverá ser respeitada nas contratações e somente será utilizada caso o melhor colocado no certame tenha seu registro cancelado ou revogado.

6.5. Para o registro do preço dos demais licitantes será exigida a análise da habilitação.

7. **CLÁUSULA VII - DAS SANÇÕES PELO DESCUMPRIMENTO DAS DIRETRIZES DA ATA DE REGISTRO DE PREÇOS**

7.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no edital e seus anexos. As sanções também se aplicam aos integrantes do cadastro de reserva no registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente.

7.2. Quando o fornecedor descumprir total ou parcialmente as condições previstas na Ata de Registro de Preços, não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, não aceitar reduzir o seu preço registrado na hipótese deste se tornar superior aqueles praticados no mercado ou sofrer sanção prevista na forma do Decreto Estadual n° 28.874/2024 em seu Capítulo VII, o preço registrado será cancelado, em conformidade com o artigo 136, inc. I a V do Decreto Estadual n° 28.874/2024.

8. **CLÁUSULA VIII - DAS CONDIÇÕES DE FORNECIMENTO**

8.1. As condições gerais referentes ao fornecimento, tais como prazo, local de entrega e recebimento do objeto, como também as relativas às penalidades e obrigações da Administração e do fornecedor detentor do registro, encontram-se definidas no Termo de Referência e Edital da licitação, partes integrantes da presente Ata.

8.2. É vedado o aditamento dos quantitativos consignados na Ata de Registro de Preços.

8.3. A detentora do registro fica obrigada a atender todas as ordens de fornecimento efetuadas pelo órgão participante, durante a vigência desta ata.

8.4. Em atenção ao art. 126 do Decreto Estadual n° 28.874/2024, faz-se necessário a permanente pesquisa de mercado, inclusive, antes da formalização da contratação, para aferição da manutenção da vantajosidade dos preços registrados.

8.5. A violação da integridade da conduta contratual, por meio do rompimento de deveres contratuais ou oriundos de outras normas aplicáveis ao caso, sujeita o contratado à aplicação das penalidades legalmente previstas nos arts. 184 ao 187 do Decreto Estadual n° 28.874/2024, bem como art. 156 da Lei n. 14.133, de 2021.

9. **CLÁUSULA IX - DO PAGAMENTO**

9.1. O pagamento, decorrente do objeto registrado nesta ata será efetuado conforme disposto no Edital e seus anexos.

10. **CLÁUSULA X – DAS DISPOSIÇÕES FINAIS**

10.1. A existência de preços registrados não obriga a Administração a firmar as contratações que deles poderão advir, facultada a realização de licitação específica para a aquisição pretendida, sendo assegurada à Detentora do registro de preços a preferência em igualdade de condições.

10.2. Fica a empresa detentora ciente que a publicidade da ata de registro de preços na imprensa oficial terá efeito de compromisso nas condições ofertadas e pactuadas na proposta apresentada à licitação.

10.3. A Ata de Registro de Preços, os ajustes dela decorrentes, suas alterações e rescisões obedecerão ao Decreto Estadual n°28.874 de 25 de janeiro de 2024, à Lei no 14.133, de 1o de abril de 2021 e às normas complementares e às disposições presentes nesta Ata e no Edital que a precedeu, aplicáveis à execução e, especialmente, aos casos omissos.

10.4. Fazem parte integrante desta Ata, para todos os efeitos legais: o Edital de Licitação e seus anexos, bem como, os ANEXOS desta ata que contém os preços registrados e seus respectivos detentores.

11. **CLÁUSULA XI - DO FORO**

11.1. Para dirimir eventuais conflitos oriundos desta Ata, é competente o Foro da Comarca de Porto Velho/RO, excluindo-se qualquer outro, por mais privilegiado que seja.

ANEXO ÚNICO

ITEM	ESPECIFICAÇÃO	CONSUMO ESTIMADO	UNID.	MARCA	PREÇO MERCADO	PREÇO REGISTRADO	DIF. %	DETENTORA

EMPRESA(S) DETENTORA(S):

CNPJ	RAZÃO SOCIAL	ENDEREÇO	CIDADE	REPRESENTANTE	CPF	TELEFONE

Geovanna Pinheiro Alves

Coordenadora do Sistema de Registro de Preços/SUPEL

Adriana Larissa da Silva Mendes Nascimento

Diretora Executiva/SUPEL

Alvaro Henrique de Lima Teixeira

Superintendente Estadual de Compras e Licitações

Elaborado por:

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

ATA

OFÍCIO DO ÓRGÃO OU ENTIDADE NÃO PARTICIPANTE DA ATA SOLICITANDO ADESÃO COMO INTERESSADO

[UNIDADE CONTRATANTE SOLICITANTE]

OFÍCIO Nº___/_____ [], [DATA DA EMISSÃO]

Prezado Gestor da Ata nº **[Nº DA ATA]** do(a) **[ÓRGÃO GESTOR DA ATA]**

Nos termos do art. 86, §2º, inciso I da Lei 14.133/21 , solicito autorização para ADERIR à Ata de Registro dePreços em epígrafe visando adquirir os itens e quantitativos relacionados na tabela abaixo.

Ressalto que o(s) fornecedor(es), detentor(es) do(s) preço(s) registrado(s), já se manifestou(ram) pela aceitação, conforme previsto na Lei 14.133/21.

Nº do item da Ata	Especificação	Quant. Adesão

ASSINATURA DO GESTOR DA UNIDADE SOLICITANTE

GOVERNO DO ESTADO DE RONDÔNIA
Superintendência Estadual de Compras e Licitações - SUPEL
Seção de Recursos Humanos - SUPEL-RH

Portaria nº 50 de 25 de fevereiro de 2026

Altera a Portaria n.º 185 de 14 de julho de 2025, que constituiu a 1ª Comissão de Tecnologia – COTEC e revoga a Portaria nº 25 de 26 de janeiro de 2026, no âmbito da Superintendência Estadual de Compras e Licitações – SUPEL/RO.

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

CONSIDERANDO a necessidade de garantir a eficiência e a continuidade das atividades relativas aos processos de aquisição de bens e serviços de tecnologia da informação e comunicação;

CONSIDERANDO a criação e reformulação periódica das Comissões Permanentes e Especiais, visando atender aos princípios da legalidade, eficiência e transparência na Administração Pública;

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

RESOLVE:

Art. 1º Alterar os incisos do Art. 1º da Portaria n.º 185 de 14 de julho de 2025, designando os servidores abaixo relacionados para a composição da Comissão de Tecnologia:

I - Agente de contratação:

a) Gabriel Alves da Silva Gama n.º: ******238.

II - Equipe de Apoio:

a) Ayanne Carmencita Ramos Dias n.º: ******964;

b) Jéssica Saraiva Guimarães n.º: ******606;

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

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

Art. 2º Revogar a Portaria nº 25 de 26 de janeiro de 2026.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

MÁRCIA ROCHA DE OLIVEIRA FRANCELINO

Superintendente de Compras e Licitações do Estado de Rondônia

sei! assinatura eletrônica	Documento assinado eletronicamente por **MARCIA ROCHA DE OLIVEIRA FRANCELINO**, **Superintendente**, em 05/03/2026, às 15:06, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.
	A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **69519740** e o código CRC **489967D3**.

Referência: Caso responda esta Portaria, indicar expressamente o Processo nº 0043.000009/2026-61 SEI nº 69519740

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

INSTRUMENTO CONVOCATÓRIO

PREGÃO ELETRÔNICO N.° 90236/2025/LEI N.° 14.133/2021

Para o **LOTE ÚNICO,** aplica-se a AMPLA PARTICIPAÇÃO **sem** a **reserva** de cota de até 25% para as **ME/EPP**

RESUMO DOS DADOS

ABERTURA DA SESSÃO PÚBLICA: 12/06/2026, às 11h (horário de Brasília), no sítio https://www.gov.br/compras/pt-br	Limite para esclarecimentos e impugnações ao edital: 09/06/2026.

OBJETO:
Registro de Preços para contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da Secretaria de Estado da Saúde - SESAU/RO, por um período de 3 (três) anos.
FUNDAMENTO:
Lei federal n.° 14.133, de 01 de Abril de 2021. Decreto estadual nº28.874, de 25 de Janeiro de 2024. dentre outros.
PROCESSO ADMINISTRATIVO: 0036.028242/2024-36
UASG: 925373 **ENDEREÇO ELETRÔNICO :** https://www.gov.br/compras/pt-br
VALOR ESTIMADO DA CONTRATAÇÃO

ORÇAMENTO ANUAL	**R$21.660.280,76 (vinte e um milhões seiscentos e sessenta mil duzentos e oitenta reais e setenta e seis centavos).**
VISTORIA	**INSTRUMENTO CONTRATUAL**

Facultativa	Ata de Registro de Preços	
DOCUMENTOS DE HABILITAÇÃO		
Requisitos Básicos: **1. Habilitação jurídica**: Conforme estabelecido no item 17.1 do Termo de Referência. **2. Qualificação econômico e financeira**: Conforme estabelecido no item 17.3. do Termo de Referência. **3. Regularidade fiscal, social e trabalhista**: Conforme estabelecido no item 17.2. do Termo de Referência. **4. Qualificação técnica:** Conforme estabelecido no item 17.6. 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**	**REGISTRO DE PREÇO**
Menor Valor Global	Aberto	Sim
TELEFONES PARA CONTATO		**E-MAIL PARA CONTATO:**
TELEFONE: (69) 3212-9243		**supelcotec@gmail.com**
OBSERVAÇÕES GERAIS:		
1. Maiores informações e esclarecimentos sobre o certame serão prestados nas dependências da Superintendência Estadual de 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. PREÂMBULO;
2. DA FORMALIZAÇÃO E AUTORIZAÇÃO;
3. DOS ÓRGÃOS E ENTIDADES PARTICIPANTES DO REGISTRO DE PREÇOS;
4. DO OBJETO;
5. DA QUANTIDADE MÍNIMA A SER COTADA;
6. DA POSSIBILIDADE DE PREVISÃO DE PREÇOS DIFERENTES;

7. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO;
8. DAS CONDIÇÕES DE PARTICIPAÇÃO;
9. DO BENEFÍCIO ÀS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE;
10. DO REGISTRO DA PROPOSTA NO SISTEMA ELETRÔNICO;
11. DA FORMULAÇÃO DE LANCES, CONVOCAÇÃO ME/EPP E CRITÉRIO DE DESEMPATE;
12. A FASE DE NEGOCIAÇÃO E JULGAMENTO DA PROPOSTA DE PREÇOS;
13. DA FASE DE HABILITAÇÃO;
14. DO RECURSO;
15. DA HOMOLOGAÇÃO;
16. DA REVOGAÇÃO E DA ANULAÇÃO;
17. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE;
18. DA RESCISÃO CONTRATUAL;
19. DO REAJUSTE E SUPRESSÃO CONTRATUAL;
20. DO PAGAMENTO;
21. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES;
22. DAS OBRIGAÇÕES DA CONTRATADA;
23. DAS OBRIGAÇÕES DA CONTRATANTE;
24. DA DOTAÇÃO ORÇAMENTÁRIA;
25. DO SISTEMA DE REGISTRO DE PREÇO;
26. CANCELAMENTO DO REGISTRO DO LICITANTE VENCEDOR E DOS PREÇOS REGISTRADOS;
27. DAS DISPOSIÇÕES GERAIS;
28. DOS ANEXOS;

1. DO PREÂMBULO

1.1. A SUPERINTENDÊNCIA ESTADUAL DE LICITAÇÕES , por meio da **Portaria nº 50/2026/GAB/SUPEL**, publicada no DOE na data 25 fevereiro de 2026, torna público que se encontra autorizada a realização da licitação na modalidade de **PREGÃO,** na forma **ELETRÔNICA, sob o nº 90236/2025/SUPEL/RO**, do tipo **ABERTO,** com o **Método de Disputa: MENOR VALOR GLOBAL** , em conformidade com a Lei Federal nº. 14.133, de 2021, Decreto Estadual nº 28.874/2024, a Lei Complementar nº 123/06, e o Decreto Estadual 21.675/2017 e suas alterações, e demais legislações vigentes, tendo como interessado Secretaria de Estado da Saúde de Rondônia – SESAU/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. DA FORMALIZAÇÃO E AUTORIZAÇÃO

2.1. Esta Licitação encontra-se formalizada e autorizada por meio do **Processo Administrativo n° 0036.028242/2024-36**, e destina-se a garantir a observância do princípio constitucional da isonomia e a selecionar a proposta mais vantajosa para a Administração Pública e será processada e julgada em estrita conformidade com os princípios básicos da legalidade, da impessoalidade, da moralidade, da igualdade, da publicidade, da probidade administrativa, da vinculação ao instrumento convocatório, do julgamento objetivo de que lhe são correlatos.

2.2. O processo acima mencionado poderá ser consultado por meio do Sistema Eletrônico de Informações-SEI (https://www.sei.ro.gov.br/sobre).

3. DOS ÓRGÃOS E ENTIDADES PARTICIPANTES DO REGISTRO DE PREÇOS

3.1. São participantes deste Sistema de Registro de Preços os seguintes órgãos e/ou entidades:

Unidade Orçamentária: Secretaria de Estado da Saúde de Rondônia – SESAU/RO.

Requisitante: SESAU-CTI - Coordenadoria de Tecnologia da Informação.

4. DO OBJETO

4.1. O objeto da presente licitação é a contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, por meio do **Sistema de Registro de Preços**, conforme condições, quantidades e exigências estabelecidas no Termo de Referência - Anexo I.

4.2. 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.

4.3. Das especificações técnicas/quantidades do objeto: Ficam aquelas estabelecidas no item 8.10. e 3.2. e seus subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente, conforme transcrevemos:

(...)

3.2 Descrição Detalhada do Objeto

GRUPO ÚNICO	ITEM	CATMAT	OBJETO	UNIDADE DE MEDIDA	QUANTIDADE
01	1	27499	Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes	Por Endpoint	2150
	2	27499	Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes	Por Servidor	139
	3	27499	Solução de segurança avançada para mitigação de ameaças na rede	Por Throughput de dados	2
	4	27499	Solução de prevenção de intrusão de próxima geração (NGIPS)	Por Throughput de dados	4
	5	27432	Serviço de suporte pro ativo, corretivo e para resposta a incidentes	Por Solução	4
	6	3840	Serviço de implantação	Por Solução	4
	7	3840	Serviço de capacitação e repasse de conhecimento	40 Horas	2

3.2.1. OBS.: A descrição completa dos objetos está presente no item**8** deste Termo de Referência.

3.3 Da Memória de Cálculo

3.3.1. Conforme relatório Relatório Parque Computacional SESAU (0049992349), extraído do

sistema GLPI até 20/06/2024 a Secretaria de Estado da Saúde, tem 1920 computadores, considerando que estão com processos para adição e substituição do computadores deixando uma margem de crescimento do parque solicitamos 2150 unidades para os desktops levando em consideração que cada computador deve ter uma licença ativa e válida.

3.3.2. Considerando que estamos com dois processos de aquisição de novos computadores para renovação do parque tecnológico 0036.006222/2024-12 - 38 Computadores e 0036.051061/2023-22- 1.470 Computadores.

3.3.3. Considerando a instalação do antivírus apenas nos equipamentos novos, para evitar maior lentidão nos computadores antigos, chegamos ao seguinte cálculo:

- 400 Computadores compatíveis atualmente
- 1.508 Processos em andamento

3.3.4. Totalizando 1.908 licenças necessárias para uso imediato, com uma reserva adicional de 242 licenças para futuras expansões.

Item	Quantidade
Computadores no Parque(atual)	1920
Licenças (item 1)	2150
0036.006222/2024-12 – Aquisição	38
0036.051061/2023-22 - Aquisição	1470

- Atualmente dispomos de 47 servidores que rodam as seguintes aplicações:

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)

Sistema	Unidade demandante	Função	Amplitude de atuação
GERADOR SENHA	POC-CGAF-BARCO	Gerar senhas para Gerenciar a Fila de Atendimento de Pacientes	POC - Policlinica Osvaldo Cruz CGAF - Gerência Farmaceutica
PAINEL CHAMADOR	POC-CGAF-BARCO	Realizar a Chamada da Senha no Painel em Voz, chamando o nome Social do Paciente, juntamente com o número da Senha e Consultório Médico.	POC - Policlinica Osvaldo Cruz CGAF - Gerência Farmaceutica
SAÚDE POC	POC	Realizar a Gestão de Atendimento Administrativo, Atendimento Médico, Prontuário Eletrônico, Configurações de Painéis de Chamada, Configurações de Áreas de Atendimento.	POC - Policlinica Osvaldo Cruz

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)			
EPEP POC	POC	Sistema para Estatísticas de Atendimentos da POC, Retirar Relatórios Estratégicos de Atendimento, assim como Dashboard em Tempo Real do Cenário da POC	POC - Policlinica Osvaldo Cruz
ADMINISTRATIVO CGAF	CGAF	Realizar a Gestão de Agendamentos de Pacientes para retirar Medicamentos na Farmácia	CGAF - Gerência Farmaceutica
E-CONSUMO	CAP	Realizar a Gestão de Estoque de Materiais de Consumo	CAP - Coordenadoria de Almoxarifado e Patrimonio HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De Buritis JP II - Hospital e Pronto Socorro João Paulo II Cemetron - Centro de Medicina Tropical de Rondônia HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião AMI - Assistencia Médica Intensiva HCAMP - Hospital de Campanha de Rondônia HRE - Hospital Regional de Extrema HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De São Francisco do Guaporé Hospital Regional De Buritis
E-CONSUMO GASES	Unidades Hospitalares	Realizar a Gestão de Estoque e Solicitação de Medicinais das Unidades Hospitalares	CAP - Coordenadoria de Almoxarifado e Patrimonio HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De Buritis JP II - Hospital e Pronto Socorro João Paulo II Cemetron - Centro de Medicina Tropical de Rondônia HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião Ami - Assistencia Médica Intensiva HCAMP - Hospital de Campanha de Rondônia HRE - Hospital Regional de Extrema HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De São Francisco do Guaporé Hospital Regional De Buritis
HOSPUB	Unidades Hospitalares	Realizar a Gestão de Prontuário Eletrônico	HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião JP II - Hospital e Pronto Socorro João Paulo II Cemetron - Centro de Medicina Tropical de Rondônia Ami - Assistencia Médica Intensiva HCAMP - Hospital de Campanha de Rondônia HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De São Francisco do Guaporé Hospital Regional de Buritis CAFI NMJ - Nucleo de Mandados Judiciais CDA - Centro de Diálise de Ariquemes POC - Policlinica Osvaldo Cruz

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)			
E-LEITOS	Regulação	Painel Dashboard da Taxa de Ocupação dos Leitos de Acordo com as Informações do Hospub, assim como Realizar Pareceres para Solicitação de Leitos para as Unidades.	Todos os leitos da SESAU
E-REFEIÇÃO	Unidades Hospitalares	Realizar a Gestão e controle das Refeições nas Unidades Hospitalares dos servidores que estão de Plantão.	Cemetron - Centro de Medicina Tropical de Rondônia HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião JP II - Hospital e Pronto Socorro João Paulo II HRC - Hospital Regional de Cacoal HEURO - Hospital de Urgência e Emergência Regional de Cacoal Cemetron - Centro de Medicina Tropical de Rondônia Hospital Regional de Buritis
NACSUS	NAC-NMJ	Auxiliar e ajudar os processos internos do NAC - Núcleo de Apoio e Conciliação, evitando que os pacientes entrem com uma Ação Judicial contra o Estado de Rondônia.	Núcleo de Apoio a Conciliação
PROCESSO SELETIVO	RH	Realizar o Cadastro dos Candidatos as vagas em Aberto no Processo Seletivo da SESAU, assim como, definir os critérios de Pontuação e deferir ou indeferir algum certificado ou experiência profissional.	RH

3.3.5. Considerando o contrato com a fábrica de software e a implantação do sistema AGHuX em todo o estado, é necessário ressaltar que cada unidade de saúde requer três servidores para o pleno funcionamento do AGHuX. Além disso, após a implantação, o sistema HOSPUB precisará permanecer hospedado por aproximadamente três anos para fins de consulta.

3.3.4. Servidores Atual: 47

3.3.7. AGHuX: 60

3.3.8. Margem de 30% Novos Sistemas: 32

3.3.9. Total: 139 Licenças ITEM (2)

AGHuX	
ID	**Unidade de Saúde**
1	Hospital Infantil Cosme Damião:
2	Pronto Socorro João Paulo II:
3	Policlínica Oswaldo Cruz:
4	Hospital De Base Dr. Ary Pinheiro:

AGHuX	
5	Laboratório Central de Saúde Pública de Rondônia – LACEN:
6	Laboratório Estadual de Patologia e Análises Clínicas de Rondônia – LEPAC:
7	Centro de Atenção Psicossocial – CAPS:
8	Assistência Médica Intensiva – AMI:
9	Serviço de Assistência Multidisciplinar em Domicílio – SAMD:
10	Centro de Medicina Tropical De Rondônia – CEMETRON:
11	Hospital Regional de Extrema:
12	Hospital Regional de São Francisco do Guaporé:
13	Hospital de Urgência e Emergência de Cacoal – HEURO:
14	Hospital Regional de Cacoal:
15	Centro de Diálise de Ariquemes
16	Hospital Regional de Buritis:
17	Hospital de Retaguarda
18	NMJ - Nucleo de Mandados Judiciais
19	CAF1
20	CAF2

3.4. Da Classificação do Objeto

3.4.1. O objeto pleiteado nos autos não envolve técnicas desconhecidas no mercado ou requerem inovação tecnológica para a sua execução, tratando-se assim de bem comum, pois é possível estabelecer, por intermédio de especificações utilizadas no mercado, padrões de qualidade e desempenho característicos ao objeto, de modo que é possível a decisão entre os materiais ofertados pelos participantes com base no menor preço.

3.4.2. A classificação como comum não se confunde com a complexidade do objeto. O que deve ser verificada é a possibilidade de seus padrões de desempenho e qualidade serem definidos objetivamente em especificações usualmente adotadas no mercado, o que fica evidente no presente instrumento convocatório.

3.4.3. Corroborando com esse entendimento, transcrevemos o relatado pelo Professor Marçal Justen Filho em seu livro Pregão - Comentários à Legislação do Pregão Comum e Eletrônico:

"Ou seja, há casos em que a Administração necessita de bens que estão disponíveis no mercado, configurados em termos mais ou menos variáveis. São hipóteses em que é público o domínio das técnicas para a produção do objeto e seu fornecimento ao adquirente (inclusive à Administração), de tal modo que não existe dificuldade em localizar um universo de fornecedores em condições de satisfazer plenamente o interesse público. Em outros casos, o objeto deverá ser produzido sob encomenda ou adequado às configurações de um caso concreto.
(...)

3.4.4. Entende-se que a contratação enquadra-se em aquisição de bens comuns,consideram-se bens e serviços comuns, aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos, por meio de especificações usuais no mercado e conforme expressa no Parecer n° 20/CONSU/CMA/PRF3/PGF/AGU nº 432/2014:

"Bens e serviços comuns são produtos cuja a escolha pode ser feita tão somente com base nos preços ofertados, haja vista serem comparáveis entre si e não necessitarem de avaliação minuciosa. São encontráveis facilmente no mercado. São exemplos de bens comuns: caneta, lápis, borrachas, papéis, mesa, cadeiras, veículos, aparelho de ar refrigerado, etc e de execução de serviços: confecção de chaves, manutenção de veículos, colocação de piso, troca de azulejos, pintura de parede, etc. O bem ou serviço será comum quando for possível estabelecer para efeito de julgamento das propostas, mediante especificações utilizadas no mercado, padrões de qualidade e desempenho peculiares ao objeto".

3.4.5. Para concluir, numa tentativa de definição, poderia dizer-se que bem ou serviço comum é aquele que apresenta sob identidade e características padronizadas e que se encontra disponível, a qualquer tempo, num mercado próprio.

3.4.6. Diante do exposto, e considerando que a Lei n° 14.133/21 define em seu Art. 6º Inciso XIII - "bens e serviços comuns: aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado", define-se que o objeto da presente contratação é comum.

8.10 . ESPECIFICAÇÕES TÉCNICAS

8.10.1. SOLUÇÃO DE PROTEÇÃO DE ENDPOINTS COM ABORDAGEM PROATIVA PARA RESPOSTA EFICAZ A INCIDENTES (ITEM 1)

8.10.1.1. Características gerais:

8.10.1.1.1. A solução deverá ser entregue na modalidade como um serviço (em nuvem);

8.10.1.1.2. Possuir console Web para gerenciamento e administração da ferramenta;

8.10.1.1.3. A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações e Controle de dispositivos em um único agente.

8.10.1.1.4. Módulo de Proteção Anti-Malware.

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

8.10.1.1..5.1. Windows 8.1 (x86/x64); Windows 10 (x86/x64); Windows 11 (x64).

8.10.1.1.6. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

8.10.1.1.7. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

8.10.1.1.8. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em: Processos em execução em memória principal (RAM);

8.10.1.1.9. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

8.10.1.1.10. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, MIME/uu, CAB;

8.10.1.1.11. Arquivos recebidos por meio de programas de comunicação instantânea (MSN messenger, yahoo messenger, google talk, icq, dentre outros).

8.10.1.1.12. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript, VBScript/Activex; Deve possuir detecção heurística de vírus desconhecidos;

8.10.1.1.13. Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada;

8.10.1.1.14. Deve permitir diferentes configurações de detecção (varredura ou rastreamento): Em tempo real de arquivos acessados pelo usuário;

8.10.1.1.15. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

8.10.1.1.16. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

8.10.1.1.17. Automáticos do sistema com as seguintes opções: Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

8.10.1.1.18. Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

8.10.1.1.19. Frequência: horária, diária, semanal e mensal;

8.10.1.1.20. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados.

8.10.1.1.21. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

8.10.1.1.22. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

8.10.1.1.23. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

8.10.1.1.24. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL’s maliciosas, de modo a prover, rápida detecção de novas ameaças;

8.10.1.1.25. Deve ser capaz de aferir a reputação das URL’s acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;

8.10.1.1.26. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;

8.10.1.1.27. Deve possuir capacidade de escaneamento de arquivos compactados e, em caso de identificação de um arquivo malicioso, apenas este deve ser removido, mantendo os demais intactos Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

8.10.1.1.28. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

8.10.1.1.29. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

8.10.1.1.30. Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;

8.10.1.1.31. Deverá ter funcionalidade de Machine Learning em runtime para evitar possíveis métodos de obfuscação que o módulo de Machine Learning em pré-execução não consiga detectar;

8.10.1.1.32. Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;

8.10.1.1.33. Deve bloquear processos comuns associados a ransomware;

8.10.1.1.34. Em casos de ataques de ransomware, a solução deve ter a capacidade de interromper o processo de criptografia e restaurar os arquivos originais aos seus respectivos diretórios;

8.10.1.1.35. Deve possuir funcionalidade de detecção de malwares conhecidos e desconhecidos por comportamento;

8.10.1.1.36. Deve permitir a integração com solução de análise de artefatos suspeitos (sandbox) do próprio fabricante. Funcionalidade de Atualização Deve permitir a programação de atualizações automáticas das listas de definições de vírus, a 8.10.1.1.37. partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

8.10.1.1.37. Deve permitir atualização incremental da lista de definições de vírus;

8.10.1.1.38.Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

8.10.1.1.39. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

8.10.1.1.40. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

8.10.1.1.41. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

8.10.1.1.42. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

8.10.1.1.43. Funcionalidade de Administração Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

8.10.1.1.44. Deve possibilitar instalação "silenciosa";

8.10.1.1.45. Deve permitir o bloqueio por nome de arquivo;

8.10.1.1.46. Deve permitir o travamento de pastas e diretórios;

8.10.1.1.47. Deve permitir o travamento de compartilhamentos;

8.10.1.1.48. Deve permitir o rastreamento e bloqueio de infecções;

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

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

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

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

8.10.1.1.53. Deve permitir a deleção dos arquivos quarentenados;

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

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

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

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

8.10.1.1.58. Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante; Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

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

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

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

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

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

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

8.10.1.1.65. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de antimalware;

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

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

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

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

8.10.1.1.70. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto. Funcionalidade de Controle de Dispositivos As configurações da funcionalidade de controle de dispositivos devem ser aplicadas por usuário;

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

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

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

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

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

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

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

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

cliente para instalação deverá possuir compatibilidade com os sistemas operacionais: macOS 12 (Monterey); macOS 11 (Big Sur) macOS 10.15 (Catalina); macOS 10.14 (Mojave); macOS 10.13 (High Sierra);

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

8.10.1.1.80. Gerenciamento integrado à console de gerência central da solução; Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;

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

8.10.1.1.82. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;

8.10.1.1.83. Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infeções a arquivos;

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

8.10.1.1.85. Deve possuir no mecanismo de autoproteção as seguintes proteções: Proteção e verificação dos arquivos de assinatura;

8.10.1.1.86. Proteção dos processos do agente de segurança; Proteção das chaves de registro do agente de segurança;

8.10.1.1.87. Proteção do diretório de instalação do agente de segurança. Funcionalidade de HIPS – Host IPS e Host Firewall Deve ser capaz de realizar a detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais: Windows 8.1 (x86/x64);

8.10.1.1.88. Windows 10 (x86/x64); Windows 11 (x64). Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;

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

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

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

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

8.10.1.1.93. Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo; O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança;

8.10.1.1.94. O modulo de HIPS deverá possuir regras pra proteger contra ameaças do tipo Ransomware;

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

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

8.10.1.1.97. Deve suportar configuração de parâmetros de pacotes como quantidade máxima de conexões TCP e timeout para pacotes UDP; Deve ter a capacidade de proteção contra exploração de vulnerabilidades do sistema operacional e de aplicações terceiras instaladas na estação de trabalho;

8.10.1.1.98. A lista de regras deve permitir que o administrador realize buscas e tenha rápida visibilidade do tipo da aplicação, em que modo a regra encontra-se (bloqueio ou monitoramento), CVE, CVSS score, quando aplicável. Módulo para Controle De Aplicações Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais: Windows 8.1 (x86/x64); Windows 10 (x64); Windows 11 (x64). As regras de controle de aplicação devem permitir as seguintes ações: Permissão de execução; Bloqueio de execução;

8.10.1.1.99. Bloqueio de novas instalações. A regra de liberação para o controle de aplicação deverá permitir que o programa liberado efetue ou não a execução de outros processos, As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra; As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações: Assinatura SHA-1 e SHA-256 do executável;

8.10.1.1.100. Atributos do certificado utilizado para assinatura digital do executável;

8.10.1.1.101. Caminho lógico do executável;

8.10.1.1.102. Base de assinaturas de cortiçados digitais válidos e seguros. As regras de controle de

aplicação devem possuir categorias pré-determinadas de aplicações;

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

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

8.10.1.1.105. Deve permitir a busca por aplicações ou fabricante destas; Deve possuir ferramenta para extrair o hash de um ou um grupo de executáveis, permitindo a importação destes hashes através de arquivo CSV. Módulo de Detecção e Resposta A solução deve ser compatível com os sistemas operacionais Windows, Linux e MacOS; O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK®, identificando técnicas e táticas dos ataques;

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

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

8.10.1.1.108.Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho; Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

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

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

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

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

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

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

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

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

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

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

8.10.1.1.119. O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

8.10.1.1.120. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

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

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

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

8.10.1.1.124. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento; Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade; Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

8.10.1.1.125. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console; Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta; Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;

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

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

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

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

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

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

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

8.10.1.1.133. Deve permitir adicionar arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

8.10.1.1.134. Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

8.10.1.1.135. Deve permitir terminar processos ativos executados nas estações de trabalhos e servidores;

8.10.1.1.136. Permitir coletar e fazer o download de um arquivo para investigação local detalhada; Isolar a estação de trabalho desconectando-a da rede e permitindo se comunicar exclusivamente com a console de gerenciamento do fabricante;

8.10.1.1.137. Restaurar a conectividade da estação de trabalho com a rede;

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

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

8.10.2. SOLUÇÃO DE PROTEÇÃO DE SERVIDORES COM ABORDAGEM PROATIVA PARA RESPOSTA EFICAZ A INCIDENTES (ITEM 2) : SOLUÇÃO DE SEGURANÇA PARA CARGAS DE TRABALHO HÍBRIDAS COM DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO

8.10.2.1. Características Gerais Da Solução

8.10.2.1.1. A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais: Windows Server 2000; Windows Server 2003 SP1 e 2003 R2 SP2; Windows Server 2008 e 2008 R2; Windows Server 2012 e 2012 R2; Windows Server 2016; Windows Server 2019;

8.10.2.1.2. Windows Server 2022; Red Hat Enterprise 5, 6, 7 e 8; CentOS 5, 6, 7 e 8; AIX 6.1, 7.1 e 7.2;

8.10.2.1.3. Oracle Linux 5, 6, 7 e 8;

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

8.10.2.1.5. Ubuntu 10, 12, 14, 16, 18 e 20;

8.10.2.1.6. Debian 6, 7, 8, 9 e 10;

8.10.2.1.7. Rocky Linux 8; AlmaLinux 8;

8.10.2.1.8. Cloud Linux 5, 6, 7 e 8;

8.10.2.1.9.Solaris 10 1/13 Sparc;

8.10.2.1.10.Solaris 10 1/13 (x86/x64);

8.10.2.1.11.Solaris 11.2/ 11.3 Sparc;

8.10.2.1.12. Solaris 11.2/ 11.3 (x86/x64);

8.10.2.1.13. Solaris 11.4 (x86, x64 ou SPARC) Amazon Linux e Amazon Linux 2 (x64). A solução deverá ser totalmente compatível e homologada com o ambiente Vmware;

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

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

gerenciamento;

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

8.10.2.1.17. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;

8.10.2.1.18. A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;

8.10.2.1.19. A console de administração deverá permitir o envio de notificações via SMTP; Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;

8.10.2.1.20. A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas; A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;

8.10.2.1.21. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;

8.10.2.1.22. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob- demanda, ou agendado com o envio automático do relatório via e-mail;

8.10.2.1.23. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;

8.10.2.1.24. A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;

8.10.2.1.25. A solução deverá prover relatórios contendo no mínimo as seguintes informações;

8.10.2.1.26. malware, regras de IPS aplicadas e Firewall;

8.10.2.1.27. Em caso de solução e nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade;

8.10.2.1.28. A solução de segurança ter a capacidade de identificar ataques entre conteineres;

8.10.2.1.29. Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";

8.10.2.1.30. Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar novas políticas de segurança;

8.10.2.1.31. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;

8.10.2.1.32. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;

8.10.2.1.33. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;

8.10.2.1.34. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;

8.10.2.1.35. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;

8.10.2.1.36.Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;

8.10.2.1.37. Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;

8.10.2.1.38. Para servidores Linux, a solução deverá possibilitar a atualização automática da versão quando o agente reiniciar;

8.10.2.1.39. Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;

8.10.2.1.40. Deve permitir a remoção automática de agentes inativos, definindo o período para, pelo menos 1 semana, 1 mês e 12 meses;

8.10.2.1.41. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;

8.10.2.1.42. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;

8.10.2.1.43. A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação;

8.10.2.1.44. A solução deverá mostrar quais máquinas estão usando determinada política;

8.10.2.1.45. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;

8.10.2.1.46. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;

8.10.2.1.47. A solução deverá permitir a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;

8.10.2.1.48. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;

8.10.2.1.49. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;

8.10.2.1.50. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;

8.10.2.1.51. A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;

8.10.2.1.52. A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;

8.10.2.1.53. A solução deverá ter a capacidade de se integrar com o Amazon SNS e os principais softwares de SIEMs contemplando, no mínimo: Splunk, IBMQradar e HPArcSight de modo a permitir enviar os seus logs para essas soluções;

8.10.2.1.54. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;

8.10.2.1.55. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;

8.10.2.1.56. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;

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

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

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

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

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

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

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

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

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

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

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

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

8.10.2.1.69. O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há,

pelo menos, 5 anos;

8.10.2.1.70. A solução deve possuir API documentada para integração na esteira de automação;

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

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

8.10.2.1.73. A solução deve permitir desabilitar os módulos individualmente;

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

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

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

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

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

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

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

8.10.2.1.81. A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas; A solução deverá oferecer escanear processos em memória em busca de Malware;

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

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

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

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

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

8.10.2.1.87. A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado;

88.10.2.1.88. Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware;

8.10.2.1.89. Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;

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

8.10.2.1.91. A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs;

8.10.2.1.92. Em servidores Windows, deve possuir capacidade de detectar ameaças por comportamento;

8.10.2.1.93. Deverá ter a possibilidade de escanear drivers de rede mapeados nos servidores. Proteção Contra URLs Maliciosas Deve permitir a proteção contra acesso a websites ou URLs consideradas maliciosas ou de baixa reputação;

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

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

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

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

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

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

8.10.2.1.100. A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança. Firewall Operar como firewall de host, através da instalação de agente nos servidores protegidos;

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

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

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

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

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

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

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

8.10.2.1.108. Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

8.10.2.1.109. O firewall deverá ser stateful bidirecional; O firewall deverá permitir liberar ou apenas logar eventos;

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

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

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

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

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

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

8.10.2.1.116. Deverá permitir limitar o número de meias conexões vindas de um computador;

8.10.2.1.117. Deverá prevenir ack storm; Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;

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

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

18.10.2.1.120. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas. Proteção De Vulnerabilidades de SO e Aplicações Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

18.10.2.1.121. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;

8.10.2.1.122. A solução deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;

8.10.2.1.123. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;

128.10.2.1.124.Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;

8.10.2.1.125. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

8.10.2.1.126. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;

8.10.2.1.127. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;

8.10.2.1.128. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting.

8.10.2.1.129. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;

8.10.2.1.130. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;

8.10.2.1.131. Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;

8.10.2.1.132. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);

8.10.2.1.133. Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

8.10.2.1.134. Deverá ser capaz de inspecionar tráfego criptografado de entrada;

8.10.2.1.135. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;

8.10.2.1.136. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

8.10.2.1.137. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;

8.10.2.1.138. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;

8.10.2.1.139. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;

8.10.2.1.140. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;

8.10.2.1.141. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;

8.10.2.1.142. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;

8.10.2.1.143. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs; As regras de IPS poderão ter sua capacidade de LOG desabilitado;

8.10.2.1.144. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta; As regras devem ser atualizadas automaticamente pelo fabricante;

8.10.2.1.145. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas. Monitoramento De Integridade A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;

8.10.2.1.146. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;

8.10.2.1.147. Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux;

8.10.2.1.148. Precisa ter a capacidade de monitorar o status de serviços e processos do sistema

operacional;

8.10.2.1.149. Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;

8.10.2.1.150. Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;

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

8.10.2.1.152. O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;

8.10.2.1.153. Deverá alertar toda vez que uma modificação ocorrer em tempo real para ambiente Windows e pseudo real-time para ambiente Linux;

8.10.2.1.154. Deverá logar e colocar em relatório todas as modificações que ocorram;

8.10.2.1.155. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;

8.10.2.1.156. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

8.10.2.1.157. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;

8.10.2.1.158. Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente. Inspeção De Logs A solução deverá permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX; Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;

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

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

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

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

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

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

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

8.10.2.1.166. Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram;

8.10.2.1.167. As regras poderão ser modificadas por severidade de ocorrência de eventos;

8.10.2.1.168. As regras devem se atualizar automaticamente pelo fabricante; Permitir modificação pelo administrador em regras para adequação ao ambiente. Controle De Aplicações A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;

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

8.10.2.1.170. O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina;

8.10.2.1.171. A console deverá exibir eventos de no mínimo 30 dias;

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

8.10.2.1.173. A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente. Detecção e Resposta A solução deve ser compatível com Linux e Windows Server 2008 R2 e superiores;

8.10.2.1.174. A solução deve possuir módulo de investigação, detecção integrados; Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio

fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

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

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

8.10.2.1.177. O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

8.10.2.1.178. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

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

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

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

8.10.2.1.182. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações; Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

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

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

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

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

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

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

8.10.3. SOLUÇÃO DE SEGURANÇA AVANÇADA PARA MITIGAÇÃO DE AMEAÇAS NA REDE (ITEM 3): SOLUÇÃO DE SEGURANÇA CONTRA AMEAÇAS AVANÇADAS COM DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 12 (DOZE) MESES.

8.10.1. Características Gerais

8.10.3.1.1.A solução deverá ser instalada de modo a detectar ameaças avançadas no ambiente da CONTRATANTE, inspecionando o tráfego de rede, independente de agentes instalados;

8.10.3.1.2.Deve ser dimensionada para inspecionar 04Gbps de throughput; A solução deve permitir que o administrador escolha uma implementação em modo inline ou em modo de monitoramento através de tráfego espelhado;

8.10.3.1.3. Caso seja implementada no modo inline, a solução deverá permitir criar um by-pass para casos de falhas de interface;

8.10.3.1.4. Quando inline, a solução deverá ter a capacidade de analisar tráfego TLS; Funcionalidades e Requisitos específicos: Deverá fornecer solução integrada de proteção contra ameaças avançadas de acordo com funcionalidades e características técnicas especificadas neste documento, contendo, no mínimo os seguintes módulos: Monitoramento, Identificação, Análise e Resposta de Incidentes de Segurança;

8.10.3.1.5. Detecção de ataques direcionados; Analisador virtual de ameaças;

8.10.3.1.6. Correlação de regras para detecção de conteúdo malicioso;

8.10.3.1.7. Análise de todos os estágios de uma sequência de ataques. Esta solução deverá ser atendida através do fornecimento de solução de um único Fabricante, contendo: Serviço de Monitoração e Análise de Ameaças Digitais em rede;

8.10.3.1.8. Serviço de Monitoração e gestão de riscos que permita a identificação de ameaças digitais conhecidas e não conhecidas por soluções de antivírus tradicionais, permitindo a composição de serviços de mitigação complementares para a segurança do ambiente;

8.10.3.1.9. Serviço que entenda ameaça digital como a representação de um software malicioso ou ação maliciosa tal como: spyware, phishing, worms, bot, trojan, adware, network Exploit, web

Exploit, Cross-site scripting, spear phishing, information stealing malware e outras ações que podem compor ataques ao patrimônio computacional do ambiente;

8.10.3.1.10. Visibilidade e relatório de incidentes de conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos;

8.10.3.1.11. Análise e correlação de atividades maliciosas tais como: Detecção específica de malwares conhecidos e arquivos contaminados através de assinaturas de antivírus tradicional no tráfego da rede;

8.10.3.1.12. Detecção de vermes de rede e de e-mail no tráfego de rede; Detecção de programas de exploração de vulnerabilidades (Exploits) na rede; Detecção de empacotamentos maliciosos no tráfego da rede;

8.10.3.1.13. Validação de tráfego web malicioso através de consultas a sistemas de reputação na Internet;

8.10.3.1.14. Visibilidade e relatório de estatísticas de ameaças, fontes de infecção na rede monitorada e máquinas comprometidas. Permitir a rápida identificação da criticidade dos eventos de segurança Permitir realizar pesquisas avançadas e customizadas dos incidentes de segurança através da console de gerenciamento;

8.10.3.1.15. Possibilidade de criação de filtros para visualização de eventos específicos conforme contexto, localização e outras variáveis que permitam investigação profunda sobre causa raiz de incidentes de segurança;

8.10.3.1.16. Permitir a customização de alertas em base ao tipo de incidente de segurança através da console de gerenciamento;

8.10.3.1.17. Permitir a integração com sistemas de serviço de diretório;

8.10.3.1.18. Capacidade de verificar em tempo real a reputação de endereços web (URL's) e servidores de correio SMTP;

8.10.3.1.19. A análise de SMTP poderá ser realizada em uma solução separada do sensor de HTTP e demais protocolos;

8.10.3.1.20. A capacidade de análise de artefatos em sandbox pode ser realizada através de no mesmo equipamento de análise; A solução deverá possuir mecanismo de conhecimento de senhas de pelo menos 90 palavras chaves em seu vocabulário de conhecimento, para derivação de arquivos protegidos;

8.10.3.1.21. Capacidade de criar e salvar investigações customizadas dos incidentes de segurança; Deve possuir pelo menos 1 sensor para inspecionar o tráfego de rede de throughput de 04Gbps de análise; Deve possuir a capacidade de detectar ameaças direcionadas, ataques do dia zero e documentos que viabilizem ataques;

8.10.3.1.22. Deve detectar atividades maliciosas que trafegam na rede através de motor de análise de comportamento de tráfego até o nível 7 (camada de aplicação) em protocolo TCP/IP;

8.10.3.1.23. Capacidade de detectar ameaças web tais como vulnerabilidades e download de conteúdo malicioso; Os módulos de captura de rede deverão suportar a coleta de arquivos pelo menos nos protocolos HTTP e HTTPS;

8.10.3.1.24. Deve possuir a habilidade de detectar e analisar os seguintes protocolos e aplicativos: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT-UDP, RTSP/RDTTCP, WMSP, SHOUTCast, RTMP, Bittorent, Kazaa, Blubster, eDonkeyeMule, Gnucleus LAN, Gnutella/Limewire/Bearshare/Shareaza, Winny, WinMX, MLDonkey, DirectConnect, SoulSeek, OpenNap, Kuro, iMesh, Skype, Google Talk, Zultrax, Foxy, eDonkey, Ares, Miranda, Kceasy, MoodAmp, Deepnet Explorer, FreeWire, Gimme, GnucDNA GWebCache, Jubster, MyNapster, Nova GWebCache, Swapper GWebCache, Xnap, Xolox, Ppstream, AIM Express, Chikka SMS Messenger, eBuddy, ICQ2Go, ILoveIM Web Messenger, IMUnitive, mabber, meebo, Yahoo Web Messenger, GPass, IP, ARP, TCP, UDP e IGMP;

8.10.3.1.25. Deve possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;

8.10.3.1.26. Capacidade de oferecer informações para análise forense de artefatos suspeitos de serem maliciosos; Gerenciamento centralizado de todas as etapas dos eventos de segurança identificados como possíveis ameaças;

8.10.3.1.27. Capacidade de identificar artefatos maliciosos direcionados para dispositivos moveis rodando o sistema operacional Android, tais como telefones inteligentes e tablets;

8.10.3.1.28. Deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos PDF´s, executáveis, PPT, DOC, XLS,

ZIP e RAR;

8.10.3.1.29. A solução deve detectar ameaças do dia zero, vulnerabilidade, URL's maliciosas e spams dirigidos no protocolo SMTP;

8.10.3.1.30. Deve possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho;

8.10.3.1.31. Deve permitir o uso de base de conhecimento na Internet do próprio fabricante para correlacionamento de informações sobre ameaças conhecidas e prover recomendações de ações;

8.10.3.1.32. Deve permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança;

8.10.3.1.33. Deverá permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo (True File Type), múltiplas camadas de empacotamento (Multi-packed/Multi-layered files) e arquivos comprimidos (compactados);

8.10.3.1.34. Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística;

8.10.3.1.35. Deve possuir foco em proteção contra APTs (Advanced Persistent Threats);

8.10.3.1.36. Deve possuir tecnologia de proteção contra ameaças desconhecidas (ataques dirigidos e ameaças de dia zero), sendo que este módulo deve pertencer ao mesmo fabricante;

38.10.3.1.37. Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLANs ou witches;

8.10.3.1.38. Deverá possuir suporte para balanceamento de carga no sensor de inspeção de tráfego, possibilitando assim obter uma melhor performance;

8.10.3.1.39. Deverá permitir a análise específica de eventos de segurança de computadores suspeitos de atividade maliciosa;

8.10.3.1.40. Os módulos que compõem a solução devem atuar de forma integrada, centralizando logs de incidentes em ponto único;

8.10.3.1.41. Deve possuir atualização automática de regras e assinaturas, sendo que estas devem ser disponibilizadas via web pelo fabricante da solução;

8.10.3.1.42. Deve possuir mecanismo de consultas automáticas em bases de reputação externas de propriedade do fabricante da solução;

8.10.3.1.43. Deve ser capaz de identificar movimentos laterais em uma rede corporativa;

48.10.3.1.44. Deve atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede;

8.10.3.1.45. Deve possuir interface web para busca e investigação local de incidentes;

8.10.3.1.46. O ambiente controlado de sandbox deve contemplar, pelo menos, os sistemas operacionais CentOS, Windows 10, Windows 7, Windows Server 2003, 2008, 2012 R2, 2016 e 2019; Deve possuir possibilidade de habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento web;

8.10.3.1.47. Deve possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e Botnets; Deve possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como: consultas DNS em servidor não autorizado, utilização de SMTP server não autorizado, Proxy Server não autorizado;

8.10.3.1.48. Deve possuir regras que identifiquem comunicações p2p, instant messengers e streaming;

48.10.3.1.49. Deve possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características: Resumidos;

8.10.3.1.50. Visão Geral dos Incidentes de Segurança Discriminação dos Tipos de Incidentes Top Ameaças Analisadas Top Hosts Infectados Recomendações de Segurança Executivos;

8.10.3.1.51.Deve possuir detalhes técnicos dos incidentes detectados; Deve possuir estatística do tráfego analisado; Deve possuir indicadores de risco do ambiente; Recomendações de Segurança.

8.10.3.1.52. Deve ser capaz de identificar, filtrar e exibir em interface gráfica, e dinamicamente atualizada, hosts com alto nível de risco, classificando os tipos de riscos/eventos detectados;

8.10.3.1.53. Deve possuir interface que apresente em Real Time estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URL's maliciosas acessadas, etc.;

8.10.3.1.54. Quando detectada uma ameaça, a solução deve prover, podendo esta realizar consultas

em site do fabricante, informações sobre ameaça, família da ameaça, estatísticas de segmentos de mercado afetados e recomendações de segurança para eliminar ameaça, correlacionando estas informações com sites ou outros vetores por onde esta ameaça é disseminada;

8.10.3.1.55. As atualizações do produto (patterns e outros componentes) não devem causar downtime ou impacto na operação;

8.10.3.1.56. Deve ser capaz de identificar ameaças que afetam dispositivos móveis (Ex. Detecção de comunicação de aplicativo malicioso na plataforma Android);

8.10.3.1.57. Deve ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns ou protocol tunneling;

8.10.3.1.58. Deve ser capaz de detectar tentativas de scan de rede; Deve ser capaz de detectar propagação de malwares na rede;

8.10.3.1.59. Deve ser capaz de detectar tentativas de brute-force; Deve ser capaz de detectar tentativas de fuga e roubo de informação;

8.10.3.1.60. Deve ser capaz de detectar ameaças que se replicam na rede; Deve ser capaz de detectar Exploits na rede;

68.10.3.1.61. O Monitoramento de protocolos de comunicação deve ser feito através de appliance único (ou virtual appliance);

8.10.3.1.62. A console de gerenciamento deve possuir mapa mundial, onde são marcadas origens de ataques e eventos de segurança monitorados pela solução;

8.10.3.1.63. Deve permitir busca por informações do destino e origem, incluindo estas: endereço IP, endereço MAC, porta e protocolo;

8.10.3.1.64. Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;

8.10.3.1.65. Capacidade de salvar uma investigação antes de ser finalizada; Capacidade de restaurar uma investigação para continuá-la ou consultá-la;

8.10.3.1.66. Capacidade de emitir relatórios baseados nas investigações;

8.10.3.1.67. Deve permitir apresentação dos dados consultados em vários formatos, incluindo tabela e gráficos;

8.10.3.1.68. Deve trabalhar com geolocalização para identificar a origem geográfica de um ataque;

8.10.3.1.69. Deve ter a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado;

8.10.3.1.70. Deve permitir exportar sob demanda os logs em texto puro (CSV ou similar);

8.10.3.1.71. Deve sugerir consultas a bases de reputação e whois quando encontrados hosts e nomes de domínio;

8.10.3.1.72. Deve permitir investigação por tags (palavras-chave) pré-configuradas para facilitar a busca de eventos;

8.10.3.1.73. Deve permitir recebimento de logs via syslog;

8.10.3.1.74. Deve permitir encaminhamento de logs via syslog;

8.10.3.1.75. Deve permitir receber logs de diferentes dispositivos;

8.10.3.1.76. Deve possuir engine de correlação de eventos;

8.10.3.1.77. Deve inserir tags personalizadas nos logs, de acordo com regras especificadas pelo usuário;

8.10.3.1.78. A solução de análise em sandbox deve ter a capacidade de analisar, de forma estática e dinâmica, ameaças com características de autoinicialização ou alteração de arquivos de sistema, rootkits/cloakings, arquivos mal-formados, engenharia social, dentre outros;

8.10.3.1.79. A análise de sandbox deve identificar e analisar ameaças que tenham características de evitar a segurança e análise em sandbox, e auto-preservação;

8.10.3.1.80. Deve enviar alertas via e-mail para pelo menos 100 e-mails diferentes; Deve permitir a configuração de alarmes personalizados, com base em investigações;

8.10.3.1.81. Deve informar em sua console alarmes que dispararam, até que o usuário tome alguma ação;

8.10.3.1.82. A console de gerenciamento deverá ser web, apresentando alta disponibilidade de modo que na ausência da principal, o restante da solução permaneça ativa e funcionando;

8.10.3.1.83. A solução deve ser escalável horizontalmente, permitindo que novas instâncias sejam habilitadas, aumentando suas capacidades de detecção e analise;

8.10.3.1.84. A console de gerenciamento deverá ter dashboards para facilidade de monitoração. As

janelas deverão ser customizadas pelo administrador em quantidade e período de monitoração;

8.10.3.1.85. O administrador deve poder optar por janelas de monitoramento no dashboard a sua disposição e poderá livremente adicionar ou remover de acordo com sua necessidade de visualização;

8.10.3.1.86. Deverá possuir mapa geográfico que permita a identificação visual sobre a origem de ameaças de modo a facilitar a visualização de eventos críticos para que ações imediatas sejam providenciadas; Deverá possuir a capacidade de atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;

8.10.3.1.87. A console de gerenciamento deverá ser gerenciada por Internet Explorer, Google Chrome e Firefox;

8.10.3.1.88. Solução deverá ter mecanismo de busca em sua console de gerenciamento de modo que seja facilitada a busca por detecções;

8.10.3.1.89. Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;

8.10.3.1.90. Deverá ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque;

8.10.3.1.91. Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações: Uso de CPU Uso de Disco;

8.10.3.1.92. Uso de Memória;

8.10.3.1.93. Tráfego malicioso analisado;

8.10.3.1.94. Todo o tráfego analisado. A solução deverá permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog e deverá conter no mínimo: Tipo de evento de detecções: Conteúdo malicioso, reputação de URL's, comportamentos maliciosos, comportamentos suspeitos, Exploits, correlações de eventos, Grayware;

8.10.3.1.95. Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações.

8.10.3.1.96. A solução deverá ter integração com ferramentas de SIEM;

8.10.3.1.97. Deve possuir capacidade de entregar relatório contendo informações da sequência de execução do artefato malicioso, assim como, detalhes de alterações locais da máquina, conexões externas e envio da informação para fora da rede corporativa;

8.10.3.1.98. A solução deve prover serviço de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em transito através de logs de sensor;

8.10.3.1.99. Solução deverá apresentar relatórios customizados de todas as suas funcionalidades e deverá conter no mínimo: Computadores infectados; Origem de infecções; Estatísticas de ameaças;

8.10.3.1.100. Riscos potenciais de segurança; Riscos de perda de informações;

8.10.3.1.101. Risco de sistema comprometido;

8.10.3.1.102.Risco de disseminação de ameaças;

8.10.3.1.103. Eventos suspeitos;

8.10.3.1.104. Infecções de malware. A solução deverá apresentar função de pesquisa por logs contendo no mínimo: Critérios de pesquisa por dia, mês e ano. Possibilidade de pesquisa pelo nome do computador, domínio ou conta, endereço IP, endereço MAC e grupos;

8.10.3.1.105. Possibilidade de pesquisa por ameaças, URL's maliciosas, análises virtuais, correlação de incidentes, nome de malware, protocolo e direção da detecção;

8.10.3.1.106. Os relatórios e logs deverão ser exportados nos formatos PDF ou CSV. Módulo de Detecção e Resposta A solução deve ter a capacidade de integrar-se com a plataforma de investigação e resposta centralizada, a fim de enviar objetos suspeitos e metadados das detecções locais para correlação com as demais soluções de segurança do ambiente;

8.10.3.1.107. A funcionalidade deve ser licenciada para analisar o throughput total do appliance;

8.10.3.1.108. A solução deve permitir a integração dos eventos ocorridos em outros segmentos de rede e outros appliances com objetivo de correlacionar os ataques na rede;

8.10.3.1.109. Deve permitir a análise em linha de tempo gráfica, representando a sequência da comunicação dos ativos, bem como seu protocolo e direção;

8.10.3.1.110. Deve identificar tentativas de ataques avançados na rede da CONTRATANTE e correlacionar com eventos das soluções de estação de trabalho, servidores e e-mail, a fim de rastrear o passo-a-passo do ataque na rede;

8.10.3.1.111. Caso necessário, a CONTRATANTE pode optar em direcionar parte do

licenciamento deste módulo para outros módulos da plataforma de Detecção e Resposta, como o monitoramento do email, endpoint ou servidores, sem acréscimos ou mudanças de licenciamento;

8.10.3.1.112. Ao clicar em um dos objetos identificados pela solução de inspeção de rede, a plataforma deverá informar um resumo do ataque em questão, contendo o IP/hostname envolvido, quais protocolos, atividades maliciosas, severidade do incidente, fases do ataque;

8.10.3.1.113. Deve exibir de forma e em tabela, as transações identificadas contendo detalhes do ataque, bem como os Indicadores de Comprometimento (IOCs).

8.10.4. SOLUÇÃO DE PREVENÇÃO DE INTRUSÃO DE PRÓXIMA GERAÇÃO (NGIPS) (ITEM 4)

8.10.4.1. Plataforma e Performance A solução NGIPS (NEXT GENERATION INTRUSION PREVENTION SYSTEM) ofertada deverá ser disponibilizada em hardware do próprio fabricante, não sendo aceitos hardwares de fabricantes terceiros, não sendo aceitos também hardwares homologados (quando o fabricante da solução-software e do hardware são empresas diferentes); Não serão aceitas soluções NGFW ou UTM; O NGIPS deverá suportar a importação de regras no padrão SNORT, podendo esta ocorrer de forma direta e nativa via interface de gerenciamento, ou então através de ferramenta de conversão, onde o arquivo padrão SNORT deverá ser importado e convertido para o padrão utilizado pela solução ofertada;

8.10.4.2. A solução NGIPS deverá possuir interfaces de rede modularizadas com, pelo menos, 2 slots para inserção de módulos;

8.10.4.3. Os módulos disponíveis para a solução NGIPS devem contemplar, pelo menos, expansão até 20 interfaces 10/100/1000Gbps, expansão até 20 interfaces 1Gbps SFP, expansão até 16 interfaces 10Gbps SFP+ e expansão até 4 interfaces 40Gbps QSFP+ (os transceivers necessários deverão ser entregues em conjunto da solução);

8.10.4.4. Para atendimento do bypass das interfaces cobre, não serão aceitos dispositivos externos. Nas interfaces de fibra óptica deverá ser ofertado módulo de bypass, que poderá ser embutido ou externo;

8.10.4.5. A solução NGIPS deverá usar discos de estado sólido (SSD), não sendo aceitos equipamentos com discos mecânicos;

8.10.4.6. Deverá ser entregue equipamento NGIPS que atenda às seguintes especificações: IPS com throughput de inspeção de 3Gbps, podendo ser expandido até 5Gbps sem necessitar trocar o equipamento;

8.10.4.7. Deverá gerar latência igual ou inferior a 40 Microsegundos;

8.10.4.8. Deverá suportar pelo menos 390.000 novas conexões por segundo;

8.10.4.9. Deverá suportar pelo menos 29 milhões de sessões concorrentes;

8.10.4.10. Deverá suportar pelo menos 3.300 novas conexões SSL por segundo;

8.10.4.11. Deverá suportar inspeção de tráfego SSL de até 3,5Gbps;

8.10.4.12. O hardware ofertado deverá possuir fontes redundantes do tipo hot-swap;

8.10.4.13. O hardware ofertado deverá operar entre 0°C até 40°C;

8.10.4.14. O hardware ofertado deverá operar em ambientes com umidade entre 5% e 95%. Requisitos Técnicos e de Segurança A solução NGIPS ofertada deverá prover funcionalidades de prevenção de intrusão, em seu modo default (configuração básica) com pelo menos 2000 regras ativas (habilitadas automaticamente quando uma nova política de segurança é criada, em modo bloqueio e com criação de notificação);

8.10.4.15. A solução NGIPS ofertada deverá prover funcionalidades de prevenção de intrusão, em seu modo default (configuração básica) com pelo menos 2000 regras ativas (habilitadas automaticamente quando uma nova política de segurança é criada, em modo bloqueio e com criação de notificação);

8.10.4.16. Os filtros providos pelo NGIPS deverão permitir a seleção de ações de resposta. Deverão existir pelo menos as seguintes ações: Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Captura de Pacotes), além de ações condicionais, que permitam a definição de ações que alternam entre permitir e bloquear determinados tráfegos / ataques de acordo com condições encontradas no ambiente como, por exemplo, permitir as 1000 primeiras conexões de um único IP para determinado tráfego de rede em um período de 15 minutos. Após a conexão 1001 na mesma janela de tempo, a ação deverá ser alternada para bloqueio;

8.10.4.17. A solução NGIPS deverá suportar assinaturas de IPS para proteger vulnerabilidades, detectar exploits, detectar roubo de informações, detecção de virus, detecção de spywares, detectar tentativas de reconhecimento de rede, possuir regras que ajudem a controlar comportamentos de rede (exemplo: permitir ou bloquear resposta de comandos ping, detectar falhas de autenticação no MS SQL Server), possuir regras que blindem equipamentos de rede contra ataques que explorem

vulnerabilidades, regras que efetuem a normalização de tráfego, ou seja, detectem tunelamento de protocolos, e cabeçalhos IP incompletos, além de filtros que permitam e detecção e controle de aplicações, tais como youtube, skype, TOR e facebook;

18.10.4.18. Os filtros do NGIPS precisam estar segmentados por categorias, com o objetivo de facilitar o gerenciamento da solução. Deverão existir pelo menos as seguintes categorias: Políticas de Segurança, Exploits, Normalização de Tráfego, Vírus, Reconhecimento de Rede, P2P e Vulnerabilidades;

8.10.4.19. O total de filtros disponíveis na solução (não necessariamente para uso simultâneo) não deve ser inferior a 16.000;

8.10.4.20. A solução NGIPS deverá ser capaz de permitir a criação e uso de políticas de segurança granulares baseados nos seguintes métodos: Por NGIPS (todos os segmentos de rede de um IPS);

8.10.4.21. Por segmento físico, podendo selecionar o modo bi-direcional ou unidirecional (permitindo ativar a política de segurança nos sentidos de comunicação de A > B e de B > A [na mesma politica de segurança]. Ou com política de segurança dedicada de A > B e também de B > A); Por TAG de VLAN (802.1Q), de forma direcional e bi-direcional;

8.10.4.22. Por CIDR (Range de endereços IP);

8.10.4.23. Baseado no horário do dia. A solução NGIPS deverá ser capaz de detectar e bloquear ataques de reconhecimento de rede;

8.10.4.24. A solução NGIPS deverá prover filtros de detecção de aplicações tais como P2P, Online Games, permitindo a ativação de controles de banda;

8.10.4.25. Deverá possuir ferramenta para criação de filtros customizados, sendo que estes deverão permitir a customização de parâmetros tais como: Nome do filtro; Descrição do filtro; Protocolo, permitindo a criação de filtros de proteção baseados nos protocolos IPv4, ICMPv4, UDP, TCP, HTTP, IPv6 e ICMPv6;

8.10.4.26. Severidade do filtro, devendo possuir pelo menos 4 níveis; Customização da categoria do filtro;

8.10.4.27. Classe do filtro (devendo possuir pelo menos as classes DoS, Exploit, Virus e Acesso); Gatilhos de acionamento (triggers), onde parâmetros ou informações/dados contidos no streaming de rede serão utilizados como gatilho para validação de parâmetros adicionais da regra;

8.10.4.28. Detecção de payload, permitindo o uso de strings e expressão regular para detecção avançada de instruções no streaming de rede; Detecção de payload dentro do protocolo HTTP, permitindo o uso de strings e expressão regular para buscar e validar a existência de informações no cabeçalho HTTP, distinguindo métodos GET, POST, OPTIONS, PUT, DELETE, TRACE, CONNECT, HEAD, LOCK, UNLOCK, PROPFIND. Também deverá permitir a validação de dados específicos em URI, URI PATH, URI Target, Header e Payload;

8.10.4.29. Criação de customizações a nível TCP, sendo possível definir portas de origem e destino, além de validação de flags TCP;

8.10.4.30. A solução NGIPS ofertada deverá suportar processamento de tráfego assimétrico;

8.10.4.31. Deverá ser possível colocar a solução em modo bypass total forçado;

8.10.4.32. A solução NGIPS deverá possuir Machine Learning, ou seja, deverá possuir filtros que implementem Machine Learning na detecção de, por exemplo, conteúdo obfuscado em HTML associado/relacionado a exploit kits;

8.10.4.33. Deverá possuir filtros de gerenciamento de tráfego, ou seja, deverá ser possível criar regras para controlar o tráfego no sentido de A para B, de B para A, liberando o tráfego (com inspeção de riscos de segurança), liberando o tráfego (sem inspecioná-lo, confiando na conexão), bloqueando o tráfego, e também permitindo a criação de políticas de controle de banda, permitindo limitar, por exemplo, determinado fluxo de dados de rede a 100kbps;

8.10.4.34. A solução de NGIPS deverá possuir controles de proteção contra ataques de DDOS, atuando como um SYN PROXY; A solução de NGIPS deverá possuir filtros que detectem a tentativa de uso de TOR, TeamViewer;

8.10.4.35. A solução de NGIPS deverá detectar e bloquear tráfego Skype; A solução de NGIPS deverá detectar e permitir o bloqueio de tunelamento de conexões DNS;

8.10.4.36. A solução de NGIPS deverá possuir assinatura que permita a validação de requisições HTTP 2.0;

8.10.4.37. A solução de NGIPS deve bloquear nativamente a transferência de arquivos maliciosos via FTP; A solução deve detectar ataques baseados em SSL, como por exemplo detectar o uso de certificados SSL/TLS maliciosos. Atualizações de Segurança A solução de NGIPS ofertada precisa entregar detalhes sobre a cobertura para vulnerabilidades Microsoft reportadas nos últimos 12 meses;

8.10.4.38. O fabricante da solução NGIPS deve prover estatísticas do número de vulnerabilidades de dia zero descobertas nos últimos 5 anos.;

8.10.4.39. O fabricante da solução NGIPS deverá possuir times de pesquisa de vulnerabilidades de dia zero e de riscos de segurança, com pelo menos 1500 pesquisadores, sejam contratados ou parceiros, sendo que deverão ser apresentadas estatísticas dos últimos 3 anos de vulnerabilidades pesquisadas e descobertas. O fabricante deverá estar entre os Top 5 maiores pesquisadores do mundo nos relatórios publicados pela entidade Frost & Sullivan (Analysis of the Global Public Vulnerability Research);

8.10.4.40.A solução NGIPS deverá suportar atualizações automáticas dos filtros/assinaturas, possuindo frequência de atualizações mínima semanal (fabricante deverá entregar 1 atualização por semana); Sempre que a solução NGIPS atualizar-se, o novo pacote de atualizações deverá conter descritivo visualizável na própria solução (console local do NGIPS ou gerenciamento centralizado), indicando quais filtros foram incluídos, quais foram modificados e quais foram removidos. O mesmo deve ocorrer para os filtros de ameaças (malwares), sendo exigidos os mesmos parâmetros para permitir o acompanhamento e monitoramento dos novos filtros adicionados pela solução. Correlação de Informações e Consultas em Nuvem Reputação de Endereços IP, DNS e URLs;

8.10.4.41. A solução NGIPS ofertada precisa permitir o bloqueio de tráfego baseado na reputação do endereço de IP de origem da conexão, de destino da conexão, através da reputação de DNS e URLs;

8.10.4.42. O serviço de reputação deverá contar com categorias tais como: Malware, Botnet, Spyware, SPAM, TOR, Web, Application Attackers, P2P e Network Worm; Deverá ser possível criar exceções baseadas em domínio e endereços IP, assim como deverá ser possível estabelecer as políticas de reputação individuais para cada perfil de segurança em uso no ambiente;

8.10.4.43. A base de reputação IP deverá suportar IPv4 e IPV6;

8.10.4.44. A base de reputação IP deverá ser baseada em informações do próprio fabricante, e também permitir o uso de bases terceiras;

8.10.4.45. Os filtros de reputação de IP deverão atuar tanto no sentido inbound quanto outbound;

8.10.4.46. As políticas de reputação deverão permitir a customização de ações tanto para bloquear ou permitir determinados acessos;

8.10.4.47. Deverá ser possível criar filtros de controle de acesso inbound e outbound baseados em geolocalização. Proteção Avançada Contra Ameaças A solução NGIPS deverá possuir funcionalidade que permita a identificação e proteção contra atividades maliciosas relacionadas a virus e spywares, no sentido inbound e outbound;

8.10.4.48. A solução NGIPS deverá possuir assinaturas de proteção contra malwares;

8.10.4.49. As assinaturas de malware deverão detectar a infiltração, exfiltração e comunicação com servidores de comando e controle através da inspeção do tráfego de rede;

8.10.4.50. A solução deverá ser capaz de interromper atividades maliciosas tais como ransomware, fuga de dados, click fraud, etc;

8.10.4.51. Deverá bloquear ameaças do tipo drive-by-downloads;

8.10.4.52. Deverá detectar atividades de comunicação com servidores de comando e controle de botnets;

8.10.4.53. Os filtros de malware deverão ser atualizados de forma regular pelo fabricante da solução. Alta Disponibilidade A solução de NGIPS deve suportar a operação de forma redundante, com possíveis cenários de operação Ativo-Passivo e AtivoAtivo;

8.10.4.54. A gerência da solução deve permanecer ativa em caso de indisponibilidade dos NGIPS e possui cenários de alta disponibilidade;

8.10.4.55. A solução NGIPS ofertada deverá suportar fontes do tipo hot-swappable;

8.10.4.56. A solução NGIPS deverá suportar software bypass; Em caso de atualizações ou reinicializações do NGIPS, a solução não deverá gerar nenhuma interrupção de rede. Gerenciamento Centralizado A solução NGIPS precisa suportar ser gerenciada de maneira centralizada por solução fornecida pelo mesmo fabricante;

8.10.4.57. A solução de gerenciamento centralizado entregue deverá permitir o gerenciamento de pelo menos 4 equipamentos NGIPS, sendo possível efetuar os mesmos níveis de configuração existentes na solução NGIPS;

8.10.4.58. A solução NGIPS deverá permitir integração com ferramentas de monitoramento de rede e SIEM tais como, HP ArcSight, além de permitir o envio de alertas por e-mail notificando incidentes de segurança;

8.10.4.59. A solução de gerenciamento centralizado deverá possuir um painel de monitoramento de

eventos, contendo pelo menos as estatísticas dos principais filtros acionados, principais atacantes, principais alvos dos ataques etc.;

8.10.4.60. A solução de gerenciamento centralizado deverá permitir a integração com dispositivos de rede, tais como switchs e roteadores, com recursos que permitam alterar a configuração de VLAN de portas de rede, e desligar determinada porta de um switch de rede. Este recurso poderá ser utilizado para contenção de incidentes internos de segurança;

8.10.4.61. A solução de gerenciamento centralizado deverá possuir API que permita soluções externas, como o próprio SIEM, a interagir com a solução NGIPS, devendo permitir pelo menos a adição e remoção de endereços IP suspeitos em listas de reputação, e permitindo adicionar e remover endereços IP suspeitos da quarentena dos NGIPS;

8.10.4.62. A solução de gerenciamento centralizado deverá possuir recurso para relacionar relatórios de testes de penetração realizados no ambiente da empresa, permitindo comparar tais relatórios com políticas de segurança em uso, indicando quais regras ou filtros são necessários ativar para alinhar a política de segurança com as vulnerabilidades identificadas no ambiente;

8.10.4.63. A solução deverá possuir suporte nativo a pelo menos as seguintes ferramentas: Qualys, Nessus e Nexpose; A solução de gerenciamento centralizado deverá possuir módulo de relatórios próprio, possuindo templates que indiquem os principais riscos de segurança detectados no ambiente, contando com pelo menos 20 modelos pré-estabelecidos.

8.10.4.64. Deverá ser possível agendar o envio destes relatórios, sendo exigidos no mínimo os seguintes formatos de arquivo: PDF, DOCX, XLS, CVS e XML; A solução de gerenciamento centralizado deverá suportar o gerenciamento paralelo de pelo menos 4 IPS. A solução ofertada deverá estar dimensionada para atender o exigido neste edital, com crescimento suportado previsto para até 20 NGIPS;

8.10.4.65. A solução de gerenciamento centralizado deverá permitir a integração com soluções de Sandboxes (detecção de ameaças desconhecidas) de modo a permitir que URLs contendo executáveis sejam analisados e testados por soluções de sandboxes que devem ser do próprio fabricante, a fim de identificar novas ameaças direcionadas ao ambiente. Indicadores como endereços IP e DNS relacionados a novas ameaças devem ser passíveis de bloqueio através da própria solução NGIPS (solução de sandbox deverá fazer o feedback dos indicadores relacionados a novas ameaças);

8.10.4.66. A solução de gerenciamento centralizado deverá possuir dashboard que permita a adição ou remoção de painéis que serão utilizados no monitoramento do ambiente, indicando os hosts comprometidos, hosts vulneráveis que sofreram ataques, lista de objetos suspeitos com quantidades de hits identificados;

8.10.4.67. A solução de gerenciamento centralizado deverá permitir a integração com serviços de diretório, tendo suporte aos métodos de autenticação CAC, RADIUS, TACACS+ e Active Directory, além de autenticação local (para uso enquanto solução não é integrada com restante da infraestrutura);

8.10.4.68. A solução deverá ser fornecida em modo de alta disponibilidade, tendo pelo menos 2 nós de redundância; Quando implementado em modo alta disponibilidade, a solução de gerenciamento centralizado deverá permitir a operação usando IP Virtual;

8.10.4.69. A solução de gerenciamento deverá possuir API que permita que soluções terceiras interajam podendo por exemplo quarantenar determinado endereço IP, desquarentenar determinado endereço IP, inserir e remover endereços IP de uma lista de reputação;

8.10.4.70. A solução de gerenciamento centralizado deverá atuar como ponto central para o gerenciamento de políticas de IPS, devendo possuir versionamento de políticas, capacidade de rollback, além de capacidade de importação e exportação de configurações.

8.10.4.71. Solução de visibilidade de superfície de ataques (ITEM 7) Deseja-se uma abordagem de avaliação de risco semi-quantitativa que forneça os benefícios de abordagens quantitativas e qualitativas. Uma comparação de riscos com outras organizações deve estar disponível para evitar os problemas.

8.10.4.72. A plataforma deve fornecer as três abordagens de análise: "Orientada por Ameaças, Ativos/Impactos e Vulnerabilidades". Análise rigorosa, a plataforma deve fornecer análises baseadas em gráficos para fornecer uma maneira eficaz de considerar as muitas relações muitos-para-muitos.

8.10.4.73. A análise de risco deve ser contínua e automatizada. A plataforma deve fornecer um índice global de risco. A plataforma deve fornecer sugestões sobre as ações de remediação mais importantes para reduzir o risco geral.

8.10.4.74. A plataforma também deve fornecer um índice de risco com base nas configurações de produtos integrados do fornecedor para reduzir o risco induzido por erros humanos. A gestão da

superfície de ataque deve ser integrada na plataforma, fornecendo informações sobre Dispositivos Internos, Ativos Voltados para a Internet, Contas e Aplicações na Nuvem. Deve ser fornecido um painel para exibir todos os usuários/dispositivos com Alto Risco para tomada de ações. As fontes de dados devem incluir sensores de Rede, Ponto de extremidade, Web, Móvel e Email.

8.10.4.75. Devem ser suportadas fontes de dados de terceiros para análises adicionais a nível de identidade, como Azure AD, Office 365, AD local. Devem ser suportadas fontes de dados de terceiros para análises adicionais a nível de dispositivo, como Qualys, Nessus e Tenable.

8.10.4.76. Deseja-se ingestão de dados de terceiros de Firewall (Fortinet/Palo Alto/Cisco) e Portais da Web (Forcepoint/Zscaler/Cisco Umbrella/Symantec ProxySG). A plataforma deve detectar a conta de um usuário na dark web.

8.10.4.77. A plataforma deve fornecer informações sobre contas de usuários que apresentaram atividades anômalas de alto risco ou que foram especificamente alvo de campanhas de e-mail maliciosas.

8.10.4.78. A plataforma deve detectar vulnerabilidades exploráveis do sistema operacional no ponto de extremidade. A plataforma deve detectar vulnerabilidades exploráveis do aplicativo no ponto de extremidade.

8.10.4.79. A plataforma deve indicar se a exploração está sendo explorada globalmente e, nesse caso, em que nível (Alto/Médio/Baixo).

8.10.4.80. A plataforma deve fornecer insights sobre o uso do armazenamento em nuvem (OneDrive/SharePoint/Outlook/Teams) pela conta que pareça anormal em comparação com o uso normal de outras contas da empresa. A plataforma deve exibir a localização geográfica e o número de vezes que seus usuários ou dispositivos acessaram o aplicativo em nuvem em um determinado dia.

8.10.4.81. A plataforma deve informar padrões de comportamento e preferências de usuário anormais em nível de dispositivo e usuário.

8.10.4.82. A plataforma deve fornecer um guia para reduzir fatores de risco detectados.

8.10.4.83. A plataforma deve permitir definir um objetivo de redução de risco. Visualizar um resumo dos eventos de risco que você deve remediar para alcançar o objetivo selecionado e alterar o status dos eventos de risco. Visualizar informações sobre os ativos que foram mais impactados por cada evento de risco.

8.10.4.84. A plataforma deve permitir as seguintes ações para responder a riscos: Desativar/Ativar conta do usuário - Forçar logout - Redefinir senha - Isolar/Restaurar Endpoint - Monitorar tentativas de login - Monitorar/Bloquear/Desbloquear/Permitir aplicativo interno - Bloquear/Desbloquear/Permitir Acesso a aplicativos ou URLs em nuvem.

8.10.4.85. A plataforma deve avaliar o risco de aplicativos em nuvem acessados pelos usuários pelo menos com base nos seguintes critérios: Conformidade com padrões (por exemplo, CSA STAR LEVEL, ISO, NIST) Recursos de segurança (por exemplo, autenticação multifator, proteção contra DoS) Cabeçalhos de segurança (por exemplo, x-frame-options, política de segurança de conteúdo) Violacões de segurança ou outros eventos que possam indicar um serviço comprometido Escudo de Privacidade UE-EUA/Suíça-EUA FINRA RGPD GLBA HIPAA/HITECH.

8.10.5. SERVIÇO DE SUPORTE PRO ATIVO, CORRETIVO E PARA RESPOSTA A INCIDENTES (ITEM 5)

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

8.10.5.2. Todo o Serviço de Suporte deverá ser prestado por profissional certificado pelo Fabricante da Solução, em nível compatível com a prestação do serviço.

8.10.5.3. Deverá ser apresentado comprovação da certificação dos profissionais responsáveis no ato da assinatura do contrato.

8.10.5.4. Deverá disponibilizar um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução ofertada; deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução.

8.10.5.5. Suporte Proativo:

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

8.10.5.5.2. A contratada deverá notificar a contratante sobre atualizações de segurança, patches e

correções assim que estiverem disponíveis, caso autorizado aplicar as atualizações de segurança e evolutiva dos produtos;

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

8.10.5.5.4. Deverá realizar avaliações regulares de riscos para identificar possíveis vulnerabilidades e pontos fracos nos sistemas e, implementar medidas corretivas com base nos resultados das avaliações de riscos;

8.10.5.5.5. Realizar auditorias regulares para garantir que as melhores práticas e os controles de segurança estejam operacionais e, utilizar resultados de auditorias para implementar melhorias contínuas;

8.10.5.5.6. A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução do problema.

8.10.5.6. Suporte Corretivo:

8.10.5.6.1. Este componente concentra-se na solução de problemas ou incidentes. O suporte corretivo atua de forma ágil para restabelecer a funcionalidade normal do sistema, minimizando impactos negativos e mantendo a continuidade operacional;

8.10.5.6.2. Serviço Especializado de Suportes corretivo para 36 (trinta e seis) meses. Serviço de Suporte especializado para ajustes, correções e configurações da solução a ser fornecida. Neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução;

8.10.5.6.3. A contratada deverá: Implementar um sistema de abertura de chamados, para registrar, rastrear e priorizar incidentes e requisições de suporte;

8.10.5.6.4. Conforme detalhado no item 8.10;

8.10.5.6.5. Atribuir números de caso exclusivos para facilitar a comunicação e o acompanhamento;

8.10.5.6.6. Garantir disponibilidade 24/7 para responder a incidentes críticos. Deverá apresentar relatório contendo as ações adotadas para a solução do problema.

8.10.5.7. Resposta a Incidentes:

8.10.5.7.1. O serviço de resposta a incidentes deverá lidar com eventos imprevistos, como violações de segurança, falhas críticas ou interrupções inesperadas. deverá ser realizada por profissionais especializados e certificados pelo fabricante;

8.10.5.7.2. Deverá realizar investigações para determinar a natureza, origem e impacto de incidentes de segurança;

8.10.5.7.3. Desenvolver planos de mitigação e estratégia de recuperação para minimizar o impacto de incidentes;

8.10.5.7.4. Elaborar relatórios detalhados sobre os incidentes, incluindo ações tomadas e recomendações de melhorias.

8.10.6. SERVIÇO DE IMPLANTAÇÃO (ITEM 6)

8.10.6.1. Nesta etapa, compreende-se a instalação e configuração da solução contratada, contados a partir da emissão da Ordem de Serviço (OS);

8.10.6.2. O serviço de implantação abrange integralmente as fases essenciais para a integração, instalação e configuração da solução contratada, alinhando-se precisamente com as especificações técnicas e requisitos predefinidos. Esta abordagem abarca desde o planejamento inicial até a conclusão efetiva, assegurando uma transição suave dos processos existentes para a nova solução;

8.10.6.3. O Plano de Implantação assume a forma de um documento fundamental que consolida a estratégia para instalação, configuração e entrega da solução contratada. Sua importância reside em orientar e alinhar as atividades, garantindo eficiência e uma implementação adequada da solução conforme os requisitos estabelecidos;

8.10.6.4. O documento deverá conter no mínimo os requisitos de ambiente tecnológicos necessários para a instalação das licenças, cronograma e detalhamento das atividades a serem realizadas, topologia do ambiente pós instalação da solução, matriz de responsabilidade, plano de comunicação;

8.10.6.5. Durante esta etapa, a equipe da Contratada deverá estar presente nos horários de instalação definidos pelo Contratante. As atividades de instalação e configuração poderão ser realizadas, conforme necessário, em horário comercial, período noturno ou final de semana;

8.10.6.6. O Contratante disponibilizará a infraestrutura de hardware e software necessária e já existente em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução durante esta etapa.

8.10.7. SERVIÇO DE CAPACITAÇÃO E REPASSE DE CONHECIMENTO (ITEM 7)

8.10.7.1. Repasse de conhecimento, na forma de treinamento para técnicos, de forma virtual, para 1 (uma) turma, com carga horária mínima de 40 (quarenta) horas, abrangendo todos os softwares integrantes da suíte de solução de segurança;

8.10.7.2. O conteúdo programático abordará tanto aspectos teóricos quanto práticos, contemplando de maneira abrangente todos os módulos relevantes da solução de segurança;

8.10.7.3. O treinamento pode ser segmentado de acordo com o produto a ser instalado no ambiente tecnológico, contemplando, no mínimo, os seguintes módulos:

8.10.7.3.1. Instalação do módulo de gerenciamento central; Instalação do software de Endpoint Protection em estações de trabalho e servidores;

8.10.7.3.2. Descrição e configuração de todas as funcionalidades contratadas da solução;

8.10.7.3.3. Melhores práticas utilizadas no mercado para otimização dos softwares e suas funcionalidades.

8.10.7.3.4. A carga horária mínima estabelecida será de 40 (quarenta) horas, divididas em expedientes de 4 horas por dia, no horário comercial.

8.10.7.3.5. A contratada é responsável por fornecer apostilas em formato digital que contemplem o conteúdo referente ao produto, oferecendo suporte ao aprendizado prático e teórico dos participantes;

8.10.7.4. Este treinamento visa capacitar adequadamente os usuários finais, garantindo que compreendam e aproveitem plenamente as funcionalidades da solução de segurança. O enfoque prático e teórico, aliado às melhores práticas do mercado, promove uma formação abrangente e eficaz.

(...)

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

(...)

10.1. Garantia (ID SEI! 0055727564)

10.1.1. A garantia do produto será por 36 (trinta e seis) meses, conforme segue:

10.1.2. Complexidade Técnica dos Equipamentos

10.1.2.1. Equipamentos como **soluções de segurança avançada, servidores, sistemas NGIPS e endpoints** possuem componentes eletrônicos e software que exigem alta especialização para manutenção e suporte. A **garantia estendida** assegura que:

10.1.2.2. Falhas técnicas serão corrigidas por profissionais qualificados, mantendo o desempenho do sistema.

10.1.2.3. Haverá substituição de peças e componentes de hardware com padrões técnicos exigidos pelo fabricante.

10.1.2.4. As atualizações de software (patches de segurança, melhorias) serão implementadas sem custos adicionais durante o período da garantia.

10.1.3. Vida Útil e Durabilidade do Equipamento

10.1.3.1. O período de 36 meses da garantia estendida está alinhado à **vida útil esperada** de equipamentos de tecnologia. Isso significa:

10.1.3.2. Durante os primeiros anos, é comum que ocorram **falhas de hardware ou software** devido ao uso contínuo e exigências operacionais.

10.1.3.3. A garantia estendida proporciona **proteção contra desgaste** ou mau funcionamento prematuro.

10.1.4. Necessidade de Manutenção Preventiva e Corretiva

10.1.4.1. Soluções avançadas exigem **manutenção contínua** para garantir a **operacionalidade** e **segurança do ambiente tecnológico**. A garantia estendida cobre:

10.1.4.2. **Manutenção preventiva**: inspeções periódicas para evitar falhas.

10.1.4.3. **Manutenção corretiva**: correção imediata em caso de falhas identificadas.

10.1.4.4. **Substituição de peças críticas**: sem custos adicionais para a administração.

10.1.5. Redução do Risco Operacional

10.1.5.1. Equipamentos como os mencionados no **item 03 (Solução de Segurança Avançada)** e demais soluções tecnológicas são **críticos** para a proteção da rede e continuidade das operações. A **garantia estendida**:

10.1.5.2. Mitiga riscos de **interrupção dos serviços**.

10.1.5.3. Reduz impactos financeiros e operacionais decorrentes de falhas no sistema.

10.1.5.4. Assegura a **disponibilidade contínua** do serviço.

10.1.5.5. Suporte Técnico Especializado

10.1.5.6. Fabricantes e parceiros certificados possuem equipes **altamente qualificadas** para atuar em falhas complexas. A garantia estendida:

10.1.5.7. Garante acesso a suporte técnico especializado.

10.1.5.8. Proporciona **respostas rápidas** para incidentes críticos.

10.1.5.9. Inclui **ferramentas exclusivas e diagnósticos avançados**, o que não é oferecido na garantia legal básica do CDC.

10.1.5.10. **Garantam a qualidade e continuidade do serviço**.

10.1.5.11. Sejam **proporcionais** ao objeto contratado.

(...)

4.5 Das condições contratuais/garantia do contratual: Ficam aquelas estabelecidas no item 21.. e seus subitens do Anexo I – Termo de Referência , as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente, conforme transcrevemos:

(...)

18. DO CONTRATO E SUA EXECUÇÃO

18.1. Conforme disposto no art. 95, inciso II, da Lei 14.133/2021, em caso de compras com entrega imediata e integral dos bens adquiridos e dos quais não resultem obrigações futuras, inclusive quanto a assistência técnica, independentemente de seu valor, o instrumento de contrato poderá ser substituído por instrumento hábil, neste caso a nota de empenho de despesas.

18.2. Portanto, para os objetos deste certame que apresentem garantia estendida, será celebrado contrato.

18.3. Convocação e Celebração do contrato

18.3.1. Oficialmente convocada pela Administração com vistas à celebração do Termo Contratual é dado à contratada o prazo de até 05 (cinco) dias úteis, contado da data da ciência ao chamamento, pela Secretaria de Estado da Saúde, para no local indicado, firmar o instrumento de Contrato.

18.3.2. Após análise dos documentos supramencionados e convocação pela Secretaria de Estado da Saúde, será dado à contratada o prazo de até 05 (cinco) dias úteis, para firmar o instrumento de Contrato.

Será designada Comissão devidamente nomeada por meio de Portaria, pelo Gestor da Pasta, para recebimento, análise e julgamento da documentação.

21. DA GARANTIA CONTRATUAL

21.1. Para fiel execução dos compromissos aqui ajustados a CONTRATADA prestará prévia garantia de 5% (cinco por cento) do valor do valor inicial do contrato, como previsto no art. 98 da lei 14.133/2021;

21.2. A critério da autoridade competente, em cada caso, poderá ser exigida, mediante previsão no edital, prestação de garantia nas contratações de obras, serviços e fornecimentos.

21.3. A CONTRATADA poderá optar por uma das modalidades de garantia previstas no art. 96, § 1°, da Lei 14.133/2021;

21.4. A CONTRATADA terá o prazo de 10 (dez) dias, prorrogáveis por igual período, posteriores à assinatura do contrato, para apresentação da garantia contratual;

21.5. A garantia prestada pelo contratado será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, atualizada monetariamente, conforme art. 100 da Lei 14.133/2021.

(...)

4.6. Do reajuste e supressão contratual: Ficam aquelas estabelecidas no item 18.5. e seus subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente, conforme transcrevemos:

(...)

18.5. DA REPACTUAÇÃO, DO REAJUSTE E DA REVISÃO DO CONTRATO

18.5.1. Considerando as necessidades de garantia do equilíbrio econômico-financeiro dos contratos da administração pública deve ser atendido e preceituado nos parâmetros dos Art. 150 ao Art. 168

do Decreto nº 28.874 de 25 de janeiro de 2024.

18.5.2. Para os fins previstos de restabelecimento do equilíbrio econômico-financeiro fica estabelecido como data-base a apresentação da proposta ou previsões restritas, nos casos de repactuação e orçamento de obras, ainda deve ser observado o prazo para apresentação do pedido, expedido no Art. 151 do Decreto nº 28.874/2024.

18.5.3. No que tange aos índices de reajuste a serem aplicados para fins do restabelecimento econômico-financeiro, adotar-se-á o que for mais vantajoso para a Administração, devendo ser observado a existência de índice próprio para o objeto contratual, conforme Art. 156 do Decreto nº 28.874/2024.

18.5.4. No caso concreto aplicar-se o Índice Nacional de Preços ao Consumidor Amplo - IPCA, para fins de reajuste e restabelecimento do equilíbrio econômico-financeiro.

18.5.5. DO REAJUSTE

18.5.5.1. Conforme previsão no arts. 154 ao 156 do Decreto nº 28.874/24.

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

18.5.5.3. Ao final dos 12 (doze) meses iniciais de vigência do contrato, caso seja optado pela prorrogação, os reajustes serão efetuados com base no índice IGP-M da Fundação Getúlio Vargas, ou em outro índice que seja mais benéfico para a Administração. Ressalta-se que, em qualquer caso, será observada a periodicidade anual para a recomposição dos preços, em conformidade com as disposições legais aplicáveis.

18.5.5.4. O reajuste em sentido estrito, espécie de reajuste nos contratos de obra, fornecimento ou serviço continuado sem dedicação exclusiva de mão de obra, consiste na aplicação de índice de correção monetária estabelecido no contrato, que retratará a variação efetiva do custo de produção, admitida a adoção de índices específicos ou setoriais.

18.5.5.5. O prazo para resposta ao pedido de restabelecimento do equilíbrio econômico-financeiro, será de até 15 (quinze) dias úteis, a contar do recebimento da solicitação.

18.5.6. DA REPACTUAÇÃO

18.5.6.1. Conforme previsão no art. 157 do Decreto nº 28.874/24: A repactuação de preços, como espécie de reajuste contratual, deverá ser utilizada nas contratações de serviços continuados com regime de dedicação exclusiva de mão de obra.

18.5.6.2. Dessa forma, a repactuação não será aplicada a pretensa contratação.

18.5.12. **REVISÃO**

18.5.12.1. Conforme previsão no arts. 163 ao 164 do Decreto nº 28.874/24.

18.5.12.2. A revisão contratual será concedida, a pedido da contratada, para promover o reequilíbrio econômico-financeiro da avença, diante da ocorrência de fatos imprevisíveis, ou previsíveis com consequências incalculáveis, retardadores ou impeditivos da execução do contrato, ou, ainda, em caso de força maior, caso fortuito ou fato do príncipe, configurando álea econômica extraordinária e extracontratual.

18.5.12.3. O pedido de revisão de contrato deverá ser instruído com os seguintes documentos:

I - requerimento da contratada devidamente assinado pelo seu responsável;

II - planilha de custos demonstrando a equação inicial do contrato;

III - planilha de custos demonstrando a equação atual do contrato;

IV - documentação hábil demonstrando a ocorrência de fatos imprevisíveis, fatos previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou, ainda, caso de força maior, caso fortuito ou fato do príncipe, que configurem álea econômica extraordinária e extracontratual;

V - ato do ordenador de despesa do órgão ou entidade que decidir pelo reconhecimento das circunstâncias que autorizam a revisão do contrato;

VI - pesquisa de preços praticados no mercado a fim verificar se o preço reequilibrado permanece atendendo o pressuposto fundamental da licitação, se for o caso.

18.5.12.4. Parágrafo único. A revisão será formalizada por meio de termo aditivo.

18.5.12.5. O prazo para resposta ao pedido de revisão para restabelecimento do equilíbrio econômico-financeiro, será de até 15 dias úteis, a contar do recebimento da solicitação.

(...)

4.7. D a fiscalização e acompanhamento do recebimento/execução do objeto: Ficam aquelas estabelecidas no item 9. e seus subitens do Anexo I – Termo de Referência, as quais foram

devidamente aprovadas pelo ordenador de despesa do órgão requerente, conforme transcrevemos:

(...)

9. MODELO DE EXECUÇÃO DO OBJETO

9.1. Execução dos Serviços

9.1.1. A CONTRATANTE no uso de suas atribuições legais nomeará Fiscais de Contrato, sendo indicado pelo representante da área requisitante o servidor que possui conhecimento técnico do objeto da contratação e designado pelo Secretário de Estado da Saúde - SESAU, mediante a Portaria, para acompanhar e fiscalizar a execução contratual, responsabilizando-se pela verificação do efetivo cumprimento das obrigações pactuadas e respectivo ateste das faturas/notas fiscais, juntamente com a comissão de recebimento em conformidade com o Art. 117º da Lei Federal n.º 14.133 de 1º Abril de 2021 e acórdão nº. 4/2006 - TCU e Anexo I - Guia de Fiscalização dos Contratos, deste Termo de Referência.

9.1.2. A prestação dos serviços deverá estar dentro dos parâmetros e rotinas estabelecidas, fornecendo todos os produtos, peças, acessórios, componentes eletrônicos, materiais, utensílios e equipamentos em quantidade, qualidade e tecnologia adequadas, com observância às recomendações aceitas pelas boas técnicas, normas e legislação vigente e em quantidades necessárias à boa execução dos serviços.

9.1.3. A CONTRATANTE fiscalizará a execução do serviço contratado e verificará o cumprimento das especificações solicitadas, no todo ou em parte, no sentido de corresponderem ao desejado ou especificado.

9.1.4. A fiscalização pela CONTRATANTE, não desobriga a CONTRATADA de sua responsabilidade quanto à perfeita execução do objeto deste instrumento;

9.1.5. A ausência de comunicação por parte da CONTRATANTE referente a irregularidades ou falhas, não exime a CONTRATADA das responsabilidades determinadas no Contrato;

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

9.1.7. A CONTRATADA se obriga a permitir que auditoria interna da CONTRATANTE e/ou auditoria externa por ela indicada tenham acesso a todos os documentos que digam respeito ao objeto deste instrumento, inclusive auditoria a ser realizada na usina de incineração.

9.1.8. A CONTRATANTE realizará avaliação da qualidade do atendimento, dos resultados concretos dos esforços sugeridos pela CONTRATADA e dos benefícios decorrentes da política de preços por ela praticada.

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

9.1.10.A Contratada deverá possuir estoque mínimo de peças para realizar o serviço da manutenção corretiva quando houver a necessidade de troca das mesmas.

9.1.11. Os serviços deverão ser executados em horários que não interfiram no bom andamento da rotina de funcionamento da contratante;

9.1.12. Requisitos Temporais

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

9.1.13. Requisitos de Segurança e Privacidade

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

9.1.14. Garantia da disponibilidade, integridade, confidencialidade e sigilo das informações:

9.1.14.1. A empresa CONTRATADA deve assegurar a disponibilidade, integridade, confidencialidade e sigilo dos documentos e informações relacionados ao contrato e aos serviços prestados. Qualquer pessoa que cause perdas e danos à CONTRATANTE ou a terceiros poderá ser responsabilizada legalmente.

9.1.15. Devolução de informações confidenciais:

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

situações:

a) término ou rompimento do contrato; ou

b) solicitação da CONTRATANTE. A formalização entre as partes é necessária nesses casos.

9.1.16. Utilização de ferramentas de proteção e segurança de informações:

9.1.16.1. É imprescindível o uso de ferramentas de proteção e segurança de informações para evitar acesso não autorizado aos sistemas e softwares. Isso se aplica tanto aos sistemas sob responsabilidade direta da CONTRATADA quanto aos disponibilizados à CONTRATANTE, mesmo que por meio de link.

9.1.17. Realização de alterações para sanar problemas de segurança ou vulnerabilidade:

9.1.17.1. Quando formalmente solicitado pela CONTRATANTE, a CONTRATADA deve priorizar e realizar alterações para solucionar possíveis problemas de segurança ou vulnerabilidade nos sistemas ou softwares utilizados para a execução do serviço contratado.

9.1.18. Comunicação de atualizações ou mudanças na configuração dos serviços:

9.1.18.1. A CONTRATADA deve informar formalmente e de forma tempestiva ao CONTRATANTE sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados.

9.1.19. Prestação de esclarecimentos e informações:

9.1.19.1. É responsabilidade da CONTRATADA prestar os esclarecimentos necessários à CONTRATANTE, bem como fornecer informações sobre a natureza e o andamento dos serviços executados ou em execução.

9.1.20. Garantia da integridade e disponibilidade dos documentos e informações:

9.1.20.1. A empresa CONTRATADA deve garantir a integridade e disponibilidade dos documentos e informações que estão sob sua guarda em função do contrato. Caso ocorram perdas ou danos, a CONTRATADA será responsabilizada.

9.1.21. Confidencialidade das informações:

9.1.21.1. A CONTRATADA não pode divulgar, mesmo que em caráter estatístico, quaisquer informações originadas na CONTRATANTE sem prévia autorização.

9.1.22. Controle de acesso e identificação dos profissionais:

9.1.22.1.O acesso às instalações da CONTRATADA onde os serviços serão realizados deve ser controlado e permitido apenas para pessoas autorizadas. Os profissionais da CONTRATADA devem estar devidamente identificados por crachás durante o trabalho. Qualquer profissional considerado inconveniente à boa ordem ou que viole as normas disciplinares da CONTRATANTE deve ser substituído imediatamente.

9.1.23. Conhecimento e observância das normas disciplinares da CONTRATANTE:

9.1.23.1.A CONTRATADA deve garantir que seus profissionais tenham conhecimento das normas disciplinares do CONTRATANTE e exijam sua fiel observância, especialmente em relação à utilização e segurança das instalações.

9.1.23.2. A CONTRATADA deve manter sigilo absoluto sobre todas as informações provenientes dos serviços realizados, documentos elaborados e informações obtidas dentro do ambiente da CONTRATANTE.

9.1.24. Requisitos Legais

9.1.24.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021 (Lei de Licitações e Contratos Administrativos), à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

9.1.25. Prazo de início de atendimento para suporte técnico e manutenção pela garantia: O início do atendimento deve seguir o que está especificado no acordo de nível de serviço presente no Termo de Referência.

(...)

4.8. Da entrega/recebimento: Ficam aquelas estabelecidas nos itens 9.2 a 9.5. e subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente, conforme transcrevemos:

(...)

9.2. **LOCAL DE ENTREGA:**

92.1. Os respectivos equipamentos serão entregues na Coordenadoria de Almoxarifado e

Patrimônio, localizado na Rua Aparício Moraes, 4378 - Industrial, Porto Velho - RO, 76821-240, onde serão atestados pela respectiva conforme Portaria Comissão de Recebimento CAP/SESAU (0050062995).. Funcionamento de segunda a sexta-feira das 7h30min às 13h30min.

9.2.2. **Horário de entrega dos equipamentos/serviços**: A entrega dos equipamentos/serviços deve ocorrer entre as 07:30 e 13:30. É possível agendar uma data e hora específica previamente com a CONTRATANTE.

9.2.3. **Verificação da conformidade dos materiais entregues:** É responsabilidade da CONTRATANTE rejeitar, total ou parcialmente, os materiais entregues que não estejam de acordo com o objeto definido no Termo de Referência.

9.2.4. **Recebimento dos produtos:** O recebimento dos produtos será feito pela equipe designada pela CONTRATANTE. Esse recebimento ocorrerá de forma provisória no momento da entrega dos equipamentos e de forma definitiva após a instalação, configuração e teste da solução.

(...)

(...)

9.3. **PRAZO DA ENTREGA:**

9.3.1. O prazo para início dos serviços será de até 30 (trinta) dias contados a partir da última assinatura do contrato.

9.3.2. **Prazo de início de atendimento para suporte técnico e manutenção pela garantia:** O início do atendimento deve seguir o que está especificado no acordo de nível de serviço presente no Termo de Referência.

9.3.3. **Prazo de entrega e instalação:** O prazo de entrega e instalação deve estar de acordo com o que foi especificado no Termo de Referência. Caso não haja uma definição específica, o prazo padrão será considerado conforme a ordem de serviço.

9.3.4. A entrega deverá ocorrer conforme solicitação da Unidade de Saúde com definição da quantidade, no prazo máximo de 30 (trinta) dias corridos, após o recebimento da nota de empenho ou assinatura do contrato de fornecimento.

9.4. Os equipamentos deverão ser entregues de acordo com as especificações técnicas e demais disposições constantes em contrato, não sendo permitido à Comissão recebê-los fora das especificações pré-definidas.

9.4.1. Todo o material deverá ser entregue em embalagens individuais, em perfeito estado de conservação, lacrada e adequadas para proteger o conteúdo contra danos durante o transporte, desde o fornecedor até o local da entrega, sob condições que envolvam embarques, desembarques, transportes, por rodovias não pavimentadas, marítimos ou aéreos;

9.4.2. Os procedimentos de recebimento provisório e definitivo do objeto diretamente na unidade requisitante deve ser orientado e acompanhado pela Coordenadoria de Almoxarifado e Patrimônio-CAP/SESAU/RO, de forma a atender os padrões regulares de recebimento e demais encaminhamentos para incorporação do bem ao patrimônio público da Secretaria.

9.4.3. O objeto deverá ser indiscutivelmente novo e sem uso. Não serão aceitos equipamentos e materiais que tenham sido objeto de quaisquer processos de reciclagem e/ou recondicionamento e ainda, os que se apresentarem fora das embalagens originais de seus fabricantes.

(...)

(...)

9.5. DA ENTREGA E DO RECEBIMENTO

9.5.1. A entrega deverá ocorrer conforme solicitação via requisição da Secretaria de Saúde até o prazo máximo de 30 (trinta) dias, a contar da data de recebimento da Ordem de Fornecimento, Ordem de Serviço e/ou Nota de Empenho.

9.5.2. A empresa concorrente homologada deverá acusar o recebimento da Ordem de Fornecimento e/ou Nota de Empenho para fornecimento em 48h (quarenta e oito horas), iniciar e comunicar à 9.5.3. Administração as providências para cumprimento dos prazos subsequentes.

9.5.4. No caso de não confirmação de recebimento da requisição do objeto pela Secretaria de Estado da Saúde de Rondônia no prazo de 05 (cinco) dias, a requisição será dada como recebida.

9.5.5. A entrega ocorrerá em parcela única, sem parcelamento da entrega.

9.5.6. O recebimento do objeto será realizada por Comissão de Recebimento de Materiais e Serviços designada pela Secretaria de Estado da Saúde de Rondônia, da unidade requisitante e/ou da Coordenadoria de Almoxarifado e Patrimônio-CAP/SESAU/RO, ou ainda por comissão especificamente designada, à critério da Administração, conforme Art. 140, inciso II da Lei Federal nº 14.133/2021.

"Art. 140. O objeto do contrato será recebido:

II - em se tratando de compras:

a) provisoriamente, de forma sumária, pelo responsável por seu acompanhamento e fiscalização, com verificação posterior da conformidade do material com as exigências contratuais;

b) definitivamente, por servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências contratuais.

§ 1º O objeto do contrato poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

§ 2º O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança da obra ou serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos pela lei ou pelo contrato.

§ 3º Os prazos e os métodos para a realização dos recebimentos provisório e definitivo serão definidos em regulamento ou no contrato.

§ 4º Salvo disposição em contrário constante do edital ou de ato normativo, os ensaios, os testes e as demais provas para aferição da boa execução do objeto do contrato exigidos por normas técnicas oficiais correrão por conta do contratado.

§ 5º Em se tratando de projeto de obra, o recebimento definitivo pela Administração não eximirá o projetista ou o consultor da responsabilidade objetiva por todos os danos causados por falha de projeto.

§ 6º Em se tratando de obra, o recebimento definitivo pela Administração não eximirá o contratado, pelo prazo mínimo de 5 (cinco) anos, admitida a previsão de prazo de garantia superior no edital e no contrato, da responsabilidade objetiva pela solidez e pela segurança dos materiais e dos serviços executados e pela funcionalidade da construção, da reforma, da recuperação ou da ampliação do bem imóvel, e, em caso de vício, defeito ou incorreção identificados, o contratado ficará responsável pela reparação, pela correção, pela reconstrução ou pela substituição necessárias."

9.5.6. A Contratante promoverá através de seus representantes, o acompanhamento e a fiscalização da entrega dos produtos sob os aspectos quantitativo e qualitativo, anotando as falhas detectadas e comunicando a Contratada as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte daquela através dos procedimentos de recebimento, que ocorrerão da seguinte forma:

9.5.7. Provisoriamente por servidor ou comissão designada pela Coordenadoria de Almoxarifado e Patrimônio-CAP/SESAU/RO, de forma sumária imediatamente depois de efetuada a entrega através de recibo aposto na nota fiscal. O recebimento provisório deve ser concluído dentro do prazo de até 05 (cinco) dias, devendo o CAP/SESAU/RO neste interim tomar as devidas providências para que ocorra o recebimento definitivo juntamente à unidade requisitante, a fim de se proceder a verificação da conformidade dos produtos com as especificações de forma integrada.

9.5.8. Definitivamente por Comissão de Recebimento de Materiais e Serviços designada da unidade requisitante, ou por comissão especificamente designada, depois de concluída a vistoria, encerrado o prazo de observação que não poderá exceder 10 (dez) dias, e, mediante termo detalhado que comprove adequação do objeto ao requerido e aprovado pela Administração, o atendimento das exigências contratuais e consequente aceitação.

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

9.5.10. Em fomento à assertividade na análise técnica do objeto a comissão de recebimento poderá dispor de avaliação complementar de setor especializado ou comissão especialmente designada, caso necessário, por sua conveniência e oportunidade.

9.5.11. Salvo disposição em contrário constante do edital ou de ato normativo, os ensaios, os testes e as demais provas para aferição da boa execução do objeto do contrato exigidos por normas técnicas oficiais correrão por conta do contratado.

9.5.12. A Contratante poderá rejeitar no todo ou em parte os materiais entregues em desacordo com as especificações técnicas do objeto ou com as obrigações assumidas.

9.5.13. Se o fornecedor vencedor tiver comprovadamente dificuldades para entregar os materiais, dentro do prazo estabelecido, não sofrerá multa, caso informe oficialmente com antecedência de mínimo 03 (três) dias úteis, antes de esgotado o prazo inicialmente previsto, apresentando justificativa circunstanciada formal, que deverá ser encaminhada ao Secretário de Estado da Saúde que, por sua vez, decidirá a possibilidade de prorrogação do prazo, ou determinará a cominação das multas cabíveis, que ocorrerá a partir da efetiva notificação;

9.5.14. Se, após o recebimento provisório, for constatado que os materiais foram entregues de forma incompleta ou em desacordo com as especificações ou com a proposta, será interrompido o

prazo de recebimento definitivo e suspenso o prazo de pagamento até que seja sanada a situação;

9.5.15. A empresa vencedora ficará obrigada a trocar, às suas expensas, o que for recusado por apresentar-se contraditório as especificações contidas no Termo de Referência;

9.5.16. O objeto deverá ser entregues de acordo com as especificações técnicas e demais disposições constantes no Termo de Referência, não sendo permitido a Comissão, receber os equipamentos fora das especificações pré-definidas.

9.5.17. O objeto deverá ser indiscutivelmente novo e sem uso. Não serão aceitos itens que tenham sido objeto de quaisquer processos de reciclagem ou recondicionamento. Deverão estar acondicionados em embalagem própria conforme ao fabricante, garantindo sua integridade.

9.5.18. A Contratada fica sujeito às sanções administrativas previstas, quando for o caso.

(...)

4.9. Do pagamento: Ficam aquelas estabelecidas no item 24. e subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente, conforme transcrevemos:

(...)

24. PAGAMENTO

24.3. Deverão ser apresentadas no ato da entrega do serviço, a Nota Fiscal em favor do**:**

a) Fundo Estadual de Saúde - RO.

b) CNPJ Nº: 00.733.062/0001-02.

c) Endereço: Av. Farquar, 2986, Complexo Rio Madeira, Edifício Rio Machado (Entrada pela PIO XII) – Bairro: Pedrinhas – CEP: 76.801-470 - Porto Velho/RO.

24.4. No corpo da Nota Fiscal/Fatura deverá conter:

a) A descrição detalhada do item;

b) Valor unitário do objeto de acordo com a nota de empenho;

c) Identificação de Número do Processo e identificação da Nota de empenho;

d) Identificação do Banco (código), da Agência Bancária, do Número da Conta Bancária, para fins de pagamento, bem com, das correções fiscais e contábeis, se for o caso.

24.5. O pagamento será efetuado conforme recebimento e atesto dos seguintes documentos:

a) Nota Fiscal devidamente devidamente atestadas pela Administração, conforme disposto no no art. 140, inciso II, alíneas "a" e "b" da Lei 14.133/2021;

b) Comprovação da entrega do item com o termo de recebimento assinado pela comissão designada em portaria.

24.6. O pagamento decorrente de contratações públicas será feito após a habilitação para pagamento, no prazo máximo de **15 (quinze) dias úteis**, consoante o disposto no art. 190 do Decreto 28.874/2024.

24.7. No caso das Notas Fiscais apresentarem erros ou dúvidas quanto à exatidão, ou documentação, a Administração Pública poderá pagar apenas a parcela incontroversa no prazo fixado para pagamento, ressalvado o direito da empresa de representar para cobrança, as partes controvertidas com devidas justificativas, nestes casos, a Administração Pública terá o prazo de até 05 (cinco) dias úteis, a partir do recebimento, para efetuar análise e pagamento devidamente atestadas pela Administração.

24.8. Na hipótese da contratada não estar regular perante a Fazenda Estadual, o contratado será instado a se manifestar sobre a possibilidade de compensação do crédito com o débito existente, caso em que os autos serão remetidos ao órgão fazendário para as providências cabíveis, com prévia oitiva da Procuradoria - Geral do Estado em caso de débito inscrito em dívida ativa. Em caso de não concordância com a compensação, imediatamente após o pagamento da contraprestação, os autos serão remetidos à Procuradoria-Geral do Estado para adoção das providências cabíveis para recuperação do crédito estadual.

24.9. Em caso de descumprimento das obrigações trabalhistas e previdenciária, o pagamento será retido até a regularização, sem prejuízo das sanções cabíveis.

24.10.Não será efetuado qualquer pagamento, salvo as parcelas incontroversas, à (s) empresa (s) Contratada (s) enquanto houver pendência de liquidação da obrigação financeira em virtude de penalidade ou inadimplência contratual.

24.11. Quando da ocorrência de eventuais atrasos de pagamento provocados exclusivamente pela Administração, o valor devido deverá ser acrescido de atualização financeira, e sua apuração se fará desde a data de seu vencimento até a data do efetivo pagamento, em que os juros de mora

serão calculados à taxa de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, mediante aplicação das seguintes fórmulas:

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

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.

24.12. Ocorrendo erro no documento da cobrança, este será devolvido e o pagamento será sustado para que a Contratada tome as medidas necessárias, passando o prazo para o pagamento a ser contado a partir de data da reapresentação do mesmo. Caso se constate erro ou irregularidade na Nota Fiscal, a Administração, a seu critério, poderá devolvê-la, para as devidas correções, ou aceitá-las, com a glosa da parte que considerar indevida.

24.13. Na hipótese de devolução, a Nota Fiscal será considerada como não apresentada, para fins de atendimento das condições contratuais.

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

24.15. Conforme a Instrução Normativa RFB nº 1.234/2012, alterada pela Instrução Normativa RFB nº 2.145/2023, e com a Instrução Normativa nº 34/2023/SEFIN-COTES, será realizada a retenção na fonte do Imposto de Renda incidente sobre os valores pagos à CONTRATADA, nos casos legalmente previstos, incluindo rendimentos oriundos de fornecimento de bens ou prestação de serviços.

(...)

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

(...)

20.1. DA CONTRATADA:

20.1.1. Além daquelas exigidas na Lei Federal 14.133/2021, e, Lei Estadual 28.874/2024, deverá:

20.1.2. Responsabilizar-se integralmente pelos materiais adquiridos, nos termos da legislação vigente;

20.1.3. Entregar o objeto da aquisição nas especificações contidas neste Termo de Referência;

20.1.4. Entregar o objeto na forma e prazo estipulados neste Termo de Referência;

20.1.5. Entregar o objeto nas quantidades indicadas pelo órgão requisitante;

20.1.6. Os materiais que não atenderem exigências deste edital não serão aceitos e recebidos, devendo ser substituídos imediatamente.

20.1.7. Não promover substituição do produto empenhado, sem anuência expressa da contratante;

20.1.8. Entregar os produtos em embalagem íntegra, sob pena de rescisão do ajuste, independentemente das combinações legais cabíveis;

20.1.9. No Pregão Eletrônico não há quantidade mínima a ser adquirida, tampouco obrigatoriedade de aquisição de todo o quantitativo licitado, e, em caso de eventuais contratos de fornecimento decorrentes da Aquisição, a Contratada se obriga a aceitar as supressões nas quantidades inicialmente previstas respeitando os limites da Lei 14.133/21 e os parâmetros da Lei 28.874/2024, tendo como base os preços constantes da(s) proposta(s) Contratada(s), diante de necessidade comprovada da Administração.

20.1.10. Responsabilizar-se pela substituição do produto entregue em desconformidade com este Termo de Referência, ou impossibilitados de uso devido, perda ou deterioração de suas características, devendo ser trocados no prazo máximo de 20 (vinte) dias uteis, contados a partir de comunicação formal do responsável. O ônus de todas as despesas decorrentes da efetivação da troca será da Contratada;

20.1.11. Manter durante toda execução da Ata, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

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

20.1.13. Considerar em todas as etapas de vinculação e arcar efetivamente com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas e todos os tributos incidentes, sem qualquer ônus à Contratante, devendo efetuar os respectivos pagamentos na forma e nos prazos previstos em Lei;

20.1.14. Indicar um preposto devidamente habilitado, com poderes para representá-lo em tudo o que se relacionar com o fornecimento objeto;

20.1.15. Ficarão a cargo da empresa vencedora os custos de frete, impostos, taxas e etc., que venham a incidir sobre a aquisição objeto deste Termo de Referência;

20.1.16. No momento da entrega a empresa deverá apresentar relação com o material entregue e nota fiscal, contendo marca, especificação e quantidade. Os preços propostos deverão incluir fretes e demais custos diretos e indiretos, inclusive os resultantes da incidência de quaisquer impostos, tributos, contribuições ou obrigações trabalhista, fiscais e previdenciárias a que estiver sujeito.

20.1.17. Garantir a qualidade dos produtos ofertados conforme este Termo de Referência e estipulado nas normas técnicas e regulamentações especializadas relacionadas ao objeto de fornecimento;

20.1.18. CUMPRIR E FAZER CUMPRIR, todas as diretrizes, normas, regulamentos impostas por este Termo de Referência e seus ANEXOS.

20.1.19. A contratada deverá reparar, corrigir, remover, reconstituir ou substituir, às suas expensas, os materiais que forem rejeitados, parcial ou totalmente, por apresentarem vícios, defeitos, incorreções, no prazo máximo de 20 (vinte) dias úteis a contar da data do recebimento da comunicação do fato.

20.1.20. A Contratada se obriga a aceitar acréscimos ou supressões nas quantidades inicialmente previstas respeitando os limites do artigo 125 da Lei 14.133/21 e suas alterações, tendo como base os preços constantes da(s) proposta(s) contratada(s), diante de necessidade comprovada da Administração.

20.1.21. É obrigação da Contratada manter durante toda execução do contrato compatibilidade com as obrigações por ela assumida, bem como todas as condições de habilitação e qualificação exigidas na licitação.

20.1.22. A futura contratada deverá cumprir as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social.

(...)

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

(...)

20.2. DA CONTRATANTE:

20.2.1. Além daquelas constantes no Termo de Referência e aquelas determinadas por leis, decretos, normas técnicas, regulamentos e demais dispositivos legais, a CONTRATANTE se obrigará:

20.2.2.Fiscalizar, acompanhar, conferir e avaliar o objeto deste Termo de Referência, através de representantes designados pela SESAU, conforme dispõe a Lei Nº 14.133/2021. Promover através da comissão nomeada, o acompanhamento e a fiscalização da entrega e recebimento dos produtos sob os aspectos quantitativo e qualitativo, anotando as inconformidades ou falhas detectadas e comunicando a Contratada as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte daquela;

20.2.3. Garantir o cumprimento de todas as cláusulas contratuais ao bom desempenho do objeto desta contratação;

20.2.4. Aplicar as penalidades regulamentares cabíveis, quando for o caso;

20.2.5. Devolver o material caso não esteja dentro das especificações constantes do presente Termo de Referência, ou impossibilitados de uso devido por perda ou deterioração de suas características;

20.2.6. Efetuar o pagamento à contratada de acordo com as condições de preços e prazos estabelecidos neste Termo de Referência.

20.2.7. Durante o processo licitatório a Contratante deverá verificar a conformidade das propostas em relação aos requisitos estabelecidos neste termo de referência e no edital.

20.2.8. A quantidade mínima a ser solicitada de cada item será de 10% do valor previsto para cada item. Não há obrigatoriedade de aquisição de todo o quantitativo licitado.

20.2.9. Serão considerados pela Contratante para o presente processo licitatório somente os requisitos da contratação indispensáveis, necessários e suficientes à escolha da melhor solução para a Administração Pública, observadas as leis e regulamentações específicas aplicáveis, bem como padrões mínimos de qualidade e desempenho.

(...)

4.12 **Dos critérios de sustentabilidade:** Ficam aquelas estabelecidas no item 19.2. e subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente, conforme transcrevemos:

(...)

19.2. POSSÍVEIS IMPACTOS AMBIENTAIS e CRITÉRIOS SUSTENTABILIDADE

19.2.1. Embora os impactos ambientais diretos de uma solução de segurança cibernética possam ser menores em comparação a outros tipos de contratações, é fundamental a inclusão de critérios ambientais nos requisitos de contratação, como a exigência de certificações verdes para data centers, a gestão responsável de resíduos eletrônicos e a preferência por fornecedores que adotem práticas sustentáveis, pode garantir que a contratação atenda aos princípios de sustentabilidade ambiental.

19.2.1.1. Certificações Ambientais

a) Certificações de Data Centers: Exigir que os fornecedores possuam certificações como LEED (Leadership in Energy and Environmental Design) ou ISO 14001, que atestam práticas de construção e operação ambientalmente responsáveis.

b) Certificações de Sustentabilidade: Preferir fornecedores que têm certificações de sustentabilidade reconhecidas, como o Energy Star, que garantem eficiência energética.

19.2.1.2. Gestão de Resíduos Eletrônicos

a) Reciclagem e Descarte Responsável: Exigir que os fornecedores adotem políticas claras de reciclagem e descarte de equipamentos eletrônicos, garantindo que eles não sejam enviados para aterros sanitários de forma inadequada.

b) Reutilização de Equipamentos: Incentivar a reutilização e a recuperação de equipamentos, promovendo práticas de economia circular.

19.2.1.3. Eficiência Energética

a) Uso de Fontes de Energia Renovável: Preferir fornecedores que utilizem energia renovável em suas operações, como solar ou eólica, e que apresentem planos para aumentar a proporção de energia limpa utilizada.

b) Otimização de Consumo Energético: Avaliar o consumo energético das soluções propostas e exigir relatórios sobre como os fornecedores planejam reduzir a pegada de carbono.

19.2.1.4. Transparência e Relatórios

a) Relatórios de Sustentabilidade: Solicitar que os fornecedores apresentem relatórios de sustentabilidade anuais que detalhem suas práticas ambientais e metas de redução de impactos.

b) Políticas de Sustentabilidade: Pedir uma declaração clara das políticas ambientais e sociais do fornecedor, incluindo objetivos e estratégias.

19.2.1.5. Inovação e Desenvolvimento Sustentável

a) Investimento em Tecnologias Verdes: Avaliar o comprometimento do fornecedor com inovações que minimizam o impacto ambiental, como soluções de segurança que exigem menos recursos computacionais.

b) Desenvolvimento de Produtos Sustentáveis: Incentivar o desenvolvimento de softwares e soluções que ajudem a otimizar recursos e reduzir o consumo de energia.

19.2.1.6. Formação e Conscientização

a) Treinamento em Sustentabilidade: Exigir que os fornecedores realizem treinamentos para suas equipes sobre práticas sustentáveis e a importância da responsabilidade ambiental.

b) Campanhas de Conscientização: Incentivar fornecedores a participar ou criar campanhas que promovam a sustentabilidade dentro e fora da organização.

(...)

5. DA QUANTIDADE MÍNIMA A SER COTADA

5.1. Não serão registrados valores mínimos ou quantidades mínimas para faturamento e

entrega, conforme item 13. e subitens do Anexo I – Termo de Referência, conforme transcrevemos:

> (...)
>
> 13. **TRATAMENTO DIFERENCIADO A MPE**
>
> 13.1. Em razão do potencial comprometimento na execução do objeto licitatório devido à indivisibilidade do item, a cota de 25% prevista na Lei Complementar nº 123, de 14 de dezembro de 2006, não será aplicada nesta contratação.
>
> 13.2. Igualmente, o critério de exclusividade para Microempresas (ME) e Empresas de Pequeno Porte (EPP) não será implementado, visto que o valor da contratação supera o limite de R$ 80.000,00, conforme disposto no Art. 48, Inciso I, da mencionada lei.
>
> 13.3. Sendo assim, não se aplicará o tratamento favorecido às microempresas, empresas de pequeno porte, sociedades cooperativas referidas no Art. 16 da Lei nº 14.133/2021, ao agricultor familiar, ao produtor rural pessoa física e ao microempreendedor individual (MEI), conforme os parâmetros estabelecidos na Lei Complementar nº 123/2006 e no Decreto nº 8.538/2015. Dado que a licitação não se enquadra nos critérios do Art. 47 da Lei nº 123/2006, por não incluir itens divisíveis ou participação exclusiva de ME/EPP, aplica-se o disposto no Art. 49, Inciso III, da referida legislação.
>
> (...)

6. DA POSSIBILIDADE DE PREVISÃO DE PREÇOS DIFERENTES

6.1. **NÃO SERÁ** admitida a previsão de preços diferentes, conforme item 15.7. e subitens do Anexo I – Termo de Referência, conforme transcrevemos:

> (...)
>
> 15.7. Relativamente a oferta de preços, conforme dispõe o art. 82, inciso III, não serão admitidos preços diferentes, uma vez que para as pesquisas de preços, não incluiu-se preços do comércio LOCAL/DE MUNICÍPIOS DISTINTOS, como forma de obter uma estimativa que contemple os custos necessários, em razão dos aspectos relacionados a localização geográfica.
>
> (...)

6.2. Na hipótese de o preço contratado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão ou entidade gerenciadora convocará o fornecedor para negociar a redução do preço registrado.

6.2.1. Caso não aceite reduzir seu preço aos valores praticados pelo mercado, o fornecedor será liberado do compromisso assumido quanto ao item contratado, sem aplicação de penalidades administrativas.

6.3. Na hipótese de o preço de mercado tornar-se superior ao preço contratado e o fornecedor não puder cumprir as obrigações estabelecidas, será facultado ao fornecedor requerer à Contratante a alteração do preço registrado, mediante comprovação de fato superveniente que supostamente o impossibilite de cumprir o compromisso.

6.4. Neste caso, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória ou a planilha de custos que demonstre a inviabilidade do preço contratado em relação às condições inicialmente pactuadas.

6.5. Na hipótese de não comprovação da existência de fato superveniente que inviabilize o preço contratado, o pedido será indeferido pela Contratante e o fornecedor deverá cumprir as obrigações estabelecidas no Contrato, sob pena de rescisão contratual, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.

6.6. Na hipótese de comprovação da majoração do preço de mercado que inviabilize o preço registrado, conforme previsto no item 5 e no item 5.4 , a Contratante atualizará o preço, de acordo com a realidade dos valores praticados pelo mercado, mediante Termo Aditivo.

7. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

7.1. De acordo com o Art. 164, da Lei n.° 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:

7.1.1. Envio exclusivo para o endereço eletrônico: **supelcotec@gmail.com;**

7.1.2. 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;

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

7.2. 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.

7.3. 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.

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

8. DAS CONDIÇÕES DE PARTICIPAÇÃO

8.1. 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.

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

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

8.3. 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.

8.4. 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 se tornem desatualizados.

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

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

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

8.6.2. 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:

8.6.2.1. 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;

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

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

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

8.6.5. Agente público do órgão, agente público de órgão ou entidade licitante ou

contratante, conforme §§ 1º e 2º do art. 9º da Lei nº 14.133, de 2021.

8.6.6. Pessoas jurídicas reunidas em consórcio observar o art. 15 da Lei n.° 14.133, de 2021 e disposição constante no item 7. do Anexo I - Termo de Referência, conforme transcrevemos:

(...)

7. PARTICIPAÇÃO DE EMPRESAS SOB A FORMA DE CONSÓRCIO E COOPERATIVAS

7.1. Fica vedada a participação de empresas reunidas sob a forma de consórcio e cooperativas, tendo em vista que o objeto da licitação não é de grande porte, complexo tecnicamente e tampouco, operacionalmente inviável de ser executado por apenas uma empresa.

7.2. A ausência de consórcio e cooperativas não trará prejuízos à competitividade do certame, visto que, em regra, a formação de consórcios é admitida quando o objeto a ser licitado envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação do edital.

(...)

8.6.7 **Da subcontratação: Ficam aquelas estabelecidas no item 22.** e subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente, conforme transcrevemos:

(...)

22. DA SUBCONTRATAÇÃO

22.1. A subcontratação será necessária conforme Art. 42, XXIII, do Decreto 28.874/2024, adicionalmente, está em conformidade com o Art. 75, §1º, e Art. 124 da Lei nº 14.133/2021, que preveem condições específicas para subcontratação. Essas condições deverão incluir comprovação de capacidade técnica e alinhamento com os princípios da Administração Pública. Neste caso a subcontratação se faz devidamente fundamentada pelos seguintes motivos (ID SEI! 0055451477 e 0055727564):

a) Falta de Experiência Interna : Se sua equipe interna não tiver a experiência ou especialização necessária em cibersegurança, o subcontratado pode trazer acesso a profissionais especializados e especializados.

b) Recursos limitados : Quando há limitações de recursos, como pessoal, tempo ou orçamento, o subcontratado pode ser uma forma eficaz de obter o nível necessário de proteção sem sobrecarregar sua equipe interna.

c) Necessidade de Soluções Avançadas : Caso sua empresa precise de tecnologias avançadas e infraestrutura robusta que seriam caras de se implementar e manter internamente, a terceirização pode ser mais econômica.

d) Escalabilidade : Se seu negócio está crescendo rápido e sua infraestrutura de TI precisa escalar rapidamente, as empresas de cibersegurança podem ajudar a acompanhar esse crescimento de forma eficaz.

e) Monitoramento Contínuo : Para garantir vigilância e resposta a incidentes em tempo real, 24 horas por dia, sete dias por semana, subcontratando você garante que haja uma equipe dedicada a supervisionar e reagir rapidamente a ameaças.

22.2. Será admitida a subcontratação dos serviços de garantia e assistência técnica, desde que previamente autorizada por escrito pelo contratante, por empresa comprovadamente autorizada pelo fabricante dos equipamentos;

22.2.1. É permitida a subcontratação parcial do objeto, pela contratada à outra empresa, a cessão ou transferência parcial do objeto licitado, nos termos do art. 122 do §2º da Lei Nº 14.133/2021;

"Art. 122. Na execução do contrato e sem prejuízo das responsabilidades contratuais e legais, o contratado poderá subcontratar partes da obra, do serviço ou do fornecimento até o limite autorizado, em cada caso, pela Administração.

§ 1º O contratado apresentará à Administração documentação que comprove a capacidade técnica do subcontratado, que será avaliada e juntada aos autos do processo correspondente.

§ 2º **Regulamento ou edital de licitação poderão vedar, restringir ou estabelecer condições para a subcontratação**. (...)".

22.2.2. Fica autorizada a subcontratação para os itens **05 - Serviço de suporte pro ativo, corretivo e para resposta a incidentes** e **06 - Serviço de implantação** no tópico 3. **Definição do Objeto c/c 3.2 descrição detalhada do objeto citados nesse Termo de referência**, nas seguintes condições:

22.2.3. É vedada a subcontratação total do objeto do contrato, sendo vedada a subcontratação dos serviços que foram utilizados na qualificação técnica da empresa Contratada, relativos às parcelas

de maior relevância técnica e de valor significativo.

22.2.4. A subcontratação depende de autorização prévia por parte do Contratante, que deverá emitir anuência de forma expressa, a quem incumbe avaliar se o subcontratado cumpre os requisitos de qualificação técnica necessários para a execução do objeto.

22.2.5. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da Contratada pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante o Contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

22.2.6. É vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na contratação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau.

(...)

8.7. 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 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.

8.8. É de responsabilidade do cadastrado conferir a exatidão de 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.

8.9. A não observância do disposto no item anterior poderá ensejar **desclassificação** ou inabilitação.

9. DO BENEFÍCIO ÀS MICROEMPRESAS E EMPRESAS DE PEQUENO PORTE

9.1. Na forma do Art. 4º, da Lei Federal n.° 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 n.° 123, de 14 de dezembro de 2006, devendo atentar às regras estabelecidas no regramento específico citado.

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

9.2.1. Declaração, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021;

9.2.2. 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 n.° 14.133, de 2021.

9.2.3. 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.

9.3. A falsidade da declaração sujeitará o licitante às sanções previstas na Lei n.° 14.133, de 2021, neste Edital e em normas correlatas.

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

10. DO REGISTRO DA PROPOSTA NO SISTEMA ELETRÔNICO

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

10.2. O licitante deverá registrar sua proposta, no sistema eletrônico, observando 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.

10.2.1. 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.

10.3. 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.

10.4. 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.

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

10.6. 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.

10.7. 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 15. do Anexo I deste edital - Termo de Referência, que somente será pública após a fase de lances, conforme transcrevemos:

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

11.1. 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.

11.2. O lance deverá ser ofertado pelo valor **UNITÁRIO** de cada item.

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

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

11.5. 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).

11.6. 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.

11.7. O procedimento seguirá de acordo com o modo de disputa Aberto, conforme item 14.1. do Anexo I deste edital - Termo de Referência, conforme transcrevemos:

> (...)
>
> 14.1. O fornecedor será selecionado por meio da realização de procedimento de **LICITAÇÃO**, na modalidade **PREGÃO**, sob a forma **ELETRÔNICA**, modo de disputa **ABERTO**, com adoção do critério de julgamento pelo **MENOR VALOR GLOBAL**
>
> (...)

11.8. 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.

11.9. 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 n.° 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.

11.10. Persistindo o empate, será realizado SORTEIO ELETRÔNICO através do sistema ComprasGov, nos processos cadastrados a partir de 14/10/2024, em sessão pública entre as propostas empatadas, nos moldes do artigo 28, §§ 1º e 2º da Instrução Normativa SEGES/MGI Nº 79.

11.11. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

11.12. 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 n.° 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 n.° 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 das margens de preferência.

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

12.1. 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 n.° 14.133/2021, legislação correlata e no item 7 deste edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação.

12.2. 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.

12.2.1. 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.

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

12.3.1. 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.

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

12.3.3.. 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.

12.4. 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.

12.5. 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.

12.6. 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.

12.7. Caso o Termo de Referência exija a apresentação de amostra, o licitante classificado em primeiro lugar deverá apresentá-la, conforme disciplinado no item 16.1. do Anexo I deste Edital - Termo de Referência, sob pena de não aceitação da proposta, conforme transcrevemos:

> (...)
>
> 16.1. Para o objeto deste TR, a aceitação das propostas não está condicionada a apresentação de amostras, considerando a relevância do produto e o dispêndio financeiro necessário, sendo que a avaliação do produto será verificada por ocasião da entrega, estando tais produtos sujeitos a recusa de recebimento definitivo, caso não corresponda às condições e especificações mínimas definidas nos autos.
>
> (...)

12.8. A PROPOSTA DE PREÇOS, inserida no sistema de Compras.gov.br deverá estar de acordo com o item 15. do Anexo I - Termo de Referência, conforme transcrevemos:

> (...)
>
> **15. DA PROPOSTA**
>
> 15.1. As propostas serão processadas e julgadas pelo **MENOR VALOR GLOBAL.**
>
> 15.2. As propostas apresentadas ao pregão deverão ter prazo de validade mínimo de 90 (noventa) dias a partir da data de apresentação da proposta.
>
> 15.3. A proposta deverá constar o preço unitário e total para cada item, expressos em moeda corrente nacional, nele incluídas todas as despesas/custos com materiais, ferramentas, mão de obra, impostos, taxas, seguro, frete, transporte, depreciação, emolumentos e quaisquer outros custos que, direta ou indiretamente venha ocorrer.
>
> 15.4. As propostas devem considerar integralmente as especificações técnicas comuns de cada item contido no termo de referência e Solicitação de aquisição de materiais e serviços-SAMS, não cabendo às proponentes quaisquer tipo de adaptação que promovam alterações nas especificações técnicas dos objetos.
>
> 15.5. As propostas apresentadas no presente certame deverão condizer à totalidade dos quantitativos respectivos dos iten(s) de interesse das licitantes, não sendo admitido quantidade mínima de unidade de bens a ser cotada, e, não sendo admitido a possibilidade dos licitantes oferecerem propostas em quantitativos inferiores aos máximos previstos no edital, conforme

elencado no Art. 82, incisos II e IV, da Lei 14.133/2021.

15.6. Relativamente a oferta de preços, conforme dispõe o art. 82, inciso III, não serão admitidos preços diferentes, uma vez que para as pesquisas de preços, não incluiu-se preços do comércio LOCAL/DE MUNICÍPIOS DISTINTOS, como forma de obter uma estimativa que contemple os custos necessários, em razão dos aspectos relacionados a localização geográfica.

15.7. PROSPECTO/FOLDER/CATÁLOGO/ENCARTES/FOLHETOS TÉCNICOS EM PORTUGUÊS OU LINKS OFICIAIS QUE O DISPONIBILIZEM, onde constem as especificações técnicas e a caracterização dos mesmos, permitindo a consistente avaliação dos itens.

(...)

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

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

12.9.2. As propostas com prazo de vencimento superior ao mencionado no item 12.9.1., serão enviadas imediatamente à Unidade Gestora sem a referida atualização temporal, para que se dê início ao procedimento homologatório.

12.9.2.1. 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.

12.9.3. 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.

12.9.4. O procedimento mencionado no item 12.9.1 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.

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

13. DA FASE DE HABILITAÇÃO

13.1. Serão realizadas consultas, ao Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual - CAGEFIMP, instituído pela Lei Estadual n.° 2.414, de 18 de fevereiro de 2011, ao Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS/CGU (Lei Federal n.° 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.

13.2. 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.

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

13.4. 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.

13.4.1. 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.

13.5. O não atendimento às exigências desta fase, sem justificativa aceita pela Administração, poderá ensejar a aplicação das sanções previstas no item 21. – Das Penalidades deste Edital.

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

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

13.8. 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.

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

13.9.1. 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

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

13.10. 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.

13.11. 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.

13.12. 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.

13.12.1. A prorrogação do prazo previsto no subitem 13.11. poderá ser concedida, a critério da Administração Pública, quando requerida pelo licitante, mediante apresentação de justificativa.

13.12.2. Ressalvado os documentos possíveis de verificação conforme item 13.4, os licitantes deverão encaminhar, nos termos deste Edital e anexos, a documentação relacionada nos itens a seguir, para fins de habilitação:

13.13. RELATIVOS À REGULARIDADE FISCAL, SOCIAL E TRABALHISTA

13.13.1. Os critérios de regularidade fiscal, social e trabalhista a serem atendidos pelo fornecedor serão aqueles estabelecidos no item 17.2. do Anexo I deste Edital – Termo de Referência, conforme transcrevemos:

> (...)
>
> **17.2. 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, estadual e/ou municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;
>
> d) Certidão de Regularidade do FGTS, relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;
>
> e) 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.

(...)

13.14. RELATIVOS À HABILITAÇÃO JURÍDICA

13.14.1. Os critérios de habilitação jurídica a serem atendidos pelo fornecedor serão aqueles estabelecidos no item 17.1. do Anexo I deste Edital – Termo de Referência, conforme transcrevemos:

(...)

17.1. 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, nos termos do Decreto Federal n° 11.802, de 28 de Novembro de 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 17 de Outubro 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.

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

(...)

13.15. RELATIVOS À QUALIFICAÇÃO ECONÔMICA-FINANCEIRA

13.15.1. Os critérios de qualificação econômico-financeira a serem atendidos pelo fornecedor serão aqueles estabelecidos no item 17.3. do Anexo I deste edital - Termo de Referência, conforme transcrevemos:

(...)

17.3. RELATIVOS À QUALIFICAÇÃO ECONÔMICO - FINANCEIRA

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

b) Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, ou o Balanço de Abertura caso a licitante tenha sido constituída em menos de um ano, devidamente autenticado ou registrado no órgão competente, para que o(a) Pregoeiro(a) possa aferir se esta possui Patrimônio Líquido (licitantes constituídos há mais de um ano) ou Capital Social (licitantes constituídos há menos de um ano), de 5% (cinco por cento) do valor estimado para o ITEM(NS) no qual estiver participando.

b.1) o caso do licitante classificado em mais de um item, o aferimento do cumprimento da disposição acima levará em consideração a soma de todos os valores referenciais;

b.2) caso seja constatada a insuficiência de patrimônio líquido ou capital social para a integralidade dos itens/lotes em que o licitante estiver classificado, o Pregoeiro o convocará para que decida sobre a desistência do(s) item(ns) até o devido enquadramento a regra acima disposta;

b.3) as regras descritas nos itens b.1 e b.2 deverão ser observadas em caso de ulterior classificação de licitante que já se consagrou classificado em outro item(ns).

OBS: As exigências de qualificação econômico-financeira encartadas acima estão em harmonia com o que prevê o art. 69 da Lei 14.133/21 sendo necessário, para garantir que a (s) vencedora (as) detenha (am) condições econômicas para executar o futuro contrato.

(...)

13.16. RELATIVOS À QUALIFICAÇÃO TÉCNICA:

13.16.1. Os critérios de qualificação técnica a serem atendidos pelo fornecedor serão aqueles estabelecidos no item 17.6. do Anexo I deste Edital – Termo de Referência, conforme transcrevemos:

> (...)
>
> **17.6.1. 1. Parcela de Maior Relevância**
>
> 17.6.1.1. A parcela de maior relevância do objeto está associada à Solução de Segurança Avançada para Mitigação de Ameaças na Rede (Item 03), uma vez que este representa o componente mais complexo e tecnicamente exigente do edital. Tal complexidade justifica a necessidade de maior atenção, considerando sua criticidade para a proteção e integridade das operações na rede.
>
> 17.6.1.2. Pela Complexidade Técnica, Criticidade para a Proteção e Integridade da Rede, podemos definir em resumo que: **Solução de Segurança Avançada** é a parte mais importante e difícil do contrato, devido à **tecnologia avançada** que envolve e à **necessidade de proteger de forma eficaz a rede**, que é fundamental para as operações da organização. A complexidade e a criticidade desse item exigem **uma atenção extra** na implementação e gestão da solução
>
> **17.6.2. 2. Documentação Relativos à Qualificação Técnica**
>
> 17.6.2.1. Deverá apresentar Atestado(s) ou Certidão(ões) de Capacidade Técnico-operacional, emitido(s) por pessoa jurídica de direito público ou privado, comprovando que a licitante forneceu, instalou e configurou solução de segurança em características e **pelo menos 30% do item 3,** Solução de Segurança Avançada para Mitigação de Ameaças na Rede, uma vez que este representa o componente mais complexo e tecnicamente exigente do edital
>
> 17.6.2.2. O(s) Atestado(s) ou Certidão(ões) de Capacidade Técnico-operacional devem ser compatíveis em condições e características com o objeto da contratação e deverão conter as seguintes informações mínimas:
>
> a) nome e cargo da pessoa que os assina;
>
> b) quantitativo associado ao fornecimento; e
>
> c) valor e/ou Contrato(s) associado(s) à da prestação dos serviços.
>
> **17.6.3. 3. Parcerias e Certificações de Fabricantes**
>
> 17.6.3.1. A empresa deve apresentar:
>
> 17.6.3.2. Parceria ativa com os fabricantes das soluções propostas, comprovada por cartas de parceria ou autorização de revenda/implementação.
>
> 17.6.3.3. Certificações de parceria que garantam a capacitação técnica e o suporte direto do fabricante.
>
> (...)

13.17. 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.

13.17.1. 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.

13.18. DAS DECLARAÇÕES:

13.18.1. As licitantes deverão dispor as seguintes declarações:

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 n.° 14.133, de 2021;

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

13.19. Não será necessária a juntada as documentações exigidas em meio eletrônico, pela plataforma Compras.gov, com os demais documentos de habilitação/proposta.

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

14. DO RECURSO

14.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021 após a fase de Julgamento e Habilitação, declarada a empresa VENCEDORA do certame, qualquer Licitante dentro do prazo poderá manifestar em campo próprio do Sistema Eletrônico, de forma imediata sua intenção de recorrer no prazo mínimo de 10 (dez) minutos, em cada fase.

14.1.1. A intenção de recorrer deverá ser registrada imediatamente, sob pena de preclusão.

14.2. 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.

14.3. 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.

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

14.5. 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.

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

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

14.8. O recurso terá efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

15. DA HOMOLOGAÇÃO

15.1. 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 n.° 14.133, de 2021.

16. DA REVOGAÇÃO E DA ANULAÇÃO

16.1. 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.

16.2 O motivo determinante para a revogação do processo licitatório deverá ser resultante

de fato superveniente devidamente comprovado.

16.3 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.

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

17. DO TERMO DE CONTRATO OU INSTRUMENTO EQUIVALENTE

17.1. Ficam aquelas estabelecidas no item 18.4. e seus subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente, conforme transcrevemos:

> (...)
>
> **18.4. Formalização do Contrato**
>
> 18.4.1. A Administração convocará regularmente o interessado para assinar o termo de contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo e condições estabelecidos, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas na lei n° 14.133/21.
>
> 18.4.2. O prazo de convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela parte durante o seu transcurso e desde que ocorra motivo justificado aceito pela Administração.
>
> 18.4.3. Será facultado à Administração, quando o convocado não assinar o termo de contrato ou não aceitar ou não retirar o instrumento equivalente no prazo e nas condições estabelecidas, convocar os licitantes remanescentes, na ordem de classificação, para a celebração do contrato nas condições propostas pelo licitante vencedor.
>
> (...)

18. DA RESCISÃO CONTRATUAL

18.1. Ficam aquelas estabelecidas no item 18.6 e seus subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente, conforme transcrevemos:

> (...)
>
> 18.6. **DA INEXECUÇÃO E DA RESCISÃO CONTRATUAL:**
>
> 18.6.1. As obrigações das partes, bem como os direitos e deveres da Contratante e da Contratada, estão estabelecidos no presente Termo e no contrato a ser firmado entre as partes, conforme os termos e condições descritas nos documentos que integram este procedimento licitatório.
>
> 18.6.2. A **Contratante** poderá, em qualquer momento, **extinguir o contrato**, **total ou parcialmente**, nas seguintes situações:
>
> a) **Por conveniência administrativa**, caso entenda que o contrato não mais oferece vantagem ou interesse para a Administração, conforme o disposto no art. 106, inciso III da Lei nº 14.133/2021, observando-se o prazo e as condições estabelecidas na legislação;
>
> b) **Por falta de créditos orçamentários**, quando a Administração não dispor dos recursos financeiros necessários para a continuidade do contrato, conforme também previsto no mencionado artigo da Lei nº 14.133/2021.
>
> 18.6.3. A rescisão ou extinção do contrato, conforme estabelecido na Lei nº 14.133/2021, será realizada mediante **notificação formal** à **Contratada**, respeitando os prazos e as condições de aviso prévio, quando aplicáveis, conforme estabelecido no **art. 106 da Lei nº 14.133/2021**.
>
> 18.6.4. O contrato poderá ser rescindido pela Contratante a qualquer tempo, no todo ou em parte, por conveniência administrativa, mediante notificação, através de ofício diretamente ou via postal com prova de recebimento, através de parecer fundamentado, assegurado, todavia os direitos adquiridos pela Contratada;
>
> 18.6.5. O inadimplemento de quaisquer das cláusulas e disposições deste instrumento, implicara na sua rescisão ou na sustação do pagamento relativo aos serviços já efetuados, a critério da Contratante, independentemente de qualquer procedimento judicial;
>
> 18.6.6. A inexecução total ou parcial do contrato enseja a sua rescisão, com as consequências contratuais e as previstas em lei ou regulamento.
>
> 18.6.7. Constituem motivo para rescisão de contrato:

I - O não cumprimento de cláusulas contratuais, especificações, projetos ou prazos.

II - O cumprimento irregular de cláusulas contratuais, especificações, projetos e prazos.

III - A lentidão do seu cumprimento, levando a Administração a comprovar a impossibilidade da conclusão do serviço ou do fornecimento, nos prazos estipulados.

IV - O atraso injustificado no início do serviço ou fornecimento.

V - A paralisação do serviço ou do fornecimento, sem justa causa e prévia comunicação à Administração.

(...)

19. DO REAJUSTE E SUPRESSÃO CONTRATUAL

19.1. Ficam aquelas estabelecidas no item 18.5. e seus subitens do Anexo I – Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

20. DO PAGAMENTO

20.1. Conforme estabelecido no item 24.e seus subitens do Anexo I deste Edital - Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

21. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

21.1. A licitante e o contratado que incorram em infrações sujeitam-se às sanções administrativas previstas nos termos dos arts. 155 e 156 da Lei Federal n.° 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 Anexo I deste Edital - Termo de Referência**,** conforme transcrevemos:

(...)

25. SANÇÕES ADMINISTRATIVAS

25.1. Considerando as **INFRAÇÕES E SANÇÕES ADMINISTRATIVAS** devem ser atendidos e preceituado como parâmetros os Art. 155 ao Art. 163 da Lei 14.133/2021 e arts. 184, 185, 186 e 187 Decreto Estadual Nº 28.874 de 25 de janeiro de 2024.

25.2. Sem prejuízo das sanções cominadas no art. 156, I, III e IV, da Lei nº 14.133 de 1º de abril de 2021, pela inexecução total ou parcial do contrato, a Administração poderá, garantida a prévia e ampla defesa, aplicar à Contratada multa de até 10% (dez por cento) sobre a parte do contrato.

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

25.4. Ficará impedido de licitar e de contratar com o Estado de Rondônia e será descredenciado no SICAF, pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, garantido o direito à ampla defesa, o licitante que, convocado dentro do prazo de validade de sua proposta:

I - não assinar o contrato;

II - não entregar a documentação exigida no edital;

III - apresentar documentação falsa;

IV - causar o atraso na execução do objeto;

V - não mantiver a proposta;

VI - falhar na execução do contrato;

VII - fraudar a execução do contrato;

VIII - comportar-se de modo inidôneo;

IX - declarar informações falsas; e

X - cometer fraude fiscal.

25.4.1. As sanções descritas no item 25.3, também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido sem justificativa ou com justificativa recusada pela administração pública.

25.4.2. As sanções serão registradas e publicadas no SICAF e Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual - CAGEFIMP.

25.5. A multa descrita no quadro de infrações, eventualmente imposta à Contratada, será automaticamente descontada da fatura a que fizer jus, acrescida de juros moratórios de 1% (um por cento) ao mês. Caso a contratada não tenha nenhum valor a receber do Estado, ser-lhe-á concedido

o prazo de 05 (cinco) dia úteis, contados de sua intimação, para efetuar o pagamento da multa. Após esse prazo, não sendo efetuado o pagamento, serão deduzidos da garantia. Mantendo-se o insucesso, seus dados serão encaminhados ao órgão competente para que seja inscrita na dívida ativa, podendo, ainda a Administração proceder à cobrança judicial.

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

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

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

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

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

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

8.	Ressarcir o órgão por eventuais danos causados por sua culpa, em qualquer bem/material.	02	0,4% sobre o valor contratado
9.	Cumprir quaisquer dos itens do Edital e seus anexos, mesmo que não previstos nesta tabela de multas, após reincidência formalmente notificada pela FISCALIZAÇÃO;	03	0,8% sobre o valor mensal do contrato
10.	Refazer serviço não aceito pela FISCALIZAÇÃO, nos prazos estabelecidos no contrato ou determinado pela FISCALIZAÇÃO; por unidade de tempo definida para determinar o atraso	03	0,8% sobre o valor mensal do contrato
11.	Cumprir determinação formal ou instrução complementar da FISCALIZAÇÃO.	03	0,8% sobre o valor mensal do contrato
12.	Iniciar execução de serviço nos prazos estabelecidos pela FISCALIZAÇÃO, observados os limites mínimos estabelecidos por este Contrato; por serviço.	02	0,4% sobre o valor mensal do contrato
13.	Manter a documentação de habilitação atualizada;	01	0,2% sobre o valor mensal do contrato

Nota: Incidente sobre o valor da parcela do contrato.

25.11. As sanções aqui previstas poderão ser aplicadas concomitantemente, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 05 (cinco) dias úteis.

25.12. Após 30 (trinta) dias da falta de execução do objeto, será considerada inexecução total do contrato, 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. As sanções previstas não poderão ser relevadas, salvo ficar comprovada a ocorrência de situações que se enquadrem no conceito jurídico de força maior ou casos fortuitos, devidos e formalmente justificados e comprovados, e sempre a critério da autoridade competente, conforme prejuízo auferido.

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

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

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

a) Tenham sofrido condenações definitivas por praticarem, por meio dolosos, fraude fiscal no recolhimento de tributos;

b) Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

c) Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

25.18. Sem prejuízo das sanções cominadas no Decreto nº 28874, de 25 de janeiro de 2024, conforme se segue:

[...]

Art. 185. A apuração de infração administrativa que enseja a imposição de advertência ou multa, isoladas ou cumulativamente, se dará mediante rito simplificado, observadas as garantias do administrado.

Parágrafo único. 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.

[...]

21.2. 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.

22. DAS OBRIGAÇÕES DA CONTRATADA

22.1. Conforme estabelecido no item 20.1. e seus subitens do Anexo I deste Edital - Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

23. DAS OBRIGAÇÕES DA CONTRATANTE

23.1. Conforme estabelecido no item 20.2. e seus subitens do Anexo I deste Edital - Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

24. DA DOTAÇÃO ORÇAMENTÁRIA

24.1. Os recursos financeiros necessários para acobertar as despesas decorrentes da contratação, estão consignados no orçamento da **Unidade Gestora:** Secretaria de Estado da Saúde de Rondônia – SESAU/RO, conforme estabelecido no item 12. do Anexo I deste Edital - Termo de Referência, conforme transcrevemos:

(...)

12.1. Conforme Informação nº 3785/2024/SESAU-NPPS (0052252474), segue abaixo a dotação orçamentária:

DESCRIÇÃO DA DESPESA			
OBJETO PROCESSUAL: Contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, visando atender às necessidades da Secretaria de Estado da Saúde de Rondônia, por um período de 01 (um) ano, podendo ser prorrogado, conforme a Lei Federal nº 14.133 de 1° de abril de 2021.			
Resposta ao:	Despacho (0052208255)		
PROGRAMA DE TRABALHO	**UNIDADE ATENDIDA**	**FONTE DE RECURSO**	**NATUREZA DA DESPESA**
17.012.10.126.1015.2064 - PROMOVER A GESTÃO DE T.I	Secretaria de Saúde	1.500.0.01002 - Recursos não vinculados de impostos - Saúde 2.500.0.01002 - Recursos não vinculados de impostos do exercício anterior - Saúde	3.3.90.39 - Outros Serviços de Terceiros - PJ 3.3.90.40 - Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica

12.2. Ressalta-se ainda que a aludida informação é exclusivamente para indicação da programação, cabendo a anuência de execução da despesa ao ordenador, desde que tenha, no momento dessa execução, recursos orçamentários e financeiros suficientes para o atendimento.

12.3. **Plano de Contratação Anual (PCA)**

12.3.1. conforme o Parecer nº 28/2026/SESAU-DIREX (70656134):

> **3. CONCLUSÃO E PARECER**
>
> Com base na análise dos autos e considerando o objeto em referência, a unidade demandante solicita autorização para realizar despesas não previstas na Programação Anual de Saúde de 2026, no valor estimado de R$ 7.749.301,17 (sete milhões, setecentos e quarenta e nove mil trezentos e um reais e dezessete centavos), conforme o Documento de Oficialização de Demanda nº 31/2024/SESAU-CTI, (0054733868), **conclui-se que é justificada.**
>
> Considera-se que a organizações estejam preparadas para enfrentar e responder a esses incidentes de forma adequada, protegendo tanto os dados de sua propriedade quanto aqueles que estão sob sua custódia.
>
> Considera-se que é fundamental investir em estratégias robustas de segurança da

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

Pelo exposto**, AUTORIZO** o prossequimento dos autos para realizar despesas não prevista na Programção Anual de 2026, conforme DESPACHO/SESAU-CITI (70618017).

(...)

25. DO SISTEMA DE REGISTRO DE PREÇO

25.1. Homologada a licitação pela Autoridade Competente, a Ata de Registro de Preços será publicada na imprensa Oficial, momento em que terá efeito de compromisso nas condições ofertadas e pactuadas na proposta apresentada à licitação.

25.2. O limites global e individual para adesões a este Sistema de Registro de Preços será de, respectivamente, de duas vezes e 50% do quantitativo.

25.3. O quantitativo mínimo para cada ordem de fornecimento a ser exarada pelos órgão gerenciador, participantes e não participantes será de 50%.

25.4. A validade desta ata de registro de preços será de 1(um) ano, contados a partir da publicação no Diário Oficial do Estado, e poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso, mediante pesquisa de mercado que leve em consideração os parâmetros fixados no art. 51 do Decreto Estadual n° 28.874/2024.

25.5. Os prazos de vigência dos eventuais contratos decorrentes do registro observarão os limites previstos no Capítulo V do Título III da Lei Federal n° 14.133/2021.

25.6. A existência de preços registrados não obriga a Administração a firmar as contratações que deles poderão advir, facultando-se a realização de licitação específica para a aquisição pretendida, sendo assegurada ao beneficiário do registro a preferência de fornecimento em igualdade de condições.

25.7. A ata de registro de preços, os ajustes dela decorrentes, suas alterações e rescisões obedecerão o Decreto Estadual n° 28.874/2024, a Lei Federal n° 14.133/2021, e as demais normas complementares e disposições desta Ata e do Edital que a precedeu, aplicáveis à execução e especialmente aos casos omissos.

25.8. Fica a Detentora ciente que a publicidade da ata de registro de preços na imprensa oficial terá efeito de compromisso nas condições ofertadas e pactuadas na proposta apresentada à licitação.

25.9. Nos termos do Decreto Estadual n° 28.874/2024, a Ata de Registro de Preços, durante a sua vigência, poderá ser utilizada por qualquer órgão ou entidade da Administração Pública que não tenha participado do certame licitatório, mediante anuência do órgão gerenciador.

25.10. - É vedada à participação do órgão ou entidade em mais de uma ata de registro de preços com o mesmo objeto no prazo de validade daquela de que já tiver participado, salvo na ocorrência de ata que tenha registrado quantitativo inferior ao máximo previsto no edital;

25.11. Por ocasião da publicação da ata de registro de preços, será verificado no SICAF e em outros meios se a adjudicatária mantém as condições de habilitação.

25.12. Após a homologação da licitação, deverão ser observadas as seguintes condições para formalização da ata de registro de preços:

25.12.1. Serão registrados na ata os preços e os quantitativos do adjudicatário, devendo ser observada a possibilidade de o licitante oferecer ou não proposta em quantitativo inferior ao máximo previsto no edital e se obrigar nos limites dela;

25.12.2. Será incluído na ata, na forma de anexo, o registro dos licitantes ou dos fornecedores que:

25.12.2.1. Aceitarem cotar os bens ou serviços com preços iguais aos do licitante vencedor

na sequência de classificação da licitação; e

25.12.2.2. Mantiverem sua proposta original.

25.13. Para o cadastro reserva disposto no item **12.2** o (a) Pregoeiro (a) realizará as convocações no chat de mensagens durante o transcurso da sessão pública.

25.14. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou dos fornecedores registrados na ata.

25.15. O registro a que se refere o item **12.2** tem por objetivo a formação de cadastro de reserva para o caso de impossibilidade de atendimento pelo detentor da ata.

25.16. A habilitação dos fornecedores que comporão o cadastro de reserva será conferida quando houver necessidade de contratação de fornecedor remanescente.

25.17. O preço registrado poderá ser revisto em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução tal como pactuado, observada a instrução processual respectiva, cabendo ao órgão gerenciador da ata promover as necessárias negociações junto aos fornecedores.

25.17.1. A alteração dos preços registrados não altera automaticamente os preços dos contratos decorrentes do Sistema de Registro de Preços, cuja revisão deverá ser feita pelo órgão contratante, observadas as disposições legais incidentes sobre os contratos.

25.18. Quando o preço inicialmente registrado, por motivo superveniente, tornar-se superior ao preço praticado no mercado o órgão gerenciador deverá convocar o fornecedor visando a negociação para redução de preços e sua adequação ao praticado pelo mercado.

25.18.1 Os fornecedores que não aceitarem reduzir seus preços aos valores praticados pelo mercado serão liberados dos compromissos assumidos, sem aplicação de penalidades administrativas.

25.18.2. A redução do preço registrado será comunicada pelo órgão gerenciador aos órgãos que tiverem formalizado contratos com fundamento no respectivo registro, para que avaliem a necessidade de efetuar a revisão dos preços contratados.

25.18.3. A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação obtida originalmente na licitação.

26. CANCELAMENTO DO REGISTRO DO LICITANTE VENCEDOR E DOS PREÇOS REGISTRADOS

26.1. O registro de preço de fornecedor ou prestador de serviço será cancelado quando:

26.1.1. For atestado o descumprimento das condições previstas na ata de registro de preços;

26.1.2. O contrato ou documento equivalente não for firmado no prazo estabelecido pela Administração;

26.1.3. O fornecedor ou prestador de serviço registrado não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior aos preços praticados no mercado;

26.1.4. Estiverem presentes razões de interesse público; e

26.1.5. Restar caracterizada a impossibilidade de concretização do objeto registrado em razão de caso fortuito ou força maior.

26.2. O cancelamento de registro, nas hipóteses previstas, assegurados o contraditório e a ampla defesa, será formalizado por despacho da autoridade competente do órgão gerenciador, após manifestação da fiscalização contratual.

26.3. O disposto no § 1° do art. 136 do Decreto 28.874/2024 poderá ser observado nas hipóteses de cancelamento do registro, sem prejuízo da prévia negociação para obtenção de condições mais vantajosas para a Administração.

27. DAS DISPOSIÇÕES GERAIS

27.1. 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.

27.2. Será divulgada ata da sessão pública nos sistemas eletrônicos: https://www.gov.br/compras/pt-br e no site https://rondonia.ro.gov.br/supel.

27.3. 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.

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

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

27.6. 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.

27.7. 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.

27.8. 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.

27.9. 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.

27.10. 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.

27.11. 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/ https://www.gov.br/compras/pt-br

27.12. 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.

27.13. 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.

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

28. DOS ANEXOS

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

ANEXO I - Termo de Referência Id. (70923055);

ANEXO II - Matriz de Risco Id. (0051893000);

ANEXO III- Mapa de Risco Id. (0051897532);

ANEXO IV - Manual de Gestão de Contratos Id. (0053828787);

ANEXO V - SAMS Id. (71034668);

ANEXO VI – Relatório de Preços Id. (68244109);

ANEXO VII - Minuta da Ata de Registro de Preços e da Adesão à ata Id. (72406873).

Porto Velho-RO, *data e horário do sistema*.

GABRIEL ALVES DA SILVA GAMA
Matrícula nº ******238
Pregoeiro da Comissão de Tecnologia - COTEC
Portaria nº 50 de 25 de fevereiro de 2026
Superintendência Estadual de Compras e Licitações - SUPEL|RO

Documento assinado eletronicamente por **Gabriel Alves Da Silva Gama**, **Pregoeiro(a)**, em 25/05/2026, às 12:22, 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 **72609716** e o código CRC **85081B87**.

Referência: Caso responda este Instrumento Convocatório, indicar expressamente o Processo nº 0036.028242/2024-36

SEI nº 72609716

GOVERNO DO ESTADO DE RONDÔNIA
Secretaria de Estado da Saúde - SESAU
NÚCLEO DE SERVIÇOS CONTINUADOS - SESAU-NSC

TERMO DE REFERÊNCIA

1. IDENTIFICAÇÃO

1.1. **Unidade Orçamentária:** Secretaria de Estado da Saúde de Rondônia – SESAU/RO.

1.2. **Requisitante:** SESAU-CTI - Coordenadoria de Tecnologia da Informação.

2. DA INTRODUÇÃO E BASE LEGAL

2.1. O presente Termo de Referência foi elaborado em atendimento ao disposto no art. 6º, XXIII da Lei nº 14.133, de 2021. O fundamento legal adotado para a presente contratação é Pregão Eletrônico - Registro de Preço, conforme artigo 28, inciso I da **Lei Federal nº 14.133/2021**, adotado para a presente contratação conformidade com regulamento das contratações públicas no âmbito da Administração Pública direta, autárquica e fundacional do Estado de Rondônia aplicado no **Decreto Estadual n° 28.874/2024.**

2.2. Dos Princípios a serem observados: conforme art. 5º da Lei 14.133/2021, eis os princípios a serem observados na sua aplicação:

> Art. 5º Na aplicação desta Lei, serão observados os princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, do interesse público, da probidade administrativa, da igualdade, do planejamento, da transparência, da eficácia, da segregação de funções, da motivação, da vinculação ao edital, do julgamento objetivo, da segurança jurídica, da razoabilidade, da competitividade, da proporcionalidade, da celeridade, da economicidade e do desenvolvimento nacional sustentável, assim como as disposições do Decreto-Lei nº 4.657, de 4 de setembro de 1942 (Lei de Introdução às Normas do Direito Brasileiro).

2.3. Modalidade de Licitação: **Pregão, na forma eletrônica**, conforme art. 6º, inc. XLI, da Lei Federal nº 14.133/2021.

2.4. Critério de Julgamento: **MENOR VALOR GLOBAL** , conforme art. 6º, inc. XLI, da Lei Federal nº 14.133/2021.

2.5. Modo de Disputa: **ABERTO**, conforme art. 56, inc. I, da Lei Federal n° 14.133/2021.

3. DEFINIÇÃO DO OBJETO

3.1. **Objeto**

3.1.1. Registro de Preços para contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da Secretaria de Estado da Saúde - SESAU/RO, por um período de 01 (um) ano, podendo ser prorrogado, conforme a Lei Federal nº 14.133 de 1° de abril de 2021.

3.2. **Descrição Detalhada do Objeto**

GRUPO ÚNICO	ITEM	CATMAT	OBJETO	UNIDADE DE MEDIDA	QUANTIDADE

GRUPO ÚNICO	ITEM	CATMAT	OBJETO	UNIDADE DE MEDIDA	QUANTIDADE
01	1	27499	Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes	Por Endpoint	2150
	2	27499	Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes	Por Servidor	139
	3	27499	Solução de segurança avançada para mitigação de ameaças na rede	Por Throughput de dados	2
	4	27499	Solução de prevenção de intrusão de próxima geração (NGIPS)	Por Throughput de dados	4
	5	27432	Serviço de suporte pro ativo, corretivo e para resposta a incidentes	Por Solução	4
	6	3840	Serviço de implantação	Por Solução	4
	7	3840	Serviço de capacitação e repasse de conhecimento	40 Horas	2

3.2.1. OBS.: A descrição completa dos objetos está presente no item **8** deste Termo de Referência.

3.3. **Da Memória de Cálculo**

3.3.1. Conforme relatório Relatório Parque Computacional SESAU (0049992349), extraído do **sistema GLPI até 20/06/2024** a Secretaria de Estado da Saúde, tem 1920 computadores, considerando que estão com processos para adição e substituição do computadores deixando uma margem de crescimento do parque solicitamos 2150 unidades para os desktops levando em consideração que cada computador deve ter uma licença ativa e válida.

3.3.2. Considerando que estamos com dois processos de aquisição de novos computadores para renovação do parque tecnológico 0036.006222/2024-12 - 38 Computadores e 0036.051061/2023-22- 1.470 Computadores.

3.3.3. Considerando a instalação do antivírus apenas nos equipamentos novos, para evitar maior lentidão nos computadores antigos, chegamos ao seguinte cálculo:

- 400 Computadores compatíveis atualmente

- 1.508 Processos em andamento

3.3.4. Totalizando 1.908 licenças necessárias para uso imediato, com uma reserva adicional de 242 licenças para futuras expansões.

Item	Quantidade
Computadores no Parque(atual)	1920
Licenças (item 1)	2150
0036.006222/2024-12 – Aquisição	38
0036.051061/2023-22 - Aquisição	1470

- Atualmente dispomos de 47 servidores que rodam as seguintes aplicações:

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)			
Sistema	**Unidade demandante**	**Função**	**Amplitude de atuação**
GERADOR SENHA	POC-CGAF-BARCO	Gerar senhas para Gerenciar a Fila de Atendimento de Pacientes	POC - Policlinica Osvaldo Cruz CGAF - Gerência Farmaceutica
PAINEL CHAMADOR	POC-CGAF-BARCO	Realizar a Chamada da Senha no Painel em Voz, chamando o nome Social do Paciente, juntamente com o número da Senha e Consultório Médico.	POC - Policlinica Osvaldo Cruz CGAF - Gerência Farmaceutica
SAÚDE POC	POC	Realizar a Gestão de Atendimento Administrativo, Atendimento Médico, Prontuário Eletrônico, Configurações de Painéis de Chamada, Configurações de Áreas de Atendimento.	POC - Policlinica Osvaldo Cruz

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)			
EPEP POC	POC	Sistema para Estatísticas de Atendimentos da POC, Retirar Relatórios Estratégicos de Atendimento, assim como Dashboard em Tempo Real do Cenário da POC	POC - Policlinica Osvaldo Cruz
ADMINISTRATIVO CGAF	CGAF	Realizar a Gestão de Agendamentos de Pacientes para retirar Medicamentos na Farmácia	CGAF - Gerência Farmaceutica

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)			
E-CONSUMO	CAP	Realizar a Gestão de Estoque de Materiais de Consumo	CAP - Coordenadoria de Almoxarifado e Patrimonio HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De Buritis JP II - Hospital e Pronto Socorro João Paulo II Cemetron - Centro de Medicina Tropical de Rondônia HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião AMI - Assistencia Médica Intensiva HCAMP - Hospital de Campanha de Rondônia HRE - Hospital Regional de Extrema HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De São Francisco do Guaporé Hospital Regional De Buritis

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)			
E-CONSUMO GASES	Unidades Hospitalares	Realizar a Gestão de Estoque e Solicitação de Medicinais das Unidades Hospitalares	CAP - Coordenadoria de Almoxarifado e Patrimonio HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De Buritis JP II - Hospital e Pronto Socorro João Paulo II Cemetron - Centro de Medicina Tropical de Rondônia HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião Ami - Assistencia Médica Intensiva HCAMP - Hospital de Campanha de Rondônia HRE - Hospital Regional de Extrema HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De São Francisco do Guaporé Hospital Regional De Buritis

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)			
HOSPUB	Unidades Hospitalares	Realizar a Gestão de Prontuário Eletrônico	HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião JP II - Hospital e Pronto Socorro João Paulo II Cemetron - Centro de Medicina Tropical de Rondônia Ami - Assistencia Médica Intensiva HCAMP - Hospital de Campanha de Rondônia HEURO - Hospital de Urgência e Emergência Regional de Cacoal HRC - Hospital Regional de Cacoal Hospital Regional De São Francisco do Guaporé Hospital Regional de Buritis CAFI NMJ - Nucleo de Mandados Judiciais CDA - Centro de Diálise de Ariquemes POC - Policlinica Osvaldo Cruz
E-LEITOS	Regulação	Painel Dashboard da Taxa de Ocupação dos Leitos de Acordo com as Informações do Hospub, assim como Realizar Pareceres para Solicitação de Leitos para as Unidades.	Todos os leitos da SESAU

Tabela 8 - Sistemas Desenvolvidos e/ou Mantidos pela SESAU (Abrangência)			
E-REFEIÇÃO	Unidades Hospitalares	Realizar a Gestão e controle das Refeições nas Unidades Hospitalares dos servidores que estão de Plantão.	Cemetron - Centro de Medicina Tropical de Rondônia HB - Hospital de Base Ary Pinheiro HICD - Hospital Infantil Cosme Damião JP II - Hospital e Pronto Socorro João Paulo II HRC - Hospital Regional de Cacoal HEURO - Hospital de Urgência e Emergência Regional de Cacoal Cemetron - Centro de Medicina Tropical de Rondônia Hospital Regional de Buritis
NACSUS	NAC-NMJ	Auxiliar e ajudar os processos internos do NAC - Núcleo de Apoio e Conciliação, evitando que os pacientes entrem com uma Ação Judicial contra o Estado de Rondônia.	Núcleo de Apoio a Conciliação
PROCESSO SELETIVO	RH	Realizar o Cadastro dos Candidatos as vagas em Aberto no Processo Seletivo da SESAU, assim como, definir os critérios de Pontuação e deferir ou indeferir algum certificado ou experiência profissional.	RH

3.3.5. Considerando o contrato com a fábrica de software e a implantação do sistema AGHuX em todo o estado, é necessário ressaltar que cada unidade de saúde requer três servidores para o pleno funcionamento do AGHuX. Além disso, após a implantação, o sistema HOSPUB precisará permanecer hospedado por

aproximadamente três anos para fins de consulta.

3.3.6. Servidores Atual: 47

3.3.7. AGHuX: 60

3.3.8. Margem de 30% Novos Sistemas: 32

3.3.9. **Total: 139 Licenças ITEM (2)**

AGHuX	
ID	**Unidade de Saúde**
1	Hospital Infantil Cosme Damião:
2	Pronto Socorro João Paulo II:
3	Policlínica Oswaldo Cruz:
4	Hospital De Base Dr. Ary Pinheiro:
5	Laboratório Central de Saúde Pública de Rondônia – LACEN:
6	Laboratório Estadual de Patologia e Análises Clínicas de Rondônia – LEPAC:
7	Centro de Atenção Psicossocial – CAPS:
8	Assistência Médica Intensiva – AMI:
9	Serviço de Assistência Multidisciplinar em Domicílio – SAMD:
10	Centro de Medicina Tropical De Rondônia – CEMETRON:
11	Hospital Regional de Extrema:
12	Hospital Regional de São Francisco do Guaporé:
13	Hospital de Urgência e Emergência de Cacoal – HEURO:
14	Hospital Regional de Cacoal:
15	Centro de Diálise de Ariquemes
16	Hospital Regional de Buritis:
17	Hospital de Retaguarda
18	NMJ - Nucleo de Mandados Judiciais
19	CAF1
20	CAF2

3.4. **Da Classificação do Objeto**

3.4.1. O objeto pleiteado nos autos não envolve técnicas desconhecidas no mercado ou requerem inovação tecnológica para a sua execução, tratando-se assim de bem comum, pois é possível estabelecer, por intermédio de especificações utilizadas no mercado, padrões de qualidade e desempenho característicos ao objeto, de modo que é possível a decisão entre os materiais ofertados pelos participantes com base no menor preço.

3.4.2. A classificação como comum não se confunde com a complexidade do objeto. O que deve ser verificada é a possibilidade de seus padrões de desempenho e qualidade serem definidos objetivamente em especificações usualmente adotadas no mercado, o que fica evidente no presente instrumento convocatório.

3.4.3. Corroborando com esse entendimento, transcrevemos o relatado pelo Professor Marçal Justen Filho em seu livro Pregão - Comentários à Legislação do Pregão Comum e Eletrônico:

> "Ou seja, há casos em que a Administração necessita de bens que estão disponíveis no mercado, configurados em termos mais ou menos variáveis. São hipóteses em que é público o domínio das técnicas para a produção do objeto e seu fornecimento ao adquirente (inclusive à Administração), de tal modo que não existe dificuldade em localizar um universo de fornecedores em condições de satisfazer plenamente o interesse público. Em outros casos, o objeto deverá ser produzido sob encomenda ou adequado às configurações de um caso concreto.
> (...)

3.4.4. Entende-se que a contratação enquadra-se em aquisição de bens comuns, consideram-se bens e serviços comuns, aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos, por meio de especificações usuais no mercado e conforme expressa no Parecer n° 20/CONSU/CMA/PRF3/PGF/AGU nº 432/2014:

> *"Bens e serviços comuns são produtos cuja a escolha pode ser feita tão somente com base nos preços ofertados, haja vista serem comparáveis entre si e não necessitarem de avaliação minuciosa. São encontráveis facilmente no mercado. São exemplos de bens comuns: caneta, lápis, borrachas, papéis, mesa, cadeiras, veículos, aparelho de ar refrigerado, etc e de execução de serviços: confecção de chaves, manutenção de veículos, colocação de piso, troca de azulejos, pintura de parede, etc. O bem ou serviço será comum quando for possível estabelecer para efeito de julgamento das propostas, mediante especificações utilizadas no mercado, padrões de qualidade e desempenho peculiares ao objeto".*

3.4.5. Para concluir, numa tentativa de definição, poderia dizer-se que bem ou serviço comum é aquele que apresenta sob identidade e características padronizadas e que se encontra disponível, a qualquer tempo, num mercado próprio.

3.4.6. Diante do exposto, e considerando que a Lei n° 14.133/21 define em seu Art. 6º Inciso XIII - "bens e serviços comuns: aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado", define-se que o objeto da presente contratação é comum.

4. FUNDAMENTAÇÃO DA NECESSIDADE DA CONTRATAÇÃO (JUSTIFICATIVA)

4.1. **DA NECESSIDADE DA COORDENADORIA DE INOVAÇÃO E TECNOLOGIA DA INFORMAÇÃO - SESAU - CITI:** A justificativa quanto a necessidade da contratação está inserida no Documento de Oficialização de Demanda nº 31/2024/SESAU-CTI (0054733868), conforme exposto abaixo:

4.1.1. A Secretaria de Estado da Saúde foi instituída pelo Decreto-Lei nº 01 de 31 de Dezembro de 1981. Em 13 de Julho de 1992, pela Lei complementar nº 59, foi criado o Fundo Estadual de Saúde – FES, como instrumento de suporte financeiro para o desenvolvimento do Sistema Único de Saúde de Rondônia – SUS/RO, atualizado pela Lei Complementar nº 134 de 05 de Junho de 1995, e em 20 de Dezembro de 2017 a Secretaria de Estado da Saúde foi reestruturada pela Lei Complementar nº 965. A finalidade e o compromisso constitucional da Sesau é o desenvolvimento das ações de atenção à saúde, voltados para a elaboração e execução da Política de Saúde do Estado, na promoção, desenvolvimento e assistência técnica aos municípios na implantação, operação e avaliação dos serviços básicos de saúde, nas ações de vigilância epidemiológica, fiscalização e controle das condições sanitárias de higiene, saneamento e trabalho. Os serviços de saúde ofertados pela Sesau aos cidadãos estão organizados com base na macro e microrregiões do Estado, divididos em dois níveis estratégicos de gestão da Saúde Pública: o nível secundário e o nível terciário. O nível secundário consiste no atendimento ambulatorial, hospitalar e outras unidades de atendimento especializado, inclusive de urgência e emergência na atenção de média complexidade. No nível terciário estão os hospitais de grande porte, os exames de diagnóstico, a tecnologia e as Especialidades médicas e profissionais que dão suporte ao atendimento de alta complexidade, que não devem ser tratados em nível primário e secundário pelo grau de complexidade.

4.2. A segurança da rede da Secretaria de Estado da Saúde - SESAU depende da utilização de recursos de segurança cibernética, que incluem várias camadas de proteção para monitorar o comportamento dos usuários, estações de trabalho e caixas postais com o objetivo de proteger o ambiente da Secretaria contra ameaças básicas e avançadas.

4.3. É fundamental tratar a informação como um recurso estratégico e econômico, devido à crescente valorização dos dados pessoais e da informação como ativos de gestão do Estado. Além disso, considerando as transações bilaterais cada vez mais frequentes que contam com o suporte de TI. O uso inadequado desses recursos oferece um alto risco de impactos negativos e pode resultar em consequências indesejadas, como prejuízo financeiro, problemas operacionais, danos à imagem do órgão ou governo, vazamento de informações e dados pessoais, e até mesmo sequestro de dados.

4.4. A Secretaria de Estado da Saúde, possui um parque computacional para atendimento aos usuários, com cerca de 3.000 usuários ativos na rede, 2.000 estações de trabalho, além de caixas postais e outros recursos, de acordo com o levantamento realizado no ambiente de infraestrutura de TI. A aferição do comportamento das

estações de usuários e caixas postais tem como objetivo detectar, bloquear, investigar e responder a incidentes de segurança da informação que possam ocorrer na rede da Secretaria.

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

4.6. De acordo com estatísticas recentes do CERT.br, que recebe notificações de CSIRTs, administradores de redes e usuários de Internet, tem havido um aumento significativo nos ataques e incidentes de segurança ao longo dos anos. Especificamente, em 2022, foram notificados 481.652 incidentes ao CERT.br, um número alarmante. **No entanto, é ainda mais preocupante que, apenas no primeiro semestre de 2023, esse número já tenha atingido 333.905 notificações, representando um aumento expressivo em relação ao período anterior.**

4.7. Esses dados evidenciam uma tendência preocupante e urgente, que exige a adoção de medidas cada vez mais eficientes por parte das organizações. A segurança das informações e a proteção de dados pessoais tornaram-se questões críticas e de extrema importância, tanto para empresas quanto para indivíduos. É necessário que as organizações estejam preparadas para enfrentar e responder a esses incidentes de forma adequada, protegendo tanto os dados de sua propriedade quanto aqueles que estão sob sua custódia.

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

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

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

4.11. Dessa forma, a contratação de recursos adicionais para cumprir com a **Lei Geral de Proteção de Dados -LGPD**- é uma medida indispensável para garantir a proteção e preservar a privacidade dos usuários da Secretaria de Estado da Saúde. Ao implementar as medidas de proteção adequadas, a secretaria estará em conformidade com a legislação vigente, assegurando a confidencialidade, integridade e disponibilidade dos dados pessoais sob sua responsabilidade.

4.12. Segue a descrição resumida e justificativa da funcionalidade de cada solução escolhida.

4.12.1. **Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes (Item 1).**

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

4.12.2. **Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes (Item 2).**

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

4.12.3. **Solução de segurança avançada para mitigação de ameaças na rede (Item 3).**

4.12.3.1. Solução de segurança avançada para mitigação de ameaças na rede é uma ferramenta de segurança cibernética que oferece uma série de benefícios para redes empresariais. Uma de suas principais vantagens é a detecção avançada de ameaças, sendo capaz de identificar e analisar ameaças sofisticadas que muitas vezes conseguem passar despercebidas por soluções de segurança convencionais proporciona uma visibilidade detalhada da rede, permitindo uma análise minuciosa do tráfego e das atividades em curso. Essa análise detalhada ajuda na identificação de comportamentos suspeitos ou anomalias que podem indicar potenciais ameaças à segurança da rede.

4.12.4. **Solução de prevenção de intrusão de próxima geração (NGIPS) - (Item 4).**

4.12.4.1. Um Sistema de Prevenção de Intrusões de Próxima Geração (NGIPS) oferece uma série de vantagens cruciais para a segurança cibernética de uma organização. Em primeiro lugar, ele é capaz de fornecer uma camada avançada de defesa contra ameaças cibernéticas, identificando e bloqueando ataques em tempo real. Essa capacidade de detecção e resposta rápida a ameaças permite proteger a rede contra malware, ataques de negação de serviço (DDoS), exploração de vulnerabilidades e outras formas de intrusões maliciosas. Além disso, o NGIPS proporciona visibilidade aprofundada da atividade da rede, permitindo uma análise detalhada do tráfego em tempo real. Essa análise contínua e em profundidade ajuda na identificação precoce de atividades suspeitas ou anomalias que possam indicar um possível ataque, permitindo uma resposta rápida e eficaz.

4.12.5. **Serviço de suporte pro ativo, corretivo e para resposta a incidentes (Item 05).**

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

4.12.6. **Serviço de implantação (Item 06).**

4.12.6.1. Oferece suporte especializado para implementar soluções de segurança digital em ambientes corporativos. Ele inclui desde a configuração inicial até a integração completa das ferramentas de segurança, garantindo uma instalação eficiente e funcional.

4.12.7. **Serviço de capacitação e repasse de conhecimento (Item 07).**

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

5. ALINHAMENTO COM AS NECESSIDADES TECNOLÓGICAS

5.1. A solução de segurança proposta, para proteção de e-mail, endpoint e redes, tem como deverá contribuir para garantir um nível adequado de disponibilidade, autenticidade e confiabilidade das informações produzidas e armazenadas nos meios tecnológicos da SESAU.

5.2. A solução deve suportar as seguintes funcionalidades:

5.3. Reputação de Arquivos: tanto para arquivos locais quanto para acesso web, a solução deve fornecer mecanismos para avaliar a reputação dos arquivos, identificando possíveis ameaças e evitando que arquivos maliciosos sejam abertos ou executados.

5.4. Redução de riscos: a solução deve fornecer acesso imediato à percepção e ao controle de segurança, permitindo uma resposta rápida a incidentes e minimizando os riscos associados a ameaças em potencial.

5.5. Aprendizado de Máquinas (Machine Learning) e Análise Comportamental (Behavioral Analysis): utilizando técnicas de aprendizado de máquinas e análise comportamental, a solução deve ser capaz de identificar comportamentos suspeitos e atividades maliciosas, fornecendo uma camada adicional de proteção contra ameaças desconhecidas.

5.6. Mitigação da Exploração de Memória (Memory Exploit Mitigation): a solução deve incluir mecanismos de mitigação de ataques que explorem vulnerabilidades de memória, protegendo contra técnicas como injeção de código malicioso e estouro de buffer.

5.7. Minimização da complexidade: a solução deve criar uma estrutura de gerenciamento centralizada e integrada, facilitando o gerenciamento de segurança e proporcionando uma defesa unificada. Além disso, deve oferecer visibilidade aos clientes e serviços monitorados, permitindo uma visão abrangente da postura de segurança da SESAU.

5.8. Gerenciamento de patches e scanning de vulnerabilidades: a solução deve possibilitar o gerenciamento centralizado de patches de segurança, permitindo a detecção de vulnerabilidades e a aplicação de

correções de forma eficiente e simplificada.

5.9. Minimização do impacto de ameaças: a solução deve permitir respostas automáticas a incidentes, ganhando tempo na mitigação de ameaças e reduzindo o impacto causado por ataques.

5.10. A implementação dessa solução tecnológica deverá atender as necessidades de segurança da SESAU, proporcionando uma proteção abrangente e eficaz contra ameaças cibernéticas, garantindo a integridade e confidencialidade das informações e fortalecendo a postura de segurança da organização.

6. DA JUSTIFICATIVA PARA O PARCELAMENTO (OU NÃO) NA SOLUÇÃO

6.1. O parcelamento da solução é a regra, devendo a licitação ser realizada por item sempre que o objeto for divisível, desde que se verifique não haver prejuízo para o conjunto da solução ou perda de economia de escala, visando propiciar a ampla participação de licitantes.

6.2. Conforme Justificativa apresentada pela Unidade, id. SEI 0049992803, a contratação de uma única empresa para fornecer e implementar todas as soluções e serviços de segurança mencionados oferece diversos benefícios e vantagens estratégicas para a organização. Abaixo estão as principais razões que justificam essa abordagem:

6.2.1. **Integração e Compatibilidade:**

6.2.1.1. Coerência Tecnológica: Uma única empresa pode garantir que todas as soluções (proteção de endpoints, servidores, segurança de rede, NGIPS) sejam tecnicamente compatíveis e se integrem perfeitamente, evitando problemas de interoperabilidade.

6.2.1.2. Plataforma Unificada: Uma abordagem unificada facilita a administração e o monitoramento centralizado das soluções de segurança, reduzindo a complexidade operacional.

6.2.2. **Eficiência Operacional**

6.2.2.1. Simplificação de Gestão: Gerenciar um único fornecedor simplifica os processos administrativos e operacionais, reduzindo a sobrecarga associada à coordenação de múltiplos fornecedores.

6.2.2.2. Facilidade de Comunicação: Comunicação direta e simplificada com um único ponto de contato para todas as questões relacionadas às soluções e serviços de segurança.

6.2.3. **Responsabilidade e Accountability**

6.2.3.1. Responsabilidade Centralizada: Um único fornecedor é responsável pela entrega e performance de todas as soluções e serviços, eliminando disputas de responsabilidade entre diferentes fornecedores em caso de falhas ou incidentes.

6.2.3.2. SLAs Consistentes: Acordos de Nível de Serviço (SLAs) uniformes e consistentes para todos os serviços, garantindo padrões elevados de desempenho e qualidade.

6.2.4. **Economia de Escala**

6.2.4.1. Custos Reduzidos: A contratação em lote único pode resultar em descontos e melhores condições comerciais devido ao volume de serviços contratados.

6.2.4.2. Eficiência de Recursos: Melhor alocação e uso de recursos financeiros e humanos, maximizando o retorno sobre o investimento em segurança cibernética.

6.2.5. **Segurança Aprimorada**

6.2.5.1. Defesa em Camadas Integrada: Uma única empresa pode coordenar melhor as várias camadas de defesa (endpoints, servidores, rede, prevenção de intrusões), criando uma estratégia de segurança mais robusta e coesa.

6.2.5.2. Resposta Rápida a Incidentes: Maior agilidade na resposta a incidentes, uma vez que todas as soluções e serviços estão sob a gestão de um único fornecedor, permitindo uma resposta coordenada e eficaz.

6.2.6. **Consistência no Suporte e Treinamento**

6.2.6.1. Suporte Uniforme: Serviço de suporte proativo, corretivo e de resposta a incidentes fornecido de maneira uniforme, garantindo a mesma qualidade e abordagem em todas as áreas de segurança.

6.2.6.2. Treinamento Coeso: Programas de capacitação e repasse de conhecimento oferecidos pelo mesmo fornecedor garantem consistência na abordagem e no conteúdo, melhorando a eficiência do treinamento da equipe interna.

6.2.7. **Facilidade na Implantação e Atualização**

6.2.7.1. Implantação Integrada: A implementação de todas as soluções por uma única empresa facilita a coordenação das atividades, minimizando o tempo de inatividade e interrupções nos serviços.

6.2.7.2. Atualizações Coordenadas: Atualizações e patches podem ser gerenciados de forma centralizada, garantindo que todas as soluções estejam sempre atualizadas e protegidas contra novas ameaças.

6.3. Assim, a contratação de uma única empresa para fornecer e implementar todas as soluções de segurança e serviços associados oferece benefícios substanciais. Esta abordagem garante uma integração perfeita, aumenta a eficiência operacional, centraliza a responsabilidade, aproveita economias de escala, melhora a segurança, assegura consistência no suporte e simplifica a implantação. Além de fortalecer as medidas de segurança cibernética, essa estratégia otimiza recursos e reduz os custos operacionais da organização.

6.4. Desta forma, na presente demanda indica-se que seja **Global**, considerando a complexidade e interdependência dos componentes que formam a solução de segurança cibernética necessária para a SESAU.

6.5. A solução proposta consiste em uma plataforma única e integrada de proteção de e-mail, Endpoint e proteção contra ataques avançados. Além disso, inclui serviços de instalação, configuração, suporte e garantia de atualização por um período de 36 meses.

6.6. Devido à natureza intrínseca e interdependente das funcionalidades e serviços oferecidos, não é viável parcelar a contratação por itens. É necessário que todos os componentes sejam fornecidos pelo mesmo fabricante e que os serviços sejam realizados por um profissional especializado na solução.

6.7. Após uma análise detalhada, a equipe de planejamento optou por adotar o modelo de contratação por menor preço global, separando a solução em itens. Essa abordagem garante a obtenção da solução completa, com todos os componentes e serviços necessários, assegurando a integridade e efetividade da solução proposta.

6.8. A escolha pelo modelo de contratação por menor preço global tem como objetivo garantir a qualidade, eficiência e cumprimento dos requisitos técnicos estabelecidos. Esse modelo assegura que todos os componentes e serviços estejam incluídos, permitindo que a solução funcione de maneira integrada e eficaz.

6.9. Portanto, a opção pelo modelo de contratação por menor preço global é justificada pela natureza integrada da solução, que requer a contratação conjunta de todos os seus componentes e serviços para garantir seu pleno funcionamento e eficácia.

6.10. A decisão de não parcelar a contratação com base em aspectos econômicos é justificada pelos seguintes motivos:

6.10.1. A solução em questão é composta por funcionalidades e serviços intrinsecamente interligados. Isso significa que todos os componentes devem ser fornecidos pelo mesmo fabricante, e os serviços devem ser executados por um profissional especializado na solução. Parcelar a contratação resultaria em uma complexidade adicional devido à necessidade de gerenciar vários fornecedores e garantir a compatibilidade e integração adequadas entre os componentes. Isso poderia aumentar os custos e comprometer a eficácia da solução.

6.10.2. O parcelamento da contratação não traria vantagens econômicas significativas. Pelo contrário, poderia resultar em custos adicionais, como a necessidade de coordenar diferentes contratos, lidar com possíveis incompatibilidades entre os componentes e arcar com os custos de integração. Ao optar por uma única contratação integrada, é possível obter um melhor custo-benefício, evitando gastos desnecessários e garantindo a eficiência operacional.

6.10.3. Ao optar por uma única contratação integrada, a gestão do contrato e dos serviços relacionados se torna mais simples e eficiente. É possível ter um único ponto de contato e responsabilidade, facilitando o monitoramento, a comunicação e a resolução de problemas. Isso reduz a necessidade de recursos dedicados à administração de múltiplos contratos e contribui para a otimização dos custos operacionais.

6.10.4. Portanto, levando em consideração a integração dos componentes, a falta de vantagem econômica no parcelamento, a disponibilidade orçamentária e os ganhos de escala, bem como a simplificação da gestão, a opção de não parcelar a contratação é a mais adequada do ponto de vista econômico.

7. PARTICIPAÇÃO DE EMPRESAS SOB A FORMA DE CONSÓRCIO E COOPERATIVAS

7.1. Fica vedada a participação de empresas reunidas sob a forma de consórcio e cooperativas, tendo em vista que o objeto da licitação não é de grande porte, complexo tecnicamente e tampouco, operacionalmente inviável de ser executado por apenas uma empresa.

7.2. A ausência de consórcio e cooperativas não trará prejuízos à competitividade do certame, visto que, em regra, a formação de consórcios é admitida quando o objeto a ser licitado envolve questões de alta complexidade ou de relevante vulto, em que empresas, isoladamente, não teriam condições de suprir os requisitos de habilitação do edital.

8. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

8.1. Em análise, verificou-se que a solução mais adequada para a presente demanda será a de Registro de Preços para contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, visando atender às necessidades da Secretaria de Estado da Saúde de Rondônia, pelo período de 1 (um) ano.

8.2. A Secretaria de Estado da Saúde de Rondônia é responsável por gerenciar uma vasta rede de serviços de saúde, que inclui hospitais, laboratórios e outras instalações de saúde pública. Essas instituições dependem de sistemas de tecnologia da informação para o funcionamento eficiente e seguro de suas operações, incluindo o armazenamento e transmissão de dados sensíveis dos pacientes e da gestão hospitalar.

8.3. A escolha da solução abrangente, que inclui proteção de e-mail, Endpoint e proteção contra ataques avançados, está alinhada com as necessidades da SESAU-RO em garantir a segurança da rede para os usuários, prevenindo de forma proativa os ataques cibernéticos.

8.4. Existem benefícios significativos proporcionados por essa solução, como a capacidade de monitorar o comportamento das estações de usuários e caixas postais, detectar, bloquear, investigar e responder a incidentes de segurança da informação que possam ocorrer na rede da Secretaria. Além disso, essa solução está em conformidade com os requisitos de segurança da informação e atende às exigências da Lei Geral de Proteção de Dados (LGPD), o que evidencia que sua adoção trará melhorias significativas para o ambiente atual da Secretaria.

8.5. A adoção dessa solução trará benefícios em termos de qualidade e eficiência. Ela permitirá acompanhar as constantes evoluções dos recursos de TIC, ao mesmo tempo em que estará em conformidade com as exigências da LGPD.

8.6. A inclusão de serviços de instalação, configuração, suporte e garantia de atualização da solução por um período de 36 meses demonstra um compromisso com a qualidade e eficiência a longo prazo. Isso garantirá a disponibilidade e continuidade dos serviços de TI, além de fornecer suporte técnico especializado durante todo o período contratual.

8.7. Em resumo, a escolha dessa solução é justificada pela sua capacidade de garantir a segurança da rede, atender aos requisitos de segurança da informação, estar em conformidade com a LGPD e oferecer melhor qualidade, eficiência e suporte técnico especializado à SESAU-RO. Com essa escolha, a Secretaria estará protegendo seus sistemas e dados de forma abrangente e estará preparada para enfrentar os desafios da segurança cibernética de forma eficaz.

8.8. Independente do modelo a ser seguido, é importante que a decisão da Administração Pública seja pautada sob a ótica da eficácia da prestação do serviço, zelando pelos princípios que a regem. Assim, é necessário que a execução atenda efetivamente à necessidade coletiva, ou seja, com a otimização de recursos, e à manutenção de um serviço adequado e de qualidade.

8.9. **Suporte Técnico**

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

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

8.9.3. Os serviços de suporte técnico abrangem:

8.9.3.1. Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução.

8.9.3.2. Elaboração de relatórios, estudos e diagnósticos sobre o ambiente.

8.9.3.3. Transferência de conhecimento aos técnicos da Contratante referente aos problemas vivenciados e às soluções aplicadas, na forma a ser determinada pelas partes. Realização de instalação, atualização e configuração de novas versões dos produtos após a disponibilização das atualizações tecnológicas pelo fabricante.

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

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

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

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

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

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

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

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

a) Portal Web; E-mail;

b) Central 0800; e/ou

c) Telefone fixo.

8.9.3.12. O atendimento deve ser contínuo, 24 horas por dia, 7 dias por semana, durante todo o ano, incluindo feriados, em língua portuguesa. O início do atendimento e o prazo de solução devem ser determinados de acordo com o nível de severidade exigido para o caso, conforme os índices de criticidade **QUE SE ENCONTRA NO** ANEXO V:

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

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

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

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

8.9.4.1. Quantidade de ocorrências (chamados) registradas no período.

8.9.4.2. Número do chamado registrado e nível de severidade, incluindo reaberturas.

8.9.4.3. Data e hora de abertura. Data e hora de início e conclusão do atendimento.

8.9.4.4. Identificação do técnico do contratante que registrou o chamado.

8.9.4.5. Identificação do técnico do contratante que atendeu o chamado da garantia. Descrição do problema. Descrição da solução.

8.9.4.6. Informações sobre eventuais escalonamentos.

8.9.4.7. Resumo da lista de chamados concluídos fora do prazo de solução estabelecido.

8.9.4.8. Total de chamados no mês e o total acumulado até a apresentação do relatório.

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

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

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

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

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

8.10. **ESPECIFICAÇÕES TÉCNICAS**

8.10.1. **SOLUÇÃO DE PROTEÇÃO DE ENDPOINTS COM ABORDAGEM PROATIVA PARA RESPOSTA EFICAZ A INCIDENTES (ITEM 1)**

8.10.1.1. Características gerais:

8.10.1.1.1. A solução deverá ser entregue na modalidade como um serviço (em nuvem);

8.10.1.1.2. Possuir console Web para gerenciamento e administração da ferramenta;

8.10.1.1.3. A proteção para estações de trabalho deverá prover Anti-Malware, Firewall, Host IPS, Controle de Aplicações e Controle de dispositivos em um único agente.

8.10.1.1.4. Módulo de Proteção Anti-Malware.

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

8.10.1.1.5.1. Windows 8.1 (x86/x64); Windows 10 (x86/x64); Windows 11 (x64).

8.10.1.1.6. Deve disponibilizar evidências de varredura em todas as estações de trabalho, identificando as atualizações de sucesso e as ações de insucesso. Para garantir que os casos de insucesso sejam monitorados para tomada de ações pontuais;

8.10.1.1.7. Deve detectar, analisar e eliminar programas maliciosos, tais como vírus, spyware, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

8.10.1.1.8. Deve detectar, analisar e eliminar, automaticamente e em tempo real, programas maliciosos em: Processos em execução em memória principal (RAM);

8.10.1.1.9. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

8.10.1.1.10. Arquivos compactados automaticamente, em pelo menos nos seguintes formatos: zip, exe, arj, MIME/uu, CAB;

8.10.1.1.11. Arquivos recebidos por meio de programas de comunicação instantânea (MSN messenger, yahoo messenger, google talk, icq, dentre outros).

8.10.1.1.12. Deve detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como Javascript, VBScript/Activex; Deve possuir detecção heurística de vírus desconhecidos;

8.10.1.1.13. Deve permitir configurar o consumo de CPU que será utilizada para uma varredura manual ou agendada;

8.10.1.1.14. Deve permitir diferentes configurações de detecção (varredura ou rastreamento): Em tempo real de arquivos acessados pelo usuário;

8.10.1.1.15. Em tempo real dos processos em memória, para a captura de programas maliciosos executados em memória, sem a necessidade de escrita de arquivo;

8.10.1.1.16. Manual, imediato ou programável, com interface gráfica em janelas, personalizável, com opção de limpeza;

8.10.1.1.17. Automáticos do sistema com as seguintes opções: Escopo: todos os discos locais, discos específicos, pastas específicas ou arquivos específicos;

8.10.1.1.18. Ação: somente alertas, limpar automaticamente, apagar automaticamente, renomear automaticamente, ou mover automaticamente para área de segurança (quarentena);

8.10.1.1.19. Frequência: horária, diária, semanal e mensal;

8.10.1.1.20. Exclusões: pastas ou arquivos (por nome e/ou extensão) que não devem ser rastreados.

8.10.1.1.21. Deve possuir mecanismo de cache de informações dos arquivos já escaneados;

8.10.1.1.22. Deve possuir cache persistente dos arquivos já escaneados para que nos eventos de desligamento e reinicialização das estações de trabalho e notebooks, a cache não seja descartada;

8.10.1.1.23. Deve possuir ferramenta de alterações de parâmetros de comunicação entre o cliente antivírus e o servidor de gerenciamento da solução de antivírus;

8.10.1.1.24. Deve permitir a utilização de servidores locais de reputação para análise de arquivos e URL's maliciosas, de modo a prover, rápida detecção de novas ameaças;

8.10.1.1.25. Deve ser capaz de aferir a reputação das URL's acessadas pelas estações de trabalho e notebooks, sem a necessidade de utilização de qualquer tipo de programa adicional ou plug-in ao navegador web, de forma a proteger o usuário independentemente da maneira de como a URL está sendo acessada;

8.10.1.1.26. Deve ser capaz de detectar variantes de malwares que possam ser geradas em tempo real na memória da estação de trabalho ou notebook, permitindo que seja tomada ação de quarentena a ameaça;

8.10.1.1.27. Deve possuir capacidade de escaneamento de arquivos compactados e, em caso de identificação de um arquivo malicioso, apenas este deve ser removido, mantendo os demais intactos Deve ser capaz de bloquear o acesso a qualquer site não previamente analisado pelo fabricante;

8.10.1.1.28. Deve permitir a restauração de maneira granular de arquivos quarentenados sob suspeita de representarem risco de segurança;

8.10.1.1.29. Deve permitir em conjunto com a restauração dos arquivos quarentenados a adição automática as listas de exclusão de modo a evitar novas detecções dos arquivos;

8.10.1.1.30. Deverá ter funcionalidade de Machine Learning para detectar e tomar ações sobre ameaças desconhecidas e suspeitas;

8.10.1.1.31. Deverá ter funcionalidade de Machine Learning em runtime para evitar possíveis métodos de obfuscação que o módulo de Machine Learning em pré-execução não consiga detectar;

8.10.1.1.32. Deve fornecer um informativo compreensivo de cada simulação que descreva as ações e respectivos metadados, bem como, o porquê do veredito emitido pela Machine Learning;

8.10.1.1.33. Deve bloquear processos comuns associados a ransomware;

8.10.1.1.34. Em casos de ataques de ransomware, a solução deve ter a capacidade de interromper o processo de criptografia e restaurar os arquivos originais aos seus respectivos diretórios;

8.10.1.1.35. Deve possuir funcionalidade de detecção de malwares conhecidos e desconhecidos por comportamento;

8.10.1.1.36. Deve permitir a integração com solução de análise de artefatos suspeitos (sandbox) do próprio fabricante. Funcionalidade de Atualização Deve permitir a programação de atualizações automáticas das listas de

definições de vírus, a partir de local predefinido da rede, ou de site seguro da internet, com frequência (no mínimo diária) e horários definidos pelo administrador da solução;

8.10.1.1.37. Deve permitir atualização incremental da lista de definições de vírus;

8.10.1.1.38. Deve permitir a atualização automática do engine do programa de proteção a partir de localização na rede local ou na internet, a partir de fonte autenticável;

8.10.1.1.39. Deve permitir o rollback das atualizações das listas de definições de vírus e engines;

8.10.1.1.40. Deve permitir a indicação de agentes para efetuar a função de replicador de atualizações e configurações, de forma que outros agentes possam utiliza-los como fonte de atualizações e configurações, não sendo necessária a comunicação direta com o servidor de anti-malware para essas tarefas;

8.10.1.1.41. Deve permitir que os agentes de atualização possam replicar os componentes de vacinas, motores de escaneamento, versão de programas, hotfix e configurações específicas de domínios da árvore de gerenciamento;

8.10.1.1.42. O agente replicador de atualizações e configurações, deve ser capaz de gerar localmente versões incrementais das vacinas a serem replicadas com os demais agentes locais, de maneira a reduzir o consumo de banda necessário para execução da tarefa de atualização.

8.10.1.1.43. Funcionalidade de Administração Deve permitir proteção das configurações da solução instalada na estação de trabalho através de senha ou controle de acesso, em ambos os casos, controlada por política gerenciada pela console de administração da solução completa;

8.10.1.1.44. Deve possibilitar instalação "silenciosa";

8.10.1.1.45. Deve permitir o bloqueio por nome de arquivo;

8.10.1.1.46. Deve permitir o travamento de pastas e diretórios;

8.10.1.1.47. Deve permitir o travamento de compartilhamentos;

8.10.1.1.48. Deve permitir o rastreamento e bloqueio de infecções;

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

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

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

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

8.10.1.1.53. Deve permitir a deleção dos arquivos quarentenados;

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

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

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

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

8.10.1.1.58. Deve possuir solução de consulta do hash dos arquivos integrada e gerenciada através da solução de antivírus, cancelando o download ou execução do arquivo, de forma automática, baseado na resposta à consulta da base do fabricante; Deve permitir criação de subdomínios consecutivos dentro da árvore de gerenciamento;

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

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

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

antivírus;

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

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

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

8.10.1.1.65. Deve possuir a integração com o Active Directory para utilização de seus usuários para administração da console de antimalware;

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

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

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

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

8.10.1.1.70. Deve permitir configuração do serviço de reputação de sites da web em níveis: baixo, médio e alto. Funcionalidade de Controle de Dispositivos As configurações da funcionalidade de controle de dispositivos devem ser aplicadas por usuário;

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

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

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

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

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

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

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

8.10.1.1.78. Deve permitir controle de permissão ou bloqueio para dispositivos que não armazenam dados tendo, pelo menos, os seguintes tipos de dispositivos: adaptadores bluetooth, dispositivos de imagem, modems, interfaces wireless externas, cartões PCMCIA, dispositivos infravermelhos e portas COM/LPT. Módulo de Proteção Anti-Malware para estações MacOS O cliente para instalação deverá possuir compatibilidade com os sistemas operacionais: macOS 12 (Monterey); macOS 11 (Big Sur) macOS 10.15 (Catalina); macOS 10.14 (Mojave); macOS 10.13 (High Sierra);

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

8.10.1.1.80. Gerenciamento integrado à console de gerência central da solução; Proteção em tempo real contra vírus, trojans, worms, cavalos-de-tróia, spyware, adwares e outros tipos de códigos maliciosos;

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

8.10.1.1.82. Permitir a criação de listas de exclusões para pastas e arquivos que não serão verificados pelo antivírus;

8.10.1.1.83. Permitir a ações de reparar arquivo ou colocar em quarentena em caso de infeções a arquivos;

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

8.10.1.1.85. Deve possuir no mecanismo de autoproteção as seguintes proteções: Proteção e verificação dos arquivos de assinatura;

8.10.1.1.86. Proteção dos processos do agente de segurança; Proteção das chaves de registro do agente de segurança;

8.10.1.1.87. Proteção do diretório de instalação do agente de segurança. Funcionalidade de HIPS – Host IPS e Host Firewall Deve ser capaz de realizar a detecção/proteção contra exploração de vulnerabilidades nos seguintes sistemas operacionais: Windows 8.1 (x86/x64);

8.10.1.1.88. Windows 10 (x86/x64); Windows 11 (x64). Deve possuir módulo para proteção de vulnerabilidades com as funcionalidades de host IPS e host firewall;

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

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

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

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

8.10.1.1.93. Deverá possuir a possibilidade de configurar níveis diferentes de segurança podendo ser eles alto, médio e baixo; O modulo de HIPS deverá possuir perfis pré-determinados baseados em performance e segurança;

8.10.1.1.94. O modulo de HIPS deverá possuir regras pra proteger contra ameaças do tipo Ransomware;

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

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

8.10.1.1.97. Deve suportar configuração de parâmetros de pacotes como quantidade máxima de conexões TCP e timeout para pacotes UDP; Deve ter a capacidade de proteção contra exploração de vulnerabilidades do sistema operacional e de aplicações terceiras instaladas na estação de trabalho;

8.10.1.1.98. A lista de regras deve permitir que o administrador realize buscas e tenha rápida visibilidade do tipo da aplicação, em que modo a regra encontra-se (bloqueio ou monitoramento), CVE, CVSS score, quando aplicável. Módulo para Controle De Aplicações Deve ser capaz de realizar a proteção a códigos maliciosos nos seguintes sistemas operacionais: Windows 8.1 (x86/x64); Windows 10 (x64); Windows 11 (x64). As regras de controle de aplicação devem permitir as seguintes ações: Permissão de execução; Bloqueio de execução;

8.10.1.1.99. Bloqueio de novas instalações. A regra de liberação para o controle de aplicação deverá permitir que o programa liberado efetue ou não a execução de outros processos, As regras de controle de aplicação devem permitir o modo de apenas coleta de eventos (logs), sem a efetivação da ação regra; As regras de controle de aplicação devem permitir os seguintes métodos para identificação das aplicações: Assinatura SHA-1 e SHA-256 do executável;

8.10.1.1.100. Atributos do certificado utilizado para assinatura digital do executável;

8.10.1.1.101. Caminho lógico do executável;

8.10.1.1.102. Base de assinaturas de cortiçados digitais válidos e seguros. As regras de controle de aplicação devem possuir categorias pré-determinadas de aplicações;

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

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

8.10.1.1.105. Deve permitir a busca por aplicações ou fabricante destas; Deve possuir ferramenta para extrair o hash de um ou um grupo de executáveis, permitindo a importação destes hashes através de arquivo CSV. Módulo de Detecção e Resposta A solução deve ser compatível com os sistemas operacionais Windows, Linux e MacOS; O fabricante deve implementar e organizar os ataques baseados no framework MITRE ATT&CK®, identificando técnicas e táticas dos ataques;

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

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

8.10.1.1.108. Possuir painéis que apresentem visualização executiva dos principais incidentes e atividades no ambiente com base nos usuários, aplicações acessadas e estações de trabalho; Utilizar bases de inteligência de ameaças integrando relatórios de inteligência do fabricante e de terceiros para ajudar a identificar ameaças no ambiente;

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

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

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

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

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

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

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

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

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

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

8.10.1.1.119. O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

8.10.1.1.120. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

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

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

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

8.10.1.1.124. Deve consolidar e correlacionar diferentes modelos de ameaça relacionados a um único evento; Deve exibir os eventos de forma a priorizar os alertas mais críticos para que o analista realize a investigação, como pontuações ou níveis de prioridade; Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações;

8.10.1.1.125. Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console; Deve ser possível interagir com cada um dos objetos relacionados ao evento para análise avançada e resposta; Deve destacar e organizar as atividades relacionadas a cada modelo de detecção por ordem cronológica, permitindo identificar a relação de cada atividade com os modelos de detecção;

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

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

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

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

8.10.1.1.130. A solução deve mostrar, pelo menos, o timestamp, objetos envolvidos (comandos, processos,

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

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

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

8.10.1.1.133. Deve permitir adicionar arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

8.10.1.1.134. Deve permitir remover arquivos SHA-1, URLs, IPs ou domínios a lista de bloqueio dos sensores;

8.10.1.1.135. Deve permitir terminar processos ativos executados nas estações de trabalhos e servidores;

8.10.1.1.136. Permitir coletar e fazer o download de um arquivo para investigação local detalhada; Isolar a estação de trabalho desconectando-a da rede e permitindo se comunicar exclusivamente com a console de gerenciamento do fabricante;

8.10.1.1.137. Restaurar a conectividade da estação de trabalho com a rede;

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

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

8.10.2. **SOLUÇÃO DE PROTEÇÃO DE SERVIDORES COM ABORDAGEM PROATIVA PARA RESPOSTA EFICAZ A INCIDENTES (ITEM 2)**: SOLUÇÃO DE SEGURANÇA PARA CARGAS DE TRABALHO HÍBRIDAS COM DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO

8.10.2.1. Características Gerais Da Solução

8.10.2.1.1. A solução deverá ser compatível com pelo menos os seguintes sistemas operacionais: Windows Server 2000; Windows Server 2003 SP1 e 2003 R2 SP2; Windows Server 2008 e 2008 R2; Windows Server 2012 e 2012 R2; Windows Server 2016; Windows Server 2019;

8.10.2.1.2. Windows Server 2022; Red Hat Enterprise 5, 6, 7 e 8; CentOS 5, 6, 7 e 8; AIX 6.1, 7.1 e 7.2;

8.10.2.1.3. Oracle Linux 5, 6, 7 e 8;

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

8.10.2.1.5. Ubuntu 10, 12, 14, 16, 18 e 20;

8.10.2.1.6. Debian 6, 7, 8, 9 e 10;

8.10.2.1.7. Rocky Linux 8; AlmaLinux 8;

8.10.2.1.8. Cloud Linux 5, 6, 7 e 8;

8.10.2.1.9. Solaris 10 1/13 Sparc;

8.10.2.1.10. Solaris 10 1/13 (x86/x64);

8.10.2.1.11. Solaris 11.2/ 11.3 Sparc;

8.10.2.1.12. Solaris 11.2/ 11.3 (x86/x64);

8.10.2.1.13. Solaris 11.4 (x86, x64 ou SPARC) Amazon Linux e Amazon Linux 2 (x64). A solução deverá ser totalmente compatível e homologada com o ambiente Vmware;

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

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

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

8.10.2.1.17. Precisa ter a capacidade de controlar e gerenciar a segurança de múltiplas plataformas e sistemas operacionais, incluindo máquinas em nuvens externas a partir de uma console única e centralizada do próprio fabricante;

8.10.2.1.18. A solução deverá permitir a entrega de agentes por pelo menos duas dentre as principais ferramentas de distribuição de software do mercado: Microsoft System Center Configuration Manager, Novel Zen Works e Puppet;

8.10.2.1.19. A console de administração deverá permitir o envio de notificações via SMTP; Todos os eventos e ações realizadas na console de gerenciamento precisam ser gravados para fins de auditoria;

8.10.2.1.20. A solução deverá possuir a funcionalidade tags para identificar falsos positivos ou facilitar a visualização de determinados alertas; A solução deverá permitir a criação de widgets para facilitar a administração e visualização dos eventos;

8.10.2.1.21. A solução deverá permitir que a distribuição de patterns e novos componentes possa ser efetuada por agentes de atualização espalhados pelo ambiente;

8.10.2.1.22. A solução precisa permitir a criação de relatórios. A criação e envio destes relatórios deverá ocorrer sob- demanda, ou agendado com o envio automático do relatório via e-mail;

8.10.2.1.23. A solução deverá fornecer pelo menos dois tipos de relatórios nos seguintes formatos PDF, CSV, XLS e RTF;

8.10.2.1.24. A solução precisa permitir que relatórios no formato PDF, possam ser enviados com uma senha única para cada destinatário;

8.10.2.1.25. A solução deverá prover relatórios contendo no mínimo as seguintes informações;

8.10.2.1.26. malware, regras de IPS aplicadas e Firewall;

8.10.2.1.27. Em caso de solução e nuvem, o ambiente do fabricante deverá fornecer alta disponibilidade;

8.10.2.1.28. A solução de segurança ter a capacidade de identificar ataques entre conteineres;

8.10.2.1.29. Os usuários devem ter a capacidade de receber determinados papéis para administração como "acesso total" e "acesso parcial", podendo ser customizado o que compõe o "acesso parcial";

8.10.2.1.30. Quando configurado o acesso parcial, este deve permitir que um usuário tenha permissões de poder gerenciar a segurança de um único computador, podendo ainda definir em quais módulos de proteção será possível ou não editar ou criar novas políticas de segurança;

8.10.2.1.31. A comunicação entre a console de gerenciamento e os agentes deverá ser criptografada;

8.10.2.1.32. Cada agente deverá ter sua própria chave para criptografia de modo que a comunicação criptografada seja feita de forma diferente para cada agente;

8.10.2.1.33. A console de gerenciamento deverá ter dashboards para facilidade de monitoração, as quais deverão ser customizadas pelo administrador em quantidade e período de monitoração;

8.10.2.1.34. Os agentes de atualização deverão buscar os updates das assinaturas e distribuí-las para os agentes. Quando ocorrer a atualização, esta deverá ocorrer de modo absolutamente seguro utilizando-se SSL/TLS com o servidor de onde ela buscará as informações;

8.10.2.1.35. Os agentes para plataforma Microsoft deverão ser instalados por pacote MSI e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de script PowerShell;

8.10.2.1.36. Os agentes para plataforma Linux deverão ser instalados por pacote RPM ou DEB e posteriormente ativados pela console de gerenciamento de forma a proporcionar maior segurança ao ambiente, ou de forma automatizada através de bash script;

8.10.2.1.37. Em servidores Windows e Linux, a solução deverá permitir a atualização automática dos agentes após sua ativação;

8.10.2.1.38. Para servidores Linux, a solução deverá possibilitar a atualização automática da versão quando o agente reiniciar;

8.10.2.1.39. Para efeito de administração, a solução deverá avisar quando um agente se encontrar não conectado a sua console de gerenciamento;

8.10.2.1.40. Deve permitir a remoção automática de agentes inativos, definindo o período para, pelo menos 1 semana, 1 mês e 12 meses;

8.10.2.1.41. A solução deve possuir a capacidade de criar políticas de forma global para todas as máquinas, por perfis e individualmente para cada host;

8.10.2.1.42. Cada perfil poderá ser atribuído para um host ou um conjunto de hosts;

8.10.2.1.43. A solução deverá vir com perfis pré-definidos e aptos a funcionarem de acordo com sua denominação;

8.10.2.1.44. A solução deverá mostrar quais máquinas estão usando determinada política;

8.10.2.1.45. Os agentes deverão ser capazes de executar rastreamento nas máquinas onde estão instalados e após isso deverão fornecer uma lista de todas as recomendações de segurança para os softwares que estejam instalados nas máquinas bem como do sistema operacional;

8.10.2.1.46. Esses rastreamentos devem ocorrer de forma periódica a ser definida pelo administrador;

8.10.2.1.47. A solução deverá permitir a configuração de componentes de integração com o vCenter, a fim de permitir a sincronização das máquinas virtuais conectadas a ele;

8.10.2.1.48. Brechas de segurança descobertas deverão ser protegidas de forma automática e transparente, interrompendo somente o tráfego de rede malicioso;

8.10.2.1.49. O administrador do sistema de segurança deverá ter a possibilidade de não aplicar automaticamente a proteção para as vulnerabilidades escolhendo o perfil ou o host;

8.10.2.1.50. A solução deve possuir a capacidade de isolamento de placa de rede de forma que apenas uma fique funcionando de acordo com preferência do administrador;

8.10.2.1.51. A solução deverá ser capaz de aplicar políticas diferentes para placas de redes diferentes em um mesmo servidor;

8.10.2.1.52. A solução deverá ser capaz de executar bypass completo de rastreamento de tráfego de forma que os módulos não atuem em determinado tipo de conexão ou pacote;

8.10.2.1.53. A solução deverá ter a capacidade de se integrar com o Amazon SNS e os principais softwares de SIEMs contemplando, no mínimo: Splunk, IBMQradar e HPArcSight de modo a permitir enviar os seus logs para essas soluções;

8.10.2.1.54. A solução deverá ter a possibilidade de enviar logs para SYSLOG servers;

8.10.2.1.55. Solução deverá permitir criar relatórios customizados de todas as suas funcionalidades;

8.10.2.1.56. Deve permitir enviar os relatórios para uma lista de contatos independente de login na console de administração;

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

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

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

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

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

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

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

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

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

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

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

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

8.10.2.1.69. O fabricante da solução deverá manter programa de pesquisa em vulnerabilidades há, pelo menos, 5 anos;

8.10.2.1.70. A solução deve possuir API documentada para integração na esteira de automação;

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

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

8.10.2.1.73. A solução deve permitir desabilitar os módulos individualmente;

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

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

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

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

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

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

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

8.10.2.1.81. A solução deverá possuir a funcionalidade de Monitoramento de Comportamento para detectar mudanças e atividades suspeitas não autorizadas; A solução deverá oferecer escanear processos em memória em busca de Malware;

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

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

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

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

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

8.10.2.1.87. A solução deverá mostrar informação de data sobre o último scan agendado ou manual executado;

8.10.2.1.88. Possuir a capacidade de efetuar backup e restore de arquivos comprometidos por Ransomware;

8.10.2.1.89. Deve possuir cache dos arquivos verificados de modo a evitar a redundância da varredura;

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

8.10.2.1.91. A solução deve possuir opção para forçar a comunicação com o agente e coletar os respectivos logs;

8.10.2.1.92. Em servidores Windows, deve possuir capacidade de detectar ameaças por comportamento;

8.10.2.1.93. Deverá ter a possibilidade de escanear drivers de rede mapeados nos servidores. Proteção Contra

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

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

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

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

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

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

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

8.10.2.1.100. A proteção deve possibilitar proteção através da instalação de agente de segurança do fabricante da solução de segurança. Firewall Operar como firewall de host, através da instalação de agente nos servidores protegidos;

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

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

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

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

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

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

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

8.10.2.1.108. Regras de firewall poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

8.10.2.1.109. O firewall deverá ser stateful bidirecional; O firewall deverá permitir liberar ou apenas logar eventos;

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

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

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

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

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

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

8.10.2.1.116. Deverá permitir limitar o número de meias conexões vindas de um computador;

8.10.2.1.117. Deverá prevenir ack storm; Deverão existir regras default que possam ser utilizadas como modelo para a criação e adição de novas regras;

8.10.2.1.118. Deverá identificar escaneamentos ativos de porta ou da rede, bloqueando o IP ofensor por um

período de tempo configurado pelo administrador;

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

8.10.2.1.120. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas. Proteção De Vulnerabilidades de SO e Aplicações Precisa ter a capacidade de detectar e bloquear qualquer conexão indesejada que tente explorar vulnerabilidades do SO e demais aplicações;

8.10.2.1.121. Precisa ter a capacidade de varrer o servidor protegido detectando o tipo e versão do SO, detectando também as demais aplicações, recomendando e aplicando automaticamente regras IDS/IPS que blindem vulnerabilidades existentes no SO e aplicações. Esta varredura deverá poder ser executada sob demanda ou agendada;

8.10.2.1.122. A solução deverá conter regras pré-definidas para detecções de ransomware para as principais famílias deste tipo de malware;

8.10.2.1.123. Precisa ter a capacidade de detectar uma conexão maliciosa, com a possibilidade de bloquear esta conexão;

8.10.2.1.124. Precisa conter regras de defesa para blindagem de vulnerabilidades e ataques que explorem os seguintes sistemas operacionais: Windows 2003, 2008, 2012, 2016, 2019, Linux Red Hat, Suse, CentOS, Ubuntu, Debian, Solaris, AIX além de regras para aplicações padrão de mercado, incluindo Microsoft IIS, SQL Server, Microsoft Exchange, Oracle Database, Adobe Acrobat, Mozilla Firefox, Microsoft Internet Explorer, Google Chrome e Web Server Apache;

8.10.2.1.125. Precisa ter a capacidade de armazenamento do pacote capturado quando detectado um ataque;

8.10.2.1.126. Deverá possibilitar a criação de regras de IPS customizadas, para proteger aplicações desenvolvidas pelo cliente;

8.10.2.1.127. Precisa possuir a capacidade de detectar e controlar conexões de aplicações específicas incluindo Team Viewer, programas P2P e instant Messaging;

8.10.2.1.128. Precisa ter a capacidade de detectar e bloquear ataques em aplicações Web tais como SQL Injection e Cross Site Scripting.

8.10.2.1.129. Deverá ainda existir a possibilidade de captura do pacote relacionado ao ataque para fins de investigação do incidente;

8.10.2.1.130. Deverá permitir customização avançada e criação de novas regras de proteção de aplicações web, protegendo contra vulnerabilidades específicas de sistemas web legados e/ou proprietários;

8.10.2.1.131. Ser capaz de permitir ou negar que métodos utilizados por Webservers por regras de IPS;

8.10.2.1.132. Regras de IDS/IPS poderão ou não ser válidas de acordo com o contexto em que a máquina se encontra (por exemplo se está no domínio ou não);

8.10.2.1.133. Regras de IDS/IPS poderão ou não ser válidas de acordo com agendamento por horário ou dia da semana;

8.10.2.1.134. Deverá ser capaz de inspecionar tráfego criptografado de entrada;

8.10.2.1.135. Deverá inspecionar tráfego de aplicações Web em servidores buscando identificar: SQL injection, Crossite script, tamanho de URI fora de padrão, caracteres fora de padrão para requisição de URI, Double Decoding Exploit;

8.10.2.1.136. As regras de blindagem contra vulnerabilidades deverão conter links com referências externas, isto quando aplicável, explicando a vulnerabilidade do fabricante ou CVE relacionado;

8.10.2.1.137. Deverá possibilitar a criação de regras manuais para o bloqueio de tráfego customizado. Como por exemplo, bloquear acesso a um determinado website ou bloquear acesso de uma aplicação X;

8.10.2.1.138. Deverá possibilitar a criação de regras manuais baseadas em padrão XML, forma de assinatura ou padrões que possuam começo e fim coincidentes;

8.10.2.1.139. Deverá bloquear tráfego por aplicação independente da porta que a aplicação utilize, de modo que a aplicação não consiga comunicar na rede, como por exemplo, bloqueio de tráfego de uma determinada web browser ou aplicação de backup;

8.10.2.1.140. Solução deve ser capaz de habilitar modo debug na coleta dos pacotes de forma a capturar o tráfego anterior e posterior ao que foi bloqueado para facilidade de análise;

8.10.2.1.141. As regras de IPS deverão obrigatoriamente ter descrições de seu propósito;

8.10.2.1.142. As regras de IPS poderão atuar detectando ou bloqueando os eventos que as violem de modo que o administrador possa optar por qual ação tomar;

8.10.2.1.143. As regras de IPS de vulnerabilidade deverão apresentar severidade baseada em CVEs; As regras de IPS poderão ter sua capacidade de LOG desabilitado;

8.10.2.1.144. As regras de IPS quando disparadas poderão ter a possibilidade de emitir um alerta; As regras devem ser atualizadas automaticamente pelo fabricante;

8.10.2.1.145. Poderá atuar no modo em linha para proteção contra-ataques ou modo escuta para monitoração e alertas. Monitoramento De Integridade A solução deverá permitir a implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX, através da instalação de agentes;

8.10.2.1.146. Precisa ter a capacidade de detectar mudanças de integridade em arquivos e diretórios do SO e aplicações terceiras;

8.10.2.1.147. Precisa ser capaz de detectar mudanças no estado de portas em sistemas operacionais Linux;

8.10.2.1.148. Precisa ter a capacidade de monitorar o status de serviços e processos do sistema operacional;

8.10.2.1.149. Precisa ter a capacidade de monitorar mudanças efetuadas no registro do Windows;

8.10.2.1.150. Precisa ter a capacidade de criação de regras de monitoramento em chaves de registro, diretórios e subdiretórios e customização de XML para criação de regras avançadas;

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

8.10.2.1.152. O monitoramento poderá ser realizado em tempo real ou utilizando de scans periódicos para detectar mudanças de integridade;

8.10.2.1.153. Deverá alertar toda vez que uma modificação ocorrer em tempo real para ambiente Windows e pseudo real-time para ambiente Linux;

8.10.2.1.154. Deverá logar e colocar em relatório todas as modificações que ocorram;

8.10.2.1.155. As regras de monitoramento de integridade deverão ser atualizadas pelo fabricante ou melhoradas de forma automática;

8.10.2.1.156. Deverá poder classificar as regras de acordo com severidade para melhor verificação nos logs e recebimento de alertas;

8.10.2.1.157. Deverá possibilitar escolher o diretório onde o arquivo será monitorado e incluir ou não incluir determinados tipos de arquivos dentro desse mesmo diretório;

8.10.2.1.158. Algumas regras podem ser modificadas pelo administrador para adequação ao seu ambiente. Inspeção De Logs A solução deverá permitir sua implantação nas plataformas Linux, Microsoft, Solaris, HP-UX, AIX; Precisa ter a capacidade de monitorar e inspecionar arquivos de log do sistema operacional e demais aplicações, gravando uma cópia deste log em um banco de dados externo e notificando o administrador sobre eventos suspeitos;

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

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

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

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

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

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

8.10.2.1.165. Deverá ter inteligência para que a cada violação relevante no log inspecionado que seja suspeita

no servidor seja alertada;

8.10.2.1.166. Deverá logar cada violação e colocar em relatório todas as violações relevantes que ocorram;

8.10.2.1.167. As regras poderão ser modificadas por severidade de ocorrência de eventos;

8.10.2.1.168. As regras devem se atualizar automaticamente pelo fabricante; Permitir modificação pelo administrador em regras para adequação ao ambiente. Controle De Aplicações A solução deverá permitir sua implantação nas plataformas Linux e Microsoft Windows;

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

8.10.2.1.170. O agrupamento dos eventos deverá ser realizado pelo menos por Hash ou por máquina;

8.10.2.1.171. A console deverá exibir eventos de no mínimo 30 dias;

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

8.10.2.1.173. A solução deverá possuir no mínimo as funcionalidades de bloquear o que não for permitido explicitamente e permitir o que não for bloqueado explicitamente. Detecção e Resposta A solução deve ser compatível com Linux e Windows Server 2008 R2 e superiores;

8.10.2.1.174. A solução deve possuir módulo de investigação, detecção integrados; Deve permitir que as detecções sejam correlacionadas com módulos de endpoint, rede e e-mail do próprio fabricante através de console dedicada. Não serão aceitas consoles de correlação de terceiros;

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

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

8.10.2.1.177. O módulo de EDR deve atuar baseado em modelos de detecção de ataques avançados e furtivos;

8.10.2.1.178. Os logs de detecções devem estar disponíveis na console por, pelo menos, 30 dias;

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

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

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

8.10.2.1.182. Deve ser possível criar usuários com permissões distintas, contendo no mínimo, permissão total e permissão para realizar investigações; Deve permitir habilitar ou desabilitar um determinado usuário sem excluí-lo da console;

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

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

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

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

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

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

8.10.3. **SOLUÇÃO DE SEGURANÇA AVANÇADA PARA MITIGAÇÃO DE AMEAÇAS NA REDE (ITEM 3):** SOLUÇÃO DE SEGURANÇA CONTRA AMEAÇAS AVANÇADAS COM DETECÇÃO E RESPOSTA, INCLUINDO GARANTIA E ATUALIZAÇÃO DE VERSÃO POR 12 (DOZE) MESES.

8.10.3.1. Características Gerais

8.10.3.1.1. A solução deverá ser instalada de modo a detectar ameaças avançadas no ambiente da CONTRATANTE, inspecionando o tráfego de rede, independente de agentes instalados;

8.10.3.1.2. Deve ser dimensionada para inspecionar 04Gbps de throughput; A solução deve permitir que o administrador escolha uma implementação em modo inline ou em modo de monitoramento através de tráfego espelhado;

8.10.3.1.3. Caso seja implementada no modo inline, a solução deverá permitir criar um by-pass para casos de falhas de interface;

8.10.3.1.4. Quando inline, a solução deverá ter a capacidade de analisar tráfego TLS; Funcionalidades e Requisitos específicos: Deverá fornecer solução integrada de proteção contra ameaças avançadas de acordo com funcionalidades e características técnicas especificadas neste documento, contendo, no mínimo os seguintes módulos: Monitoramento, Identificação, Análise e Resposta de Incidentes de Segurança;

8.10.3.1.5. Detecção de ataques direcionados; Analisador virtual de ameaças;

8.10.3.1.6. Correlação de regras para detecção de conteúdo malicioso;

8.10.3.1.7. Análise de todos os estágios de uma sequência de ataques. Esta solução deverá ser atendida através do fornecimento de solução de um único Fabricante, contendo: Serviço de Monitoração e Análise de Ameaças Digitais em rede;

8.10.3.1.8. Serviço de Monitoração e gestão de riscos que permita a identificação de ameaças digitais conhecidas e não conhecidas por soluções de antivírus tradicionais, permitindo a composição de serviços de mitigação complementares para a segurança do ambiente;

8.10.3.1.9. Serviço que entenda ameaça digital como a representação de um software malicioso ou ação maliciosa tal como: spyware, phishing, worms, bot, trojan, adware, network Exploit, web Exploit, Cross-site scripting, spear phishing, information stealing malware e outras ações que podem compor ataques ao patrimônio computacional do ambiente;

8.10.3.1.10. Visibilidade e relatório de incidentes de conexões da rede interna com sites maliciosos ou servidores de central de comando (C&C) externos;

8.10.3.1.11. Análise e correlação de atividades maliciosas tais como: Detecção específica de malwares conhecidos e arquivos contaminados através de assinaturas de antivírus tradicional no tráfego da rede;

8.10.3.1.12. Detecção de vermes de rede e de e-mail no tráfego de rede; Detecção de programas de exploração de vulnerabilidades (Exploits) na rede; Detecção de empacotamentos maliciosos no tráfego da rede;

8.10.3.1.13. Validação de tráfego web malicioso através de consultas a sistemas de reputação na Internet;

8.10.3.1.14. Visibilidade e relatório de estatísticas de ameaças, fontes de infecção na rede monitorada e máquinas comprometidas. Permitir a rápida identificação da criticidade dos eventos de segurança Permitir realizar pesquisas avançadas e customizadas dos incidentes de segurança através da console de gerenciamento;

8.10.3.1.15. Possibilidade de criação de filtros para visualização de eventos específicos conforme contexto, localização e outras variáveis que permitam investigação profunda sobre causa raiz de incidentes de segurança;

8.10.3.1.16. Permitir a customização de alertas em base ao tipo de incidente de segurança através da console de gerenciamento;

8.10.3.1.17. Permitir a integração com sistemas de serviço de diretório;

8.10.3.1.18. Capacidade de verificar em tempo real a reputação de endereços web (URL's) e servidores de correio SMTP;

8.10.3.1.19. A análise de SMTP poderá ser realizada em uma solução separada do sensor de HTTP e demais protocolos;

8.10.3.1.20. A capacidade de análise de artefatos em sandbox pode ser realizada através de no mesmo equipamento de análise; A solução deverá possuir mecanismo de conhecimento de senhas de pelo menos 90 palavras chaves em seu vocabulário de conhecimento, para derivação de arquivos protegidos;

8.10.3.1.21. Capacidade de criar e salvar investigações customizadas dos incidentes de segurança; Deve possuir pelo menos 1 sensor para inspecionar o tráfego de rede de throughput de 04Gbps de análise; Deve possuir a capacidade de detectar ameaças direcionadas, ataques do dia zero e documentos que viabilizem ataques;

8.10.3.1.22. Deve detectar atividades maliciosas que trafegam na rede através de motor de análise de comportamento de tráfego até o nível 7 (camada de aplicação) em protocolo TCP/IP;

8.10.3.1.23. Capacidade de detectar ameaças web tais como vulnerabilidades e download de conteúdo malicioso; Os módulos de captura de rede deverão suportar a coleta de arquivos pelo menos nos protocolos HTTP e HTTPS;

8.10.3.1.24. Deve possuir a habilidade de detectar e analisar os seguintes protocolos e aplicativos: P2P, SMTP, POP3, IRC, DNS, HTTP, FTP, TFTP, SMB, MSN, AIM, YMSG, Yahoo Mail, Hotmail, RDP, DHCP, TELNET, File Transfer, VNC, Cisco-TELNET, Kerberos, DCE-RPC, SQL, HTTPS, SMB2, MMS, IMAP4, RTSP/RTP-UDP, RTSP/RTP-TCP, RTSP/RDT-UDP, RTSP/RDTTCP, WMSP, SHOUTCast, RTMP, Bittorent, Kazaa, Blubster, eDonkeyeMule, Gnucleus LAN, Gnutella/Limewire/Bearshare/Shareaza, Winny, WinMX, MLDonkey, DirectConnect, SoulSeek, OpenNap, Kuro, iMesh, Skype, Google Talk, Zultrax, Foxy, eDonkey, Ares, Miranda, Kceasy, MoodAmp, Deepnet Explorer, FreeWire, Gimme, GnucDNA GWebCache, Jubster, MyNapster, Nova GWebCache, Swapper GWebCache, Xnap, Xolox, Ppstream, AIM Express, Chikka SMS Messenger, eBuddy, ICQ2Go, ILoveIM Web Messenger, IMUnitive, mabber, meebo, Yahoo Web Messenger, GPass, IP, ARP, TCP, UDP e IGMP;

8.10.3.1.25. Deve possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;

8.10.3.1.26. Capacidade de oferecer informações para análise forense de artefatos suspeitos de serem maliciosos; Gerenciamento centralizado de todas as etapas dos eventos de segurança identificados como possíveis ameaças;

8.10.3.1.27. Capacidade de identificar artefatos maliciosos direcionados para dispositivos moveis rodando o sistema operacional Android, tais como telefones inteligentes e tablets;

8.10.3.1.28. Deve analisar em tempo real o comportamento através de simulação de execução de arquivos provenientes do tráfego de rede incluindo arquivos PDF´s, executáveis, PPT, DOC, XLS, ZIP e RAR;

8.10.3.1.29. A solução deve detectar ameaças do dia zero, vulnerabilidade, URL’s maliciosas e spams dirigidos no protocolo SMTP;

8.10.3.1.30. Deve possuir tecnologia de análise de arquivos binários através de simulação e avaliação de execução dos artefatos suspeitos para identificação de comportamento malicioso, com capacidade de operar vários ambientes simultâneos e integrados a solução para processamento de alto desempenho;

8.10.3.1.31. Deve permitir o uso de base de conhecimento na Internet do próprio fabricante para correlacionamento de informações sobre ameaças conhecidas e prover recomendações de ações;

8.10.3.1.32. Deve permitir o uso de portas espelhadas de switch (mirror port) para monitorar o tráfego e detectar potenciais riscos à Segurança;

8.10.3.1.33. Deverá permitir o rastreio por malwares utilizando métodos de detecção baseados no tipo de arquivo (True File Type), múltiplas camadas de empacotamento (Multi-packed/Multi-layered files) e arquivos comprimidos (compactados);

8.10.3.1.34. Deverá analisar arquivos maliciosos na rede utilizando vacinas e técnicas de heurística;

8.10.3.1.35. Deve possuir foco em proteção contra APTs (Advanced Persistent Threats);

8.10.3.1.36. Deve possuir tecnologia de proteção contra ameaças desconhecidas (ataques dirigidos e ameaças de dia zero), sendo que este módulo deve pertencer ao mesmo fabricante;

8.10.3.1.37. Deverá possuir suporte para monitorar múltiplas interfaces de rede conectadas a diferentes VLANs ou witches;

8.10.3.1.38. Deverá possuir suporte para balanceamento de carga no sensor de inspeção de tráfego, possibilitando assim obter uma melhor performance;

8.10.3.1.39. Deverá permitir a análise específica de eventos de segurança de computadores suspeitos de atividade maliciosa;

8.10.3.1.40. Os módulos que compõem a solução devem atuar de forma integrada, centralizando logs de incidentes em ponto único;

8.10.3.1.41. Deve possuir atualização automática de regras e assinaturas, sendo que estas devem ser disponibilizadas via web pelo fabricante da solução;

8.10.3.1.42. Deve possuir mecanismo de consultas automáticas em bases de reputação externas de propriedade do fabricante da solução;

8.10.3.1.43. Deve ser capaz de identificar movimentos laterais em uma rede corporativa;

8.10.3.1.44. Deve atuar de forma passiva na captura de tráfego sem oferecer impacto no desempenho da rede;

8.10.3.1.45. Deve possuir interface web para busca e investigação local de incidentes;

8.10.3.1.46. O ambiente controlado de sandbox deve contemplar, pelo menos, os sistemas operacionais CentOS, Windows 10, Windows 7, Windows Server 2003, 2008, 2012 R2, 2016 e 2019; Deve possuir possibilidade de habilitação e desabilitação de regras de inspeção, individualmente, através de interface de gerenciamento web;

8.10.3.1.47. Deve possuir regras que identifiquem comunicações dos seguintes tipos: C&C, Exploits, Executáveis Maliciosos, Comunicação com Sites Maliciosos, backdoors e Botnets; Deve possuir regras que identifiquem comunicações de estações de trabalho e servidores com serviços não autorizados, tais como: consultas DNS em servidor não autorizado, utilização de SMTP server não autorizado, Proxy Server não autorizado;

8.10.3.1.48. Deve possuir regras que identifiquem comunicações p2p, instant messengers e streaming;

8.10.3.1.49. Deve possuir capacidade de geração de relatórios dos seguintes tipos e contendo as seguintes características: Resumidos;

8.10.3.1.50. Visão Geral dos Incidentes de Segurança Discriminação dos Tipos de Incidentes Top Ameaças Analisadas Top Hosts Infectados Recomendações de Segurança Executivos;

8.10.3.1.51. Deve possuir detalhes técnicos dos incidentes detectados; Deve possuir estatística do tráfego analisado; Deve possuir indicadores de risco do ambiente; Recomendações de Segurança.

8.10.3.1.52. Deve ser capaz de identificar, filtrar e exibir em interface gráfica, e dinamicamente atualizada, hosts com alto nível de risco, classificando os tipos de riscos/eventos detectados;

8.10.3.1.53. Deve possuir interface que apresente em Real Time estatísticas de top ameaças detectadas, top arquivos analisados, top hosts afetados, top URL’s maliciosas acessadas, etc.;

8.10.3.1.54. Quando detectada uma ameaça, a solução deve prover, podendo esta realizar consultas em site do fabricante, informações sobre ameaça, família da ameaça, estatísticas de segmentos de mercado afetados e recomendações de segurança para eliminar ameaça, correlacionando estas informações com sites ou outros vetores por onde esta ameaça é disseminada;

8.10.3.1.55. As atualizações do produto (patterns e outros componentes) não devem causar downtime ou impacto na operação;

8.10.3.1.56. Deve ser capaz de identificar ameaças que afetam dispositivos móveis (Ex. Detecção de comunicação de aplicativo malicioso na plataforma Android);

8.10.3.1.57. Deve ser capaz de detectar tentativas de mascaramento ou evasão de detecção através do uso de portas comuns ou protocol tunneling;

8.10.3.1.58. Deve ser capaz de detectar tentativas de scan de rede; Deve ser capaz de detectar propagação de malwares na rede;

8.10.3.1.59. Deve ser capaz de detectar tentativas de brute-force; Deve ser capaz de detectar tentativas de fuga e roubo de informação;

8.10.3.1.60. Deve ser capaz de detectar ameaças que se replicam na rede; Deve ser capaz de detectar Exploits na rede;

8.10.3.1.61. O Monitoramento de protocolos de comunicação deve ser feito através de appliance único (ou virtual appliance);

8.10.3.1.62. A console de gerenciamento deve possuir mapa mundial, onde são marcadas origens de ataques e eventos de segurança monitorados pela solução;

8.10.3.1.63. Deve permitir busca por informações do destino e origem, incluindo estas: endereço IP, endereço MAC, porta e protocolo;

8.10.3.1.64. Deve permitir consultas personalizáveis, usando comandos SQL ou atributos pré-definidos;

8.10.3.1.65. Capacidade de salvar uma investigação antes de ser finalizada; Capacidade de restaurar uma investigação para continuá-la ou consultá-la;

8.10.3.1.66. Capacidade de emitir relatórios baseados nas investigações;

8.10.3.1.67. Deve permitir apresentação dos dados consultados em vários formatos, incluindo tabela e gráficos;

8.10.3.1.68. Deve trabalhar com geolocalização para identificar a origem geográfica de um ataque;

8.10.3.1.69. Deve ter a capacidade de sugerir termos de busca, de acordo com o conteúdo já buscado numa investigação, para agilizar a obtenção do resultado;

8.10.3.1.70. Deve permitir exportar sob demanda os logs em texto puro (CSV ou similar);

8.10.3.1.71. Deve sugerir consultas a bases de reputação e whois quando encontrados hosts e nomes de domínio;

8.10.3.1.72. Deve permitir investigação por tags (palavras-chave) pré-configuradas para facilitar a busca de eventos;

8.10.3.1.73. Deve permitir recebimento de logs via syslog;

8.10.3.1.74. Deve permitir encaminhamento de logs via syslog;

8.10.3.1.75. Deve permitir receber logs de diferentes dispositivos;

8.10.3.1.76. Deve possuir engine de correlação de eventos;

8.10.3.1.77. Deve inserir tags personalizadas nos logs, de acordo com regras especificadas pelo usuário;

8.10.3.1.78. A solução de análise em sandbox deve ter a capacidade de analisar, de forma estática e dinâmica, ameaças com características de autoinicialização ou alteração de arquivos de sistema, rootkits/cloakings, arquivos mal-formados, engenharia social, dentre outros;

8.10.3.1.79. A análise de sandbox deve identificar e analisar ameaças que tenham características de evitar a segurança e análise em sandbox, e auto-preservação;

8.10.3.1.80. Deve enviar alertas via e-mail para pelo menos 100 e-mails diferentes; Deve permitir a configuração de alarmes personalizados, com base em investigações;

8.10.3.1.81. Deve informar em sua console alarmes que dispararam, até que o usuário tome alguma ação;

8.10.3.1.82. A console de gerenciamento deverá ser web, apresentando alta disponibilidade de modo que na ausência da principal, o restante da solução permaneça ativa e funcionando;

8.10.3.1.83. A solução deve ser escalável horizontalmente, permitindo que novas instâncias sejam habilitadas, aumentando suas capacidades de detecção e analise;

8.10.3.1.84. A console de gerenciamento deverá ter dashboards para facilidade de monitoração. As janelas deverão ser customizadas pelo administrador em quantidade e período de monitoração;

8.10.3.1.85. O administrador deve poder optar por janelas de monitoramento no dashboard a sua disposição e poderá livremente adicionar ou remover de acordo com sua necessidade de visualização;

8.10.3.1.86. Deverá possuir mapa geográfico que permita a identificação visual sobre a origem de ameaças de modo a facilitar a visualização de eventos críticos para que ações imediatas sejam providenciadas; Deverá possuir a capacidade de atualizar as vacinas, engines, assinaturas e recursos de inspeção de conteúdo de forma agendada e automática;

8.10.3.1.87. A console de gerenciamento deverá ser gerenciada por Internet Explorer, Google Chrome e Firefox;

8.10.3.1.88. Solução deverá ter mecanismo de busca em sua console de gerenciamento de modo que seja facilitada a busca por detecções;

8.10.3.1.89. Deverá ser capaz de identificar ameaças evasivas em tempo real com o provimento de análise profunda e inteligência para identificar e prevenir ataques;

8.10.3.1.90. Deverá ser capaz de correlacionar regras de detecção de conteúdo malicioso durante todas as fases de um ataque;

8.10.3.1.91. Deve permitir a adição e remoção dos diversos recursos de visualização de informações na tela principal de monitoramento da ferramenta, permitindo no mínimo a visualização das seguintes informações: Uso de CPU Uso de Disco;

8.10.3.1.92. Uso de Memória;

8.10.3.1.93. Tráfego malicioso analisado;

8.10.3.1.94. Todo o tráfego analisado. A solução deverá permitir o envio de logs dos recursos para servidor de logs por meio do protocolo syslog e deverá conter no mínimo: Tipo de evento de detecções: Conteúdo malicioso,

reputação de URL's, comportamentos maliciosos, comportamentos suspeitos, Exploits, correlações de eventos, Grayware;

8.10.3.1.95. Tipo de eventos de sistemas: Eventos de sistema e eventos de atualizações.

8.10.3.1.96. A solução deverá ter integração com ferramentas de SIEM;

8.10.3.1.97. Deve possuir capacidade de entregar relatório contendo informações da sequência de execução do artefato malicioso, assim como, detalhes de alterações locais da máquina, conexões externas e envio da informação para fora da rede corporativa;

8.10.3.1.98. A solução deve prover serviço de agregação e correlação de logs de eventos de segurança possibilitando coleta de fontes de monitoração para proporcionar informação e identificação de ameaças digitais conhecidas e desconhecidas em transito através de logs de sensor;

8.10.3.1.99. Solução deverá apresentar relatórios customizados de todas as suas funcionalidades e deverá conter no mínimo: Computadores infectados; Origem de infecções; Estatísticas de ameaças;

8.10.3.1.100. Riscos potenciais de segurança; Riscos de perda de informações;

8.10.3.1.101. Risco de sistema comprometido;

8.10.3.1.102. Risco de disseminação de ameaças;

8.10.3.1.103. Eventos suspeitos;

8.10.3.1.104. Infecções de malware. A solução deverá apresentar função de pesquisa por logs contendo no mínimo: Critérios de pesquisa por dia, mês e ano. Possibilidade de pesquisa pelo nome do computador, domínio ou conta, endereço IP, endereço MAC e grupos;

8.10.3.1.105. Possibilidade de pesquisa por ameaças, URL's maliciosas, análises virtuais, correlação de incidentes, nome de malware, protocolo e direção da detecção;

8.10.3.1.106. Os relatórios e logs deverão ser exportados nos formatos PDF ou CSV. Módulo de Detecção e Resposta A solução deve ter a capacidade de integrar-se com a plataforma de investigação e resposta centralizada, a fim de enviar objetos suspeitos e metadados das detecções locais para correlação com as demais soluções de segurança do ambiente;

8.10.3.1.107. A funcionalidade deve ser licenciada para analisar o throughput total do appliance;

8.10.3.1.108. A solução deve permitir a integração dos eventos ocorridos em outros segmentos de rede e outros appliances com objetivo de correlacionar os ataques na rede;

8.10.3.1.109. Deve permitir a análise em linha de tempo gráfica, representando a sequência da comunicação dos ativos, bem como seu protocolo e direção;

8.10.3.1.110. Deve identificar tentativas de ataques avançados na rede da CONTRATANTE e correlacionar com eventos das soluções de estação de trabalho, servidores e e-mail, a fim de rastrear o passo-a-passo do ataque na rede;

8.10.3.1.111. Caso necessário, a CONTRATANTE pode optar em direcionar parte do licenciamento deste módulo para outros módulos da plataforma de Detecção e Resposta, como o monitoramento do email, endpoint ou servidores, sem acréscimos ou mudanças de licenciamento;

8.10.3.1.112. Ao clicar em um dos objetos identificados pela solução de inspeção de rede, a plataforma deverá informar um resumo do ataque em questão, contendo o IP/hostname envolvido, quais protocolos, atividades maliciosas, severidade do incidente, fases do ataque;

8.10.3.1.113. Deve exibir de forma e em tabela, as transações identificadas contendo detalhes do ataque, bem como os Indicadores de Comprometimento (IOCs).

8.10.4. **SOLUÇÃO DE PREVENÇÃO DE INTRUSÃO DE PRÓXIMA GERAÇÃO (NGIPS) (ITEM 4)**

8.10.4.1. Plataforma e Performance A solução NGIPS (NEXT GENERATION INTRUSION PREVENTION SYSTEM) ofertada deverá ser disponibilizada em hardware do próprio fabricante, não sendo aceitos hardwares de fabricantes terceiros, não sendo aceitos também hardwares homologados (quando o fabricante da solução-software e do hardware são empresas diferentes); Não serão aceitas soluções NGFW ou UTM; O NGIPS deverá suportar a importação de regras no padrão SNORT, podendo esta ocorrer de forma direta e nativa via interface de gerenciamento, ou então através de ferramenta de conversão, onde o arquivo padrão SNORT deverá ser importado e convertido para o padrão utilizado pela solução ofertada;

8.10.4.2. A solução NGIPS deverá possuir interfaces de rede modularizadas com, pelo menos, 2 slots para inserção de módulos;

8.10.4.3. Os módulos disponíveis para a solução NGIPS devem contemplar, pelo menos, expansão até 20 interfaces 10/100/1000Gbps, expansão até 20 interfaces 1Gbps SFP, expansão até 16 interfaces 10Gbps SFP+ e expansão até 4 interfaces 40Gbps QSFP+ (os transceivers necessários deverão ser entregues em conjunto da solução);

8.10.4.4. Para atendimento do bypass das interfaces cobre, não serão aceitos dispositivos externos. Nas interfaces de fibra óptica deverá ser ofertado módulo de bypass, que poderá ser embutido ou externo;

8.10.4.5. A solução NGIPS deverá usar discos de estado sólido (SSD), não sendo aceitos equipamentos com discos mecânicos;

8.10.4.6. Deverá ser entregue equipamento NGIPS que atenda às seguintes especificações: IPS com throughput de inspeção de 3Gbps, podendo ser expandido até 5Gbps sem necessitar trocar o equipamento;

8.10.4.7. Deverá gerar latência igual ou inferior a 40 Microsegundos;

8.10.4.8. Deverá suportar pelo menos 390.000 novas conexões por segundo;

8.10.4.9. Deverá suportar pelo menos 29 milhões de sessões concorrentes;

8.10.4.10. Deverá suportar pelo menos 3.300 novas conexões SSL por segundo;

8.10.4.11. Deverá suportar inspeção de tráfego SSL de até 3,5Gbps;

8.10.4.12. O hardware ofertado deverá possuir fontes redundantes do tipo hot-swap;

8.10.4.13. O hardware ofertado deverá operar entre 0°C até 40°C;

8.10.4.14. O hardware ofertado deverá operar em ambientes com umidade entre 5% e 95%. Requisitos Técnicos e de Segurança A solução NGIPS ofertada deverá prover funcionalidades de prevenção de intrusão, em seu modo default (configuração básica) com pelo menos 2000 regras ativas (habilitadas automaticamente quando uma nova política de segurança é criada, em modo bloqueio e com criação de notificação);

8.10.4.15. A solução NGIPS ofertada deverá prover funcionalidades de prevenção de intrusão, em seu modo default (configuração básica) com pelo menos 2000 regras ativas (habilitadas automaticamente quando uma nova política de segurança é criada, em modo bloqueio e com criação de notificação);

8.10.4.16. Os filtros providos pelo NGIPS deverão permitir a seleção de ações de resposta. Deverão existir pelo menos as seguintes ações: Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Captura de Pacotes), além de ações condicionais, que permitam a definição de ações que alternam entre permitir e bloquear determinados tráfegos / ataques de acordo com condições encontradas no ambiente como, por exemplo, permitir as 1000 primeiras conexões de um único IP para determinado tráfego de rede em um período de 15 minutos. Após a conexão 1001 na mesma janela de tempo, a ação deverá ser alternada para bloqueio;

8.10.4.17. A solução NGIPS deverá suportar assinaturas de IPS para proteger vulnerabilidades, detectar exploits, detectar roubo de informações, detecção de virus, detecção de spywares, detectar tentativas de reconhecimento de rede, possuir regras que ajudem a controlar comportamentos de rede (exemplo: permitir ou bloquear resposta de comandos ping, detectar falhas de autenticação no MS SQL Server), possuir regras que blindem equipamentos de rede contra ataques que explorem vulnerabilidades, regras que efetuem a normalização de tráfego, ou seja, detectem tunelamento de protocolos, e cabeçalhos IP incompletos, além de filtros que permitam e detecção e controle de aplicações, tais como youtube, skype, TOR e facebook;

8.10.4.18. Os filtros do NGIPS precisam estar segmentados por categorias, com o objetivo de facilitar o gerenciamento da solução. Deverão existir pelo menos as seguintes categorias: Políticas de Segurança, Exploits, Normalização de Tráfego, Vírus, Reconhecimento de Rede, P2P e Vulnerabilidades;

8.10.4.19. O total de filtros disponíveis na solução (não necessariamente para uso simultâneo) não deve ser inferior a 16.000;

8.10.4.20. A solução NGIPS deverá ser capaz de permitir a criação e uso de políticas de segurança granulares baseados nos seguintes métodos: Por NGIPS (todos os segmentos de rede de um IPS);

8.10.4.21. Por segmento físico, podendo selecionar o modo bi-direcional ou unidirecional (permitindo ativar a política de segurança nos sentidos de comunicação de A > B e de B > A [na mesma politica de segurança]. Ou com política de segurança dedicada de A > B e também de B > A); Por TAG de VLAN (802.1Q), de forma direcional e bi-direcional;

8.10.4.22. Por CIDR (Range de endereços IP);

8.10.4.23. Baseado no horário do dia. A solução NGIPS deverá ser capaz de detectar e bloquear ataques de reconhecimento de rede;

8.10.4.24. A solução NGIPS deverá prover filtros de detecção de aplicações tais como P2P, Online Games, permitindo a ativação de controles de banda;

8.10.4.25. Deverá possuir ferramenta para criação de filtros customizados, sendo que estes deverão permitir a customização de parâmetros tais como: Nome do filtro; Descrição do filtro; Protocolo, permitindo a criação de filtros de proteção baseados nos protocolos IPv4, ICMPv4, UDP, TCP, HTTP, IPv6 e ICMPv6;

8.10.4.26. Severidade do filtro, devendo possuir pelo menos 4 níveis; Customização da categoria do filtro;

8.10.4.27. Classe do filtro (devendo possuir pelo menos as classes DoS, Exploit, Virus e Acesso); Gatilhos de acionamento (triggers), onde parâmetros ou informações/dados contidos no streaming de rede serão utilizados como gatilho para validação de parâmetros adicionais da regra;

8.10.4.28. Detecção de payload, permitindo o uso de strings e expressão regular para detecção avançada de instruções no streaming de rede; Detecção de payload dentro do protocolo HTTP, permitindo o uso de strings e expressão regular para buscar e validar a existência de informações no cabeçalho HTTP, distinguindo métodos GET, POST, OPTIONS, PUT, DELETE, TRACE, CONNECT, HEAD, LOCK, UNLOCK, PROPFIND. Também deverá permitir a validação de dados específicos em URI, URI PATH, URI Target, Header e Payload;

8.10.4.29. Criação de customizações a nível TCP, sendo possível definir portas de origem e destino, além de validação de flags TCP;

8.10.4.30. A solução NGIPS ofertada deverá suportar processamento de tráfego assimétrico;

8.10.4.31. Deverá ser possível colocar a solução em modo bypass total forçado;

8.10.4.32. A solução NGIPS deverá possuir Machine Learning, ou seja, deverá possuir filtros que implementem Machine Learning na detecção de, por exemplo, conteúdo obfuscado em HTML associado/relacionado a exploit kits;

8.10.4.33. Deverá possuir filtros de gerenciamento de tráfego, ou seja, deverá ser possível criar regras para controlar o tráfego no sentido de A para B, de B para A, liberando o tráfego (com inspeção de riscos de segurança), liberando o tráfego (sem inspecioná-lo, confiando na conexão), bloqueando o tráfego, e também permitindo a criação de políticas de controle de banda, permitindo limitar, por exemplo, determinado fluxo de dados de rede a 100kbps;

8.10.4.34. A solução de NGIPS deverá possuir controles de proteção contra ataques de DDOS, atuando como um SYN PROXY; A solução de NGIPS deverá possuir filtros que detectem a tentativa de uso de TOR, TeamViewer;

8.10.4.35. A solução de NGIPS deverá detectar e bloquear tráfego Skype; A solução de NGIPS deverá detectar e permitir o bloqueio de tunelamento de conexões DNS;

8.10.4.36. A solução de NGIPS deverá possuir assinatura que permita a validação de requisições HTTP 2.0;

8.10.4.37. A solução de NGIPS deve bloquear nativamente a transferência de arquivos maliciosos via FTP; A solução deve detectar ataques baseados em SSL, como por exemplo detectar o uso de certificados SSL/TLS maliciosos. Atualizações de Segurança A solução de NGIPS ofertada precisa entregar detalhes sobre a cobertura para vulnerabilidades Microsoft reportadas nos últimos 12 meses;

8.10.4.38. O fabricante da solução NGIPS deve prover estatísticas do número de vulnerabilidades de dia zero descobertas nos últimos 5 anos.;

8.10.4.39. O fabricante da solução NGIPS deverá possuir times de pesquisa de vulnerabilidades de dia zero e de riscos de segurança, com pelo menos 1500 pesquisadores, sejam contratados ou parceiros, sendo que deverão ser apresentadas estatísticas dos últimos 3 anos de vulnerabilidades pesquisadas e descobertas. O fabricante deverá estar entre os Top 5 maiores pesquisadores do mundo nos relatórios publicados pela entidade Frost & Sullivan (Analysis of the Global Public Vulnerability Research);

8.10.4.40. A solução NGIPS deverá suportar atualizações automáticas dos filtros/assinaturas, possuindo frequência de atualizações mínima semanal (fabricante deverá entregar 1 atualização por semana); Sempre que a solução NGIPS atualizar-se, o novo pacote de atualizações deverá conter descritivo visualizável na própria solução (console local do NGIPS ou gerenciamento centralizado), indicando quais filtros foram incluídos, quais foram modificados e quais foram removidos. O mesmo deve ocorrer para os filtros de ameaças (malwares), sendo exigidos os mesmos parâmetros para permitir o acompanhamento e monitoramento dos novos filtros adicionados pela solução. Correlação de Informações e Consultas em Nuvem Reputação de Endereços IP, DNS e

URLs;

8.10.4.41. A solução NGIPS ofertada precisa permitir o bloqueio de tráfego baseado na reputação do endereço de IP de origem da conexão, de destino da conexão, através da reputação de DNS e URLs;

8.10.4.42. O serviço de reputação deverá contar com categorias tais como: Malware, Botnet, Spyware, SPAM, TOR, Web, Application Attackers, P2P e Network Worm; Deverá ser possível criar exceções baseadas em domínio e endereços IP, assim como deverá ser possível estabelecer as políticas de reputação individuais para cada perfil de segurança em uso no ambiente;

8.10.4.43. A base de reputação IP deverá suportar IPv4 e IPV6;

8.10.4.44. A base de reputação IP deverá ser baseada em informações do próprio fabricante, e também permitir o uso de bases terceiras;

8.10.4.45. Os filtros de reputação de IP deverão atuar tanto no sentido inbound quanto outbound;

8.10.4.46. As políticas de reputação deverão permitir a customização de ações tanto para bloquear ou permitir determinados acessos;

8.10.4.47. Deverá ser possível criar filtros de controle de acesso inbound e outbound baseados em geolocalização. Proteção Avançada Contra Ameaças A solução NGIPS deverá possuir funcionalidade que permita a identificação e proteção contra atividades maliciosas relacionadas a virus e spywares, no sentido inbound e outbound;

8.10.4.48. A solução NGIPS deverá possuir assinaturas de proteção contra malwares;

8.10.4.49. As assinaturas de malware deverão detectar a infiltração, exfiltração e comunicação com servidores de comando e controle através da inspeção do tráfego de rede;

8.10.4.50. A solução deverá ser capaz de interromper atividades maliciosas tais como ransomware, fuga de dados, click fraud, etc;

8.10.4.51. Deverá bloquear ameaças do tipo drive-by-downloads;

8.10.4.52. Deverá detectar atividades de comunicação com servidores de comando e controle de botnets;

8.10.4.53. Os filtros de malware deverão ser atualizados de forma regular pelo fabricante da solução. Alta Disponibilidade A solução de NGIPS deve suportar a operação de forma redundante, com possíveis cenários de operação Ativo-Passivo e AtivoAtivo;

8.10.4.54. A gerência da solução deve permanecer ativa em caso de indisponibilidade dos NGIPS e possui cenários de alta disponibilidade;

8.10.4.55. A solução NGIPS ofertada deverá suportar fontes do tipo hot-swappable;

8.10.4.56. A solução NGIPS deverá suportar software bypass; Em caso de atualizações ou reinicializações do NGIPS, a solução não deverá gerar nenhuma interrupção de rede. Gerenciamento Centralizado A solução NGIPS precisa suportar ser gerenciada de maneira centralizada por solução fornecida pelo mesmo fabricante;

8.10.4.57. A solução de gerenciamento centralizado entregue deverá permitir o gerenciamento de pelo menos 4 equipamentos NGIPS, sendo possível efetuar os mesmos níveis de configuração existentes na solução NGIPS;

8.10.4.58. A solução NGIPS deverá permitir integração com ferramentas de monitoramento de rede e SIEM tais como, HP ArcSight, além de permitir o envio de alertas por e-mail notificando incidentes de segurança;

8.10.4.59. A solução de gerenciamento centralizado deverá possuir um painel de monitoramento de eventos, contendo pelo menos as estatísticas dos principais filtros acionados, principais atacantes, principais alvos dos ataques etc.;

8.10.4.60. A solução de gerenciamento centralizado deverá permitir a integração com dispositivos de rede, tais como switchs e roteadores, com recursos que permitam alterar a configuração de VLAN de portas de rede, e desligar determinada porta de um switch de rede. Este recurso poderá ser utilizado para contenção de incidentes internos de segurança;

8.10.4.61. A solução de gerenciamento centralizado deverá possuir API que permita soluções externas, como o próprio SIEM, a interagir com a solução NGIPS, devendo permitir pelo menos a adição e remoção de endereços IP suspeitos em listas de reputação, e permitindo adicionar e remover endereços IP suspeitos da quarentena dos NGIPS;

8.10.4.62. A solução de gerenciamento centralizado deverá possuir recurso para relacionar relatórios de testes de penetração realizados no ambiente da empresa, permitindo comparar tais relatórios com políticas de

segurança em uso, indicando quais regras ou filtros são necessários ativar para alinhar a política de segurança com as vulnerabilidades identificadas no ambiente;

8.10.4.63. A solução deverá possuir suporte nativo a pelo menos as seguintes ferramentas: Qualys, Nessus e Nexpose; A solução de gerenciamento centralizado deverá possuir módulo de relatórios próprio, possuindo templates que indiquem os principais riscos de segurança detectados no ambiente, contando com pelo menos 20 modelos pré-estabelecidos.

8.10.4.64. Deverá ser possível agendar o envio destes relatórios, sendo exigidos no mínimo os seguintes formatos de arquivo: PDF, DOCX, XLS, CVS e XML; A solução de gerenciamento centralizado deverá suportar o gerenciamento paralelo de pelo menos 4 IPS. A solução ofertada deverá estar dimensionada para atender o exigido neste edital, com crescimento suportado previsto para até 20 NGIPS;

8.10.4.65. A solução de gerenciamento centralizado deverá permitir a integração com soluções de Sandboxes (detecção de ameaças desconhecidas) de modo a permitir que URLs contendo executáveis sejam analisados e testados por soluções de sandboxes que devem ser do próprio fabricante, a fim de identificar novas ameaças direcionadas ao ambiente. Indicadores como endereços IP e DNS relacionados a novas ameaças devem ser passíveis de bloqueio através da própria solução NGIPS (solução de sandbox deverá fazer o feedback dos indicadores relacionados a novas ameaças);

8.10.4.66. A solução de gerenciamento centralizado deverá possuir dashboard que permita a adição ou remoção de painéis que serão utilizados no monitoramento do ambiente, indicando os hosts comprometidos, hosts vulneráveis que sofreram ataques, lista de objetos suspeitos com quantidades de hits identificados;

8.10.4.67. A solução de gerenciamento centralizado deverá permitir a integração com serviços de diretório, tendo suporte aos métodos de autenticação CAC, RADIUS, TACACS+ e Active Directory, além de autenticação local (para uso enquanto solução não é integrada com restante da infraestrutura);

8.10.4.68. A solução deverá ser fornecida em modo de alta disponibilidade, tendo pelo menos 2 nós de redundância; Quando implementado em modo alta disponibilidade, a solução de gerenciamento centralizado deverá permitir a operação usando IP Virtual;

8.10.4.69. A solução de gerenciamento deverá possuir API que permita que soluções terceiras interajam podendo por exemplo quarantenar determinado endereço IP, desquarentenar determinado endereço IP, inserir e remover endereços IP de uma lista de reputação;

8.10.4.70. A solução de gerenciamento centralizado deverá atuar como ponto central para o gerenciamento de políticas de IPS, devendo possuir versionamento de políticas, capacidade de rollback, além de capacidade de importação e exportação de configurações.

8.10.4.71. Solução de visibilidade de superfície de ataques (ITEM 7) Deseja-se uma abordagem de avaliação de risco semi-quantitativa que forneça os benefícios de abordagens quantitativas e qualitativas. Uma comparação de riscos com outras organizações deve estar disponível para evitar os problemas.

8.10.4.72. A plataforma deve fornecer as três abordagens de análise: "Orientada por Ameaças, Ativos/Impactos e Vulnerabilidades". Análise rigorosa, a plataforma deve fornecer análises baseadas em gráficos para fornecer uma maneira eficaz de considerar as muitas relações muitos-para-muitos.

8.10.4.73. A análise de risco deve ser contínua e automatizada. A plataforma deve fornecer um índice global de risco. A plataforma deve fornecer sugestões sobre as ações de remediação mais importantes para reduzir o risco geral.

8.10.4.74. A plataforma também deve fornecer um índice de risco com base nas configurações de produtos integrados do fornecedor para reduzir o risco induzido por erros humanos. A gestão da superfície de ataque deve ser integrada na plataforma, fornecendo informações sobre Dispositivos Internos, Ativos Voltados para a Internet, Contas e Aplicações na Nuvem. Deve ser fornecido um painel para exibir todos os usuários/dispositivos com Alto Risco para tomada de ações. As fontes de dados devem incluir sensores de Rede, Ponto de extremidade, Web, Móvel e Email.

8.10.4.75. Devem ser suportadas fontes de dados de terceiros para análises adicionais a nível de identidade, como Azure AD, Office 365, AD local. Devem ser suportadas fontes de dados de terceiros para análises adicionais a nível de dispositivo, como Qualys, Nessus e Tenable.

8.10.4.76. Deseja-se ingestão de dados de terceiros de Firewall (Fortinet/Palo Alto/Cisco) e Portais da Web (Forcepoint/Zscaler/Cisco Umbrella/Symantec ProxySG). A plataforma deve detectar a conta de um usuário na dark web.

8.10.4.77. A plataforma deve fornecer informações sobre contas de usuários que apresentaram atividades

anômalas de alto risco ou que foram especificamente alvo de campanhas de e-mail maliciosas.

8.10.4.78. A plataforma deve detectar vulnerabilidades exploráveis do sistema operacional no ponto de extremidade. A plataforma deve detectar vulnerabilidades exploráveis do aplicativo no ponto de extremidade.

8.10.4.79. A plataforma deve indicar se a exploração está sendo explorada globalmente e, nesse caso, em que nível (Alto/Médio/Baixo).

8.10.4.80. A plataforma deve fornecer insights sobre o uso do armazenamento em nuvem (OneDrive/SharePoint/Outlook/Teams) pela conta que pareça anormal em comparação com o uso normal de outras contas da empresa. A plataforma deve exibir a localização geográfica e o número de vezes que seus usuários ou dispositivos acessaram o aplicativo em nuvem em um determinado dia.

8.10.4.81. A plataforma deve informar padrões de comportamento e preferências de usuário anormais em nível de dispositivo e usuário.

8.10.4.82. A plataforma deve fornecer um guia para reduzir fatores de risco detectados.

8.10.4.83. A plataforma deve permitir definir um objetivo de redução de risco. Visualizar um resumo dos eventos de risco que você deve remediar para alcançar o objetivo selecionado e alterar o status dos eventos de risco. Visualizar informações sobre os ativos que foram mais impactados por cada evento de risco.

8.10.4.84. A plataforma deve permitir as seguintes ações para responder a riscos: Desativar/Ativar conta do usuário - Forçar logout - Redefinir senha - Isolar/Restaurar Endpoint - Monitorar tentativas de login - Monitorar/Bloquear/Desbloquear/Permitir aplicativo interno - Bloquear/Desbloquear/Permitir Acesso a aplicativos ou URLs em nuvem.

8.10.4.85. A plataforma deve avaliar o risco de aplicativos em nuvem acessados pelos usuários pelo menos com base nos seguintes critérios: Conformidade com padrões (por exemplo, CSA STAR LEVEL, ISO, NIST) Recursos de segurança (por exemplo, autenticação multifator, proteção contra DoS) Cabeçalhos de segurança (por exemplo, x-frame-options, política de segurança de conteúdo) Violacões de segurança ou outros eventos que possam indicar um serviço comprometido Escudo de Privacidade UE-EUA/Suíça-EUA FINRA RGPD GLBA HIPAA/HITECH.

8.10.5. **SERVIÇO DE SUPORTE PRO ATIVO, CORRETIVO E PARA RESPOSTA A INCIDENTES (ITEM 5)**

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

8.10.5.2. Todo o Serviço de Suporte deverá ser prestado por profissional certificado pelo Fabricante da Solução, em nível compatível com a prestação do serviço.

8.10.5.3. Deverá ser apresentado comprovação da certificação dos profissionais responsáveis no ato da assinatura do contrato.

8.10.5.4. Deverá disponibilizar um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução ofertada; deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução.

8.10.5.5. **Suporte Proativo:**

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

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

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

8.10.5.5.4. Deverá realizar avaliações regulares de riscos para identificar possíveis vulnerabilidades e pontos fracos nos sistemas e, implementar medidas corretivas com base nos resultados das avaliações de riscos;

8.10.5.5.5. Realizar auditorias regulares para garantir que as melhores práticas e os controles de segurança estejam operacionais e, utilizar resultados de auditorias para implementar melhorias contínuas;

8.10.5.5.6. A CONTRATADA deverá apresentar relatório contendo as ações adotadas para a solução do

problema.

8.10.5.6. **Suporte Corretivo:**

8.10.5.6.1. Este componente concentra-se na solução de problemas ou incidentes. O suporte corretivo atua de forma ágil para restabelecer a funcionalidade normal do sistema, minimizando impactos negativos e mantendo a continuidade operacional;

8.10.5.6.2. Serviço Especializado de Suportes corretivo para 36 (trinta e seis) meses. Serviço de Suporte especializado para ajustes, correções e configurações da solução a ser fornecida. Neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução;

8.10.5.6.3. A contratada deverá: Implementar um sistema de abertura de chamados, para registrar, rastrear e priorizar incidentes e requisições de suporte;

8.10.5.6.4. Conforme detalhado no item 8.10;

8.10.5.6.5. Atribuir números de caso exclusivos para facilitar a comunicação e o acompanhamento;

8.10.5.6.6. Garantir disponibilidade 24/7 para responder a incidentes críticos. Deverá apresentar relatório contendo as ações adotadas para a solução do problema.

8.10.5.7. **Resposta a Incidentes:**

8.10.5.7.1. O serviço de resposta a incidentes deverá lidar com eventos imprevistos, como violações de segurança, falhas críticas ou interrupções inesperadas. deverá ser realizada por profissionais especializados e certificados pelo fabricante;

8.10.5.7.2. Deverá realizar investigações para determinar a natureza, origem e impacto de incidentes de segurança;

8.10.5.7.3. Desenvolver planos de mitigação e estratégia de recuperação para minimizar o impacto de incidentes;

8.10.5.7.4. Elaborar relatórios detalhados sobre os incidentes, incluindo ações tomadas e recomendações de melhorias.

8.10.6. **SERVIÇO DE IMPLANTAÇÃO (ITEM 6)**

8.10.6.1. Nesta etapa, compreende-se a instalação e configuração da solução contratada, contados a partir da emissão da Ordem de Serviço (OS);

8.10.6.2. O serviço de implantação abrange integralmente as fases essenciais para a integração, instalação e configuração da solução contratada, alinhando-se precisamente com as especificações técnicas e requisitos predefinidos. Esta abordagem abarca desde o planejamento inicial até a conclusão efetiva, assegurando uma transição suave dos processos existentes para a nova solução;

8.10.6.3. O Plano de Implantação assume a forma de um documento fundamental que consolida a estratégia para instalação, configuração e entrega da solução contratada. Sua importância reside em orientar e alinhar as atividades, garantindo eficiência e uma implementação adequada da solução conforme os requisitos estabelecidos;

8.10.6.4. O documento deverá conter no mínimo os requisitos de ambiente tecnológicos necessários para a instalação das licenças, cronograma e detalhamento das atividades a serem realizadas, topologia do ambiente pós instalação da solução, matriz de responsabilidade, plano de comunicação;

8.10.6.5. Durante esta etapa, a equipe da Contratada deverá estar presente nos horários de instalação definidos pelo Contratante. As atividades de instalação e configuração poderão ser realizadas, conforme necessário, em horário comercial, período noturno ou final de semana;

8.10.6.6. O Contratante disponibilizará a infraestrutura de hardware e software necessária e já existente em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução durante esta etapa.

8.10.7. **SERVIÇO DE CAPACITAÇÃO E REPASSE DE CONHECIMENTO (ITEM 7)**

8.10.7.1. Repasse de conhecimento, na forma de treinamento para técnicos, de forma virtual, para 1 (uma) turma, com carga horária mínima de 40 (quarenta) horas, abrangendo todos os softwares integrantes da suíte de solução de segurança;

8.10.7.2. O conteúdo programático abordará tanto aspectos teóricos quanto práticos, contemplando de maneira abrangente todos os módulos relevantes da solução de segurança;

8.10.7.3. O treinamento pode ser segmentado de acordo com o produto a ser instalado no ambiente tecnológico, contemplando, no mínimo, os seguintes módulos:

8.10.7.3.1. Instalação do módulo de gerenciamento central; Instalação do software de Endpoint Protection em estações de trabalho e servidores;

8.10.7.3.2. Descrição e configuração de todas as funcionalidades contratadas da solução;

8.10.7.3.3. Melhores práticas utilizadas no mercado para otimização dos softwares e suas funcionalidades.

8.10.7.3.4. A carga horária mínima estabelecida será de 40 (quarenta) horas, divididas em expedientes de 4 horas por dia, no horário comercial.

8.10.7.3.5. A contratada é responsável por fornecer apostilas em formato digital que contemplem o conteúdo referente ao produto, oferecendo suporte ao aprendizado prático e teórico dos participantes;

8.10.7.4. Este treinamento visa capacitar adequadamente os usuários finais, garantindo que compreendam e aproveitem plenamente as funcionalidades da solução de segurança. O enfoque prático e teórico, aliado às melhores práticas do mercado, promove uma formação abrangente e eficaz.

9. MODELO DE EXECUÇÃO DO OBJETO

9.1. Execução dos Serviços

9.1.1. A CONTRATANTE no uso de suas atribuições legais nomeará Fiscais de Contrato, sendo indicado pelo representante da área requisitante o servidor que possui conhecimento técnico do objeto da contratação e designado pelo Secretário de Estado da Saúde - SESAU, mediante a Portaria, para acompanhar e fiscalizar a execução contratual, responsabilizando-se pela verificação do efetivo cumprimento das obrigações pactuadas e respectivo ateste das faturas/notas fiscais, juntamente com a comissão de recebimento em conformidade com o Art. 117º da Lei Federal n.º 14.133 de 1º Abril de 2021 e acórdão nº. 4/2006 - TCU e Anexo I **-** Guia de Fiscalização dos Contratos, deste Termo de Referência.

9.1.2. A prestação dos serviços deverá estar dentro dos parâmetros e rotinas estabelecidas, fornecendo todos os produtos, peças, acessórios, componentes eletrônicos, materiais, utensílios e equipamentos em quantidade, qualidade e tecnologia adequadas, com observância às recomendações aceitas pelas boas técnicas, normas e legislação vigente e em quantidades necessárias à boa execução dos serviços.

9.1.3. A CONTRATANTE fiscalizará a execução do serviço contratado e verificará o cumprimento das especificações solicitadas, no todo ou em parte, no sentido de corresponderem ao desejado ou especificado.

9.1.4. A fiscalização pela CONTRATANTE **,** não desobriga a CONTRATADA de sua responsabilidade quanto à perfeita execução do objeto deste instrumento;

9.1.5. A ausência de comunicação por parte da CONTRATANTE referente a irregularidades ou falhas, não exime a CONTRATADA das responsabilidades determinadas no Contrato;

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

9.1.7. A CONTRATADA se obriga a permitir que auditoria interna da CONTRATANTE e/ou auditoria externa por ela indicada tenham acesso a todos os documentos que digam respeito ao objeto deste instrumento, inclusive auditoria a ser realizada na usina de incineração.

9.1.8. A CONTRATANTE realizará avaliação da qualidade do atendimento, dos resultados concretos dos esforços sugeridos pela CONTRATADA e dos benefícios decorrentes da política de preços por ela praticada.

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

9.1.10. A Contratada deverá possuir estoque mínimo de peças para realizar o serviço da manutenção corretiva quando houver a necessidade de troca das mesmas.

9.1.11. Os serviços deverão ser executados em horários que não interfiram no bom andamento da rotina de funcionamento da contratante;

9.1.12. **Requisitos Temporais**

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

9.1.13. **Requisitos de Segurança e Privacidade**

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

9.1.14. **Garantia da disponibilidade, integridade, confidencialidade e sigilo das informações:**

9.1.14.1. A empresa CONTRATADA deve assegurar a disponibilidade, integridade, confidencialidade e sigilo dos documentos e informações relacionados ao contrato e aos serviços prestados. Qualquer pessoa que cause perdas e danos à CONTRATANTE ou a terceiros poderá ser responsabilizada legalmente.

9.1.15. **Devolução de informações confidenciais:**

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

a) término ou rompimento do contrato; ou

b) solicitação da CONTRATANTE. A formalização entre as partes é necessária nesses casos.

9.1.16. **Utilização de ferramentas de proteção e segurança de informações:**

9.1.16.1. É imprescindível o uso de ferramentas de proteção e segurança de informações para evitar acesso não autorizado aos sistemas e softwares. Isso se aplica tanto aos sistemas sob responsabilidade direta da CONTRATADA quanto aos disponibilizados à CONTRATANTE, mesmo que por meio de link.

9.1.17. **Realização de alterações para sanar problemas de segurança ou vulnerabilidade:**

9.1.17.1. Quando formalmente solicitado pela CONTRATANTE, a CONTRATADA deve priorizar e realizar alterações para solucionar possíveis problemas de segurança ou vulnerabilidade nos sistemas ou softwares utilizados para a execução do serviço contratado.

9.1.18. **Comunicação de atualizações ou mudanças na configuração dos serviços:**

9.1.18.1. A CONTRATADA deve informar formalmente e de forma tempestiva ao CONTRATANTE sobre quaisquer necessidades de atualização ou mudança na configuração dos serviços prestados.

9.1.19. **Prestação de esclarecimentos e informações:**

9.1.19.1. É responsabilidade da CONTRATADA prestar os esclarecimentos necessários à CONTRATANTE, bem como fornecer informações sobre a natureza e o andamento dos serviços executados ou em execução.

9.1.20. **Garantia da integridade e disponibilidade dos documentos e informações:**

9.1.20.1. A empresa CONTRATADA deve garantir a integridade e disponibilidade dos documentos e informações que estão sob sua guarda em função do contrato. Caso ocorram perdas ou danos, a CONTRATADA será responsabilizada.

9.1.21. **Confidencialidade das informações:**

9.1.21.1. A CONTRATADA não pode divulgar, mesmo que em caráter estatístico, quaisquer informações originadas na CONTRATANTE sem prévia autorização.

9.1.22. **Controle de acesso e identificação dos profissionais:**

9.1.22.1. O acesso às instalações da CONTRATADA onde os serviços serão realizados deve ser controlado e permitido apenas para pessoas autorizadas. Os profissionais da CONTRATADA devem estar devidamente identificados por crachás durante o trabalho. Qualquer profissional considerado inconveniente à boa ordem ou que viole as normas disciplinares da CONTRATANTE deve ser substituído imediatamente.

9.1.23. **Conhecimento e observância das normas disciplinares da CONTRATANTE:**

9.1.23.1. A CONTRATADA deve garantir que seus profissionais tenham conhecimento das normas disciplinares do CONTRATANTE e exijam sua fiel observância, especialmente em relação à utilização e segurança das instalações.

9.1.23.2. A CONTRATADA deve manter sigilo absoluto sobre todas as informações provenientes dos serviços realizados, documentos elaborados e informações obtidas dentro do ambiente da CONTRATANTE.

9.1.24. **Requisitos Legais**

9.1.24.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021 (Lei de Licitações e Contratos Administrativos), à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis;

9.1.25. **Prazo de início de atendimento para suporte técnico e manutenção pela garantia:** O início do atendimento deve seguir o que está especificado no acordo de nível de serviço presente no Termo de Referência.

9.2. **LOCAL DE ENTREGA:**

9.2.1. Os respectivos equipamentos serão entregues na Coordenadoria de Almoxarifado e Patrimônio, localizado na Rua Aparício Moraes, 4378 - Industrial, Porto Velho - RO, 76821-240, onde serão atestados pela respectiva conforme Portaria Comissão de Recebimento CAP/SESAU (0050062995).. Funcionamento de segunda a sexta-feira das 7h30min às 13h30min.

9.2.2. **Horário de entrega dos equipamentos/serviços**: A entrega dos equipamentos/serviços deve ocorrer entre as 07:30 e 13:30. É possível agendar uma data e hora específica previamente com a CONTRATANTE.

9.2.3. **Verificação da conformidade dos materiais entregues:** É responsabilidade da CONTRATANTE rejeitar, total ou parcialmente, os materiais entregues que não estejam de acordo com o objeto definido no Termo de Referência.

9.2.4. **Recebimento dos produtos:** O recebimento dos produtos será feito pela equipe designada pela CONTRATANTE. Esse recebimento ocorrerá de forma provisória no momento da entrega dos equipamentos e de forma definitiva após a instalação, configuração e teste da solução.

9.3. **PRAZO DA ENTREGA:**

9.3.1. O prazo para início dos serviços será de até 30 (trinta) dias contados a partir da última assinatura do contrato.

9.3.2. **Prazo de início de atendimento para suporte técnico e manutenção pela garantia:** O início do atendimento deve seguir o que está especificado no acordo de nível de serviço presente no Termo de Referência.

9.3.3. **Prazo de entrega e instalação:** O prazo de entrega e instalação deve estar de acordo com o que foi especificado no Termo de Referência. Caso não haja uma definição específica, o prazo padrão será considerado conforme a ordem de serviço.

9.3.4. A entrega deverá ocorrer conforme solicitação da Unidade de Saúde com definição da quantidade, no prazo máximo de 30 (trinta) dias corridos, após o recebimento da nota de empenho ou assinatura do contrato de fornecimento.

9.4. Os equipamentos deverão ser entregues de acordo com as especificações técnicas e demais disposições constantes em contrato, não sendo permitido à Comissão recebê-los fora das especificações pré-definidas.

9.4.1. Todo o material deverá ser entregue em embalagens individuais, em perfeito estado de conservação, lacrada e adequadas para proteger o conteúdo contra danos durante o transporte, desde o fornecedor até o local da entrega, sob condições que envolvam embarques, desembarques, transportes, por rodovias não pavimentadas, marítimos ou aéreos;

9.4.2. Os procedimentos de recebimento provisório e definitivo do objeto diretamente na unidade requisitante deve ser orientado e acompanhado pela Coordenadoria de Almoxarifado e Patrimônio-CAP/SESAU/RO, de forma a atender os padrões regulares de recebimento e demais encaminhamentos para incorporação do bem ao patrimônio público da Secretaria.

9.4.3. O objeto deverá ser indiscutivelmente novo e sem uso. Não serão aceitos equipamentos e materiais que tenham sido objeto de quaisquer processos de reciclagem e/ou recondicionamento e ainda, os que se apresentarem fora das embalagens originais de seus fabricantes.

9.5. **DA ENTREGA E DO RECEBIMENTO**

9.5.1. A entrega deverá ocorrer conforme solicitação via requisição da Secretaria de Saúde até o prazo máximo de 30 (trinta) dias, a contar da data de recebimento da Ordem de Fornecimento, Ordem de Serviço e/ou Nota de Empenho.

9.5.2. A empresa concorrente homologada deverá acusar o recebimento da Ordem de Fornecimento e/ou

Nota de Empenho para fornecimento em 48h (quarenta e oito horas), iniciar e comunicar à Administração as providências para cumprimento dos prazos subsequentes.

9.5.3. No caso de não confirmação de recebimento da requisição do objeto pela Secretaria de Estado da Saúde de Rondônia no prazo de 05 (cinco) dias, a requisição será dada como recebida.

9.5.4. A entrega ocorrerá em parcela única, sem parcelamento da entrega.

9.5.5. O recebimento do objeto será realizada por Comissão de Recebimento de Materiais e Serviços designada pela Secretaria de Estado da Saúde de Rondônia, da unidade requisitante e/ou da Coordenadoria de Almoxarifado e Patrimônio-CAP/SESAU/RO, ou ainda por comissão especificamente designada, à critério da Administração, conforme Art. 140, inciso II da Lei Federal nº 14.133/2021.

> "Art. 140. O objeto do contrato será recebido:
>
> II - em se tratando de compras:
>
> a) provisoriamente, de forma sumária, pelo responsável por seu acompanhamento e fiscalização, com verificação posterior da conformidade do material com as exigências contratuais;
>
> b) definitivamente, por servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências contratuais.
>
> § 1º O objeto do contrato poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.
>
> § 2º O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança da obra ou serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos pela lei ou pelo contrato.
>
> § 3º Os prazos e os métodos para a realização dos recebimentos provisório e definitivo serão definidos em regulamento ou no contrato.
>
> § 4º Salvo disposição em contrário constante do edital ou de ato normativo, os ensaios, os testes e as demais provas para aferição da boa execução do objeto do contrato exigidos por normas técnicas oficiais correrão por conta do contratado.
>
> § 5º Em se tratando de projeto de obra, o recebimento definitivo pela Administração não eximirá o projetista ou o consultor da responsabilidade objetiva por todos os danos causados por falha de projeto.
>
> § 6º Em se tratando de obra, o recebimento definitivo pela Administração não eximirá o contratado, pelo prazo mínimo de 5 (cinco) anos, admitida a previsão de prazo de garantia superior no edital e no contrato, da responsabilidade objetiva pela solidez e pela segurança dos materiais e dos serviços executados e pela funcionalidade da construção, da reforma, da recuperação ou da ampliação do bem imóvel, e, em caso de vício, defeito ou incorreção identificados, o contratado ficará responsável pela reparação, pela correção, pela reconstrução ou pela substituição necessárias."

9.5.6. A Contratante promoverá através de seus representantes, o acompanhamento e a fiscalização da entrega dos produtos sob os aspectos quantitativo e qualitativo, anotando as falhas detectadas e comunicando a Contratada as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte daquela através dos procedimentos de recebimento, que ocorrerão da seguinte forma:

9.5.7. **Provisoriamente** por servidor ou comissão designada pela Coordenadoria de Almoxarifado e Patrimônio-CAP/SESAU/RO, de forma sumária imediatamente depois de efetuada a entrega através de recibo aposto na nota fiscal. O recebimento provisório deve ser concluído dentro do prazo de até 05 (cinco) dias, devendo o CAP/SESAU/RO neste interim tomar as devidas providências para que ocorra o recebimento definitivo juntamente à unidade requisitante, a fim de se proceder a verificação da conformidade dos produtos com as especificações de forma integrada.

9.5.8. **Definitivamente** por Comissão de Recebimento de Materiais e Serviços designada da unidade requisitante, ou por comissão especificamente designada, depois de concluída a vistoria, encerrado o prazo de observação que não poderá exceder 10 (dez) dias, e, mediante termo detalhado que comprove adequação do objeto ao requerido e aprovado pela Administração, o atendimento das exigências contratuais e consequente aceitação.

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

9.5.10. Em fomento à assertividade na análise técnica do objeto a comissão de recebimento poderá dispor de avaliação complementar de setor especializado ou comissão especialmente designada, caso necessário, por sua conveniência e oportunidade.

9.5.11. Salvo disposição em contrário constante do edital ou de ato normativo, os ensaios, os testes e as demais provas para aferição da boa execução do objeto do contrato exigidos por normas técnicas oficiais

correrão por conta do contratado.

9.5.12. A Contratante poderá rejeitar no todo ou em parte os materiais entregues em desacordo com as especificações técnicas do objeto ou com as obrigações assumidas.

9.5.13. Se o fornecedor vencedor tiver comprovadamente dificuldades para entregar os materiais, dentro do prazo estabelecido, não sofrerá multa, caso informe oficialmente com antecedência de mínimo 03 (três) dias úteis, antes de esgotado o prazo inicialmente previsto, apresentando justificativa circunstanciada formal, que deverá ser encaminhada ao Secretário de Estado da Saúde que, por sua vez, decidirá a possibilidade de prorrogação do prazo, ou determinará a cominação das multas cabíveis, que ocorrerá a partir da efetiva notificação;

9.5.14. Se, após o recebimento provisório, for constatado que os materiais foram entregues de forma incompleta ou em desacordo com as especificações ou com a proposta, será interrompido o prazo de recebimento definitivo e suspenso o prazo de pagamento até que seja sanada a situação;

9.5.15. A empresa vencedora ficará obrigada a trocar, às suas expensas, o que for recusado por apresentar-se contraditório as especificações contidas no Termo de Referência;

9.5.16. O objeto deverá ser entregues de acordo com as especificações técnicas e demais disposições constantes no Termo de Referência, não sendo permitido a Comissão, receber os equipamentos fora das especificações pré-definidas.

9.5.17. O objeto deverá ser indiscutivelmente novo e sem uso. Não serão aceitos itens que tenham sido objeto de quaisquer processos de reciclagem ou recondicionamento. Deverão estar acondicionados em embalagem própria conforme ao fabricante, garantindo sua integridade.

9.5.18. A Contratada fica sujeito às sanções administrativas previstas, quando for o caso.

9.6. **DO LOCAL DE DESTINAÇÃO E UTILIZAÇÃO DOS BENS**

9.6.1. Os equipamentos e licenças de software devem ser entregues conforme disposto no Termo de Referência.

9.6.2. Os equipamentos serão destinados as unidades que compõem a Secretária de Estado da Saúde, sua distribuição será realizada pela Coordenadora de Tecnologia da Informação conforme necessidade da unidade requisitante.

9.7. **Local de Utilização:**

I - Coordenadoria de Tecnologia da Informação - **SESAU-CTI**: Rua Pio XII, 2986 - Bairro Pedrinhas Palácio Rio Madeira - Edifício Rio Machado 1° Andar , Porto Velho, RO CEP 76801470.

10. ESPECIFICAÇÃO DA GARANTIA DO PRODUTO

10.1. **Garantia** (ID SEI! 0055727564)

10.1.1. A garantia do produto será por 36 (trinta e seis) meses, conforme segue:

10.1.2. **Complexidade Técnica dos Equipamentos**

10.1.2.1. Equipamentos como **soluções de segurança avançada, servidores, sistemas NGIPS e endpoints** possuem componentes eletrônicos e software que exigem alta especialização para manutenção e suporte. A **garantia estendida** assegura que:

10.1.2.2. Falhas técnicas serão corrigidas por profissionais qualificados, mantendo o desempenho do sistema.

10.1.2.3. Haverá substituição de peças e componentes de hardware com padrões técnicos exigidos pelo fabricante.

10.1.2.4. As atualizações de software (patches de segurança, melhorias) serão implementadas sem custos adicionais durante o período da garantia.

10.1.3. **Vida Útil e Durabilidade do Equipamento**

10.1.3.1. O período de 36 meses da garantia estendida está alinhado à **vida útil esperada** de equipamentos de tecnologia. Isso significa:

10.1.3.2. Durante os primeiros anos, é comum que ocorram **falhas de hardware ou software** devido ao uso

contínuo e exigências operacionais.

10.1.3.3. A garantia estendida proporciona **proteção contra desgaste** ou mau funcionamento prematuro.

10.1.4. **Necessidade de Manutenção Preventiva e Corretiva**

10.1.4.1. Soluções avançadas exigem **manutenção contínua** para garantir a **operacionalidade** e **segurança do ambiente tecnológico**. A garantia estendida cobre:

10.1.4.2. **Manutenção preventiva**: inspeções periódicas para evitar falhas.

10.1.4.3. **Manutenção corretiva**: correção imediata em caso de falhas identificadas.

10.1.4.4. **Substituição de peças críticas**: sem custos adicionais para a administração.

10.1.5. **Redução do Risco Operacional**

10.1.5.1. Equipamentos como os mencionados no **item 03 (Solução de Segurança Avançada)** e demais soluções tecnológicas são **críticos** para a proteção da rede e continuidade das operações. A **garantia estendida**:

10.1.5.2. Mitiga riscos de **interrupção dos serviços**.

10.1.5.3. Reduz impactos financeiros e operacionais decorrentes de falhas no sistema.

10.1.5.4. Assegura a **disponibilidade contínua** do serviço.

10.1.5.5. **Suporte Técnico Especializado**

10.1.5.6. Fabricantes e parceiros certificados possuem equipes **altamente qualificadas** para atuar em falhas complexas. A garantia estendida:

10.1.5.7. Garante acesso a suporte técnico especializado.

10.1.5.8. Proporciona **respostas rápidas** para incidentes críticos.

10.1.5.9. Inclui **ferramentas exclusivas e diagnósticos avançados**, o que não é oferecido na garantia legal básica do CDC.

10.1.5.10. **Garantam a qualidade e continuidade do serviço**.

10.1.5.11. Sejam **proporcionais** ao objeto contratado.

11. VALOR MÁXIMO ESTIMADO UNITÁRIO E GLOBAL DA CONTRATAÇÃO

11.1. Foi utilizado como estimativa o Relatório de Preços 68244109 e validado pela Coordenadoria de Pesquisa e Análise de Preço (SUPEL-CPEAP)- (68573114), o qual obteve-se os valores abaixo:

11.1.1. Valor anual estimado: **R$ 21.660.280,76 (vinte e um milhões seiscentos e sessenta mil duzentos e oitenta reais e setenta e seis centavos);**

12. CLASSIFICAÇÃO ORÇAMENTÁRIA DA DESPESA (DOTAÇÃO ORÇAMENTÁRIA)

12.1. Conforme Informação nº 3785/2024/SESAU-NPPS (0052252474), segue abaixo a dotação orçamentária:

DESCRIÇÃO DA DESPESA			
OBJETO PROCESSUAL: Contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, visando atender às necessidades da Secretaria de Estado da Saúde de Rondônia, por um período de 01 (um) ano, podendo ser prorrogado, conforme a Lei Federal nº 14.133 de 1° de abril de 2021.			
Resposta ao:	Despacho (0052208255)		
PROGRAMA DE TRABALHO	**UNIDADE ATENDIDA**	**FONTE DE RECURSO**	**NATUREZA DA DESPESA**

PROGRAMA DE TRABALHO	UNIDADE ATENDIDA	FONTE DE RECURSO	NATUREZA DA DESPESA
17.012.10.126.1015.2064 - PROMOVER A GESTÃO DE T.I	Secretaria de Saúde	1.500.0.01002 - Recursos não vinculados de impostos - Saúde 2.500.0.01002 - Recursos não vinculados de impostos do exercício anterior - Saúde	3.3.90.39 - Outros Serviços de Terceiros - PJ 3.3.90.40 - Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica

12.2. Ressalta-se ainda que a aludida informação é exclusivamente para indicação da programação, cabendo a anuência de execução da despesa ao ordenador, desde que tenha, no momento dessa execução, recursos orçamentários e financeiros suficientes para o atendimento.

12.3. **Plano de Contratação Anual (PCA)**

12.3.1. conforme o Parecer nº 28/2026/SESAU-DIREX (70656134):

> **3. CONCLUSÃO E PARECER**
>
> Com base na análise dos autos e considerando o objeto em referência, a unidade demandante solicita autorização para realizar despesas não previstas na Programação Anual de Saúde de 2026, no valor estimado de R$ 7.749.301,17 (sete milhões, setecentos e quarenta e nove mil trezentos e um reais e dezessete centavos), conforme o Documento de Oficialização de Demanda nº 31/2024/SESAU-CTI, (0054733868), **conclui-se que é justificada.**
>
> Considera-se que a organizações estejam preparadas para enfrentar e responder a esses incidentes de forma adequada, protegendo tanto os dados de sua propriedade quanto aqueles que estão sob sua custódia.
>
> Considera-se que é fundamental investir em estratégias robustas de segurança da informação, incluindo a implementação de sistemas de detecção e prevenção de ameaças, atualizações regulares de software e hardware, treinamento e conscientização dos usuários, além de políticas de segurança claras e bem definidas. Além disso, é importante contar com equipes especializadas em segurança cibernética, capazes de identificar e responder rapidamente aos incidentes, minimizando danos e prejuízos.
>
> Pelo exposto**, AUTORIZO** o prossequimento dos autos para realizar despesas não prevista na Programção Anual de 2026, conforme DESPACHO/SESAU-CITI (70618017).

13. TRATAMENTO DIFERENCIADO A MPE

13.1. Em razão do potencial comprometimento na execução do objeto licitatório devido à indivisibilidade do item, a cota de 25% prevista na Lei Complementar nº 123, de 14 de dezembro de 2006, não será aplicada nesta contratação.

13.2. Igualmente, o critério de exclusividade para Microempresas (ME) e Empresas de Pequeno Porte (EPP) não será implementado, visto que o valor da contratação supera o limite de R$ 80.000,00, conforme disposto no Art. 48, Inciso I, da mencionada lei.

13.3. Sendo assim, não se aplicará o tratamento favorecido às microempresas, empresas de pequeno porte, sociedades cooperativas referidas no Art. 16 da Lei nº 14.133/2021, ao agricultor familiar, ao produtor rural pessoa física e ao microempreendedor individual (MEI), conforme os parâmetros estabelecidos na Lei Complementar nº 123/2006 e no Decreto nº 8.538/2015. Dado que a licitação não se enquadra nos critérios do Art. 47 da Lei nº 123/2006, por não incluir itens divisíveis ou participação exclusiva de ME/EPP, aplica-se o disposto no Art. 49, Inciso III, da referida legislação.

14. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

14.1. O fornecedor será selecionado por meio da realização de procedimento de **LICITAÇÃO**, na modalidade **PREGÃO**, sob a forma **ELETRÔNICA**, modo de disputa **ABERTO**, com adoção do critério de julgamento pelo **MENOR VALOR GLOBAL.**

14.2. Essa escolha é fundamentada na necessidade de garantir uma solução integrada e de alta qualidade que atenda de forma eficaz às exigências de segurança e operacionais da SESAU. Esta abordagem assegura que todos os aspectos críticos da contratação sejam considerados de maneira abrangente, promovendo a escolha da solução mais adequada e eficiente.

14.3. **DA CONTRATAÇÃO DE PESSOA FÍSICA**

14.3.1. Em atenção ao art. 34, inciso XIV do Decreto Estadual nº 28.874/2024, justifica-se a exclusão de participação de pessoas físicas no presente processo, considerando que a Administração Pública tem a obrigação de garantir a segurança e a qualidade dos serviços que contrata. Em razão disso, é importante que os contratados tenham a capacidade técnica e a estrutura necessária para prestar o serviço de forma adequada.

14.3.2. Desta forma, as pessoas físicas, em geral, não possuem a mesma capacidade técnica e estrutura que empresas especializadas. Por isso, a participação de pessoas físicas na contratação pretendida pode colocar em risco a segurança e a qualidade dos serviços a serem prestados.

14.3.3. Assim, a vedação da participação de pessoas físicas em tais processos de contratação visa garantir que os serviços sejam prestados com a qualidade, segurança e continuidade necessárias, minimizando riscos e assegurando o cumprimento das obrigações contratuais, fiscais e regulatórias.

15. DA PROPOSTA

15.1. A proposta deverá ser elaborada de acordo com a Solicitação e Aquisição de Materiais/Serviços - **SAMS** sendo que o julgamento das propostas será considerado o critério de **MENOR VALOR GLOBAL** , para fins de obtenção da proposta mais vantajosa para Administração.

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

15.3. Caberá ao contratante, depreender indício de que o levantamento prévio de preços padece de fragilidade, a exemplo da disparidade entre o preço inicialmente previsto.

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

15.5. Decorridos 90 (noventa) dias da data da entrega das propostas, sem convocação para a contratação, ficam os licitantes liberados dos compromissos assumidos

15.6. A inobservância do prazo fixado para a entrega das respostas e/ou informações solicitadas em eventual diligência ou ainda o envio de informações ou documentos considerados insuficientes/incompletos ocasionará a desclassificação da proposta.

15.7. Relativamente a oferta de preços, conforme dispõe o art. 82, inciso III, não serão admitidos preços diferentes, uma vez que para as pesquisas de preços, não incluiu-se preços do comércio LOCAL/DE MUNICÍPIOS DISTINTOS, como forma de obter uma estimativa que contemple os custos necessários, em razão dos aspectos relacionados a localização geográfica.

15.8. PROSPECTO/FOLDER/CATÁLOGO/ENCARTES/FOLHETOS TÉCNICOS EM PORTUGUÊS OU LINKS OFICIAIS QUE O DISPONIBILIZEM, onde constem as especificações técnicas e a caracterização dos mesmos, permitindo a consistente avaliação dos itens.

16. DA EXIGÊNCIA DE AMOSTRA

16.1. Para o objeto deste TR, a aceitação das propostas não está condicionada a apresentação de amostras, considerando a relevância do produto e o dispêndio financeiro necessário, sendo que a avaliação do produto será verificada por ocasião da entrega, estando tais produtos sujeitos a recusa de recebimento definitivo, caso não corresponda às condições e especificações mínimas definidas nos autos.

17. REQUISITOS DE HABILITAÇÃO

17.1. 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, nos termos do Decreto Federal n° 11.802, de 28 de Novembro de 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 17 de Outubro 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.

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

17.2. **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, estadual e/ou municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

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

e) 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.

17.3. **RELATIVOS À QUALIFICAÇÃO ECONÔMICO - FINANCEIRA**

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

b) Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, ou o Balanço de Abertura caso a licitante tenha sido constituída em menos de um ano, devidamente autenticado ou registrado no órgão competente, para que o(a) Pregoeiro(a) possa aferir se esta possui Patrimônio Líquido (licitantes constituídos há mais de um ano) ou Capital Social (licitantes constituídos há menos de um ano), de 5% (cinco por cento) do valor total estimado.

17.3.1. Tais requisitos estão plenamente alinhados ao art. 69 da Lei 14.133/21, que prevê a comprovação da capacidade econômico-financeira em contratações de natureza contínua.

17.3.2. A exigência do percentual de 5% é adequada e proporcional à complexidade do objeto e encontra respaldo no §4º do art. 69 da Lei 14.133/2021, que permite a fixação de limite de até 10%. O percentual adotado é suficiente para demonstrar a capacidade financeira da empresa, sem restringir de forma excessiva a competitividade.

17.3.3. Ressalta-se, ainda, que a Administração promoverá a análise da capacidade econômico-financeira das licitantes com base na documentação contábil apresentada, inclusive nos casos de empresas em recuperação judicial, nos termos do art. 69, §1º, da Lei nº 14.133/2021, a fim de verificar a viabilidade econômica e a aptidão para o cumprimento das obrigações contratuais, vedando-se a aceitação de índices incompatíveis com a realidade de mercado.

17.3.4. Portanto, a exigência de qualificação econômico-financeira é medida necessária para assegurar a execução contínua, segura e regular dos eventual aquisição de Servidor de Hiperconvergência e serviços de instalação, resguardando o interesse público e evitando riscos de descontinuidade que possam comprometer as condições sanitárias das unidades de saúde do Estado.

17.3.5. OBS: As exigências de qualificação econômico-financeira encartadas acima estão em harmonia com o que prevê o art. 69 da Lei 14.133/21 sendo necessário, para garantir que a (s) vencedora (as) detenha (am) condições econômicas para executar o futuro contrato.

17.4. **DECLARAÇÕES**

a) A empresa deverá apresentar declaração de que não emprega menor de 18 anos, conforme disposto no inciso 33 do art. 7º da Constituição Federal.

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

17.4.1. 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.

17.4.2. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

17.4.3. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

17.4.4. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir.

17.4.5. 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.

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

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

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

17.4.9. 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

17.4.10. Atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

17.4.11. 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.

17.4.12. 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.

17.5. **OUTRAS DECLARAÇÕES**

17.5.1. Art. 63, Lei 14.133/21. Na fase de habilitação das licitações serão observadas as seguintes disposições:

> IV - será exigida do licitante declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.
>
> § 1º Constará do edital de licitação cláusula que exija dos licitantes, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais,

nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

17.6. **DOCUMENTAÇÃO RELATIVOS À QUALIFICAÇÃO TÉCNICA:** (ID SE! 0055863665)

17.6.1. **1. Parcela de Maior Relevância**

17.6.1.1. A parcela de maior relevância do objeto está associada à Solução de Segurança Avançada para Mitigação de Ameaças na Rede (Item 03), uma vez que este representa o componente mais complexo e tecnicamente exigente do edital. Tal complexidade justifica a necessidade de maior atenção, considerando sua criticidade para a proteção e integridade das operações na rede.

17.6.1.2. Pela Complexidade Técnica, Criticidade para a Proteção e Integridade da Rede, podemos definir em resumo que: **Solução de Segurança Avançada** é a parte mais importante e difícil do contrato, devido à **tecnologia avançada** que envolve e à **necessidade de proteger de forma eficaz a rede**, que é fundamental para as operações da organização. A complexidade e a criticidade desse item exigem **uma atenção extra** na implementação e gestão da solução

17.6.2. **2. Documentação Relativos à Qualificação Técnica**

17.6.2.1. Deverá apresentar Atestado(s) ou Certidão(ões) de Capacidade Técnico-operacional, emitido(s) por pessoa jurídica de direito público ou privado, comprovando que a licitante forneceu, instalou e configurou solução de segurança em características e **pelo menos 10% do item 3,** Solução de Segurança Avançada para Mitigação de Ameaças na Rede, uma vez que este representa o componente mais complexo e tecnicamente exigente do edital

17.6.2.2. O(s) Atestado(s) ou Certidão(ões) de Capacidade Técnico-operacional devem ser compatíveis em condições e características com o objeto da contratação e deverão conter as seguintes informações mínimas:

a) nome e cargo da pessoa que os assina;

b) quantitativo associado ao fornecimento; e

c) valor e/ou Contrato(s) associado(s) à da prestação dos serviços.

17.6.3. **3. Parcerias e Certificações de Fabricantes**

17.6.3.1. Apresentar Declaração Formal de que **antes da assinatura do contrato entregará.**

a) Parceria ativa com os fabricantes das soluções propostas, comprovada por cartas de parceria ou autorização de revenda/implementação.

b) Certificações de parceria que garantam a capacitação técnica e o suporte direto do fabricante.

18. DO CONTRATO E SUA EXECUÇÃO

18.1. Conforme disposto no art. 95, inciso II, da Lei 14.133/2021, em caso de compras com entrega imediata e integral dos bens adquiridos e dos quais não resultem obrigações futuras, inclusive quanto a assistência técnica, independentemente de seu valor, o instrumento de contrato poderá ser substituído por instrumento hábil, neste caso a nota de empenho de despesas.

18.2. Portanto, para os objetos deste certame que apresentem garantia estendida, será celebrado contrato.

18.3. **Convocação e Celebração do contrato**

18.3.1. Oficialmente convocada pela Administração com vistas à celebração do Termo Contratual é dado à contratada o prazo de até 05 (cinco) dias úteis, contado da data da ciência ao chamamento, pela Secretaria de Estado da Saúde, para no local indicado, firmar o instrumento de Contrato.

18.3.2. Após análise dos documentos supramencionados e convocação pela Secretaria de Estado da Saúde, será dado à contratada o prazo de até 05 (cinco) dias úteis, para firmar o instrumento de Contrato.

18.3.3. Será designada Comissão devidamente nomeada por meio de Portaria, pelo Gestor da Pasta, para recebimento, análise e julgamento da documentação.

18.4. **Da Formalização e Execução do Contrato**

18.4.1. A Administração convocará regularmente o interessado para assinar o termo de contrato, aceitar ou retirar o instrumento equivalente, dentro do prazo e condições estabelecidos, sob pena de decair o direito à

contratação, sem prejuízo das sanções previstas no art. 90 da lei n° 14.133/21.

18.4.2. O prazo de convocação poderá ser prorrogado uma vez, por igual período, quando solicitado pela parte durante o seu transcurso e desde que ocorra motivo justificado aceito pela Administração.

18.4.3. É facultado à Administração, quando o convocado não assinar o termo de contrato ou não aceitar ou retirar o instrumento equivalente no prazo e condições estabelecidos, convocar os licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pelo primeiro classificado, inclusive quanto aos preços atualizados de conformidade com o ato convocatório, ou revogar a licitação independentemente da cominação prevista no art. 90 §2º da lei n° 14.133/21.

18.5. **DA REPACTUAÇÃO, DO REAJUSTE E DA REVISÃO DO CONTRATO**

18.5.1. Considerando as necessidades de garantia do equilíbrio econômico-financeiro dos contratos da administração pública deve ser atendido e preceituado nos parâmetros dos Art. 150 ao Art. 168 do Decreto nº 28.874 de 25 de janeiro de 2024.

18.5.2. Para os fins previstos de restabelecimento do equilíbrio econômico-financeiro fica estabelecido como data-base a apresentação da proposta ou previsões restritas, nos casos de repactuação e orçamento de obras, ainda deve ser observado o prazo para apresentação do pedido, expedido no Art. 151 do Decreto nº 28.874/2024.

18.5.3. No que tange aos índices de reajuste a serem aplicados para fins do restabelecimento econômico-financeiro, adotar-se-á o que for mais vantajoso para a Administração, devendo ser observado a existência de índice próprio para o objeto contratual, conforme Art. 156 do Decreto nº 28.874/2024.

18.5.4. No caso concreto aplicar-se o Índice Nacional de Preços ao Consumidor Amplo - IPCA, para fins de reajuste e restabelecimento do equilíbrio econômico-financeiro.

18.5.5. **DO REAJUSTE**

18.5.6. Conforme previsão no arts. 154 ao 156 do Decreto nº 28.874/24.

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

18.5.8. Dito isto, ao final dos 12 (doze) meses iniciais de vigência do contrato ou do último reajustamento levado a efeito no contrato, uma vez que solicitada pela contratada, os reajustes serão aplicados com base no Índice Nacional de Preços ao Consumidor Amplo (IPCA) ou em outro índice que eventualmente o substitua, observando-se, anualmente, os critérios legais e contratuais aplicáveis.

18.5.9. O reajuste em sentido estrito, espécie de reajuste nos contratos de obra, fornecimento ou serviço continuado sem dedicação exclusiva de mão de obra, consiste na aplicação de índice de correção monetária estabelecido no contrato, que retratará a variação efetiva do custo de produção, admitida a adoção de índices específicos ou setoriais.

18.5.10. O prazo para resposta ao pedido de restabelecimento do equilíbrio econômico-financeiro, será de até 15 (quinze) dias úteis, a contar do recebimento da solicitação.

18.5.11. **DA REPACTUAÇÃO**

18.5.11.1. Conforme previsão nos art. 157 ao 162 o Decreto nº 28.874/24.

18.5.11.2. Haja vista a presente contratação não tratar-se de Dedicação Exclusiva de Mão de Obra (DEMO), não se aplica as condições para atendimento dos referidos artigos do Decreto nº 28.874/24, para fins de Repactuação do Contrato.

18.5.11.3. Dessa forma, a repactuação não será aplicada a pretensa contratação.

18.5.12. **REVISÃO**

18.5.12.1. Conforme previsão no arts. 163 ao 164 do Decreto nº 28.874/24.

18.5.12.2. A revisão contratual será concedida, a pedido da contratada, para promover o reequilíbrio econômico-financeiro da avença, diante da ocorrência de fatos imprevisíveis, ou previsíveis com consequências incalculáveis, retardadores ou impeditivos da execução do contrato, ou, ainda, em caso de força maior, caso fortuito ou fato do príncipe, configurando álea econômica extraordinária e extracontratual.

18.5.12.3. O pedido de revisão de contrato deverá ser instruído com os seguintes documentos:

I - requerimento da contratada devidamente assinado pelo seu responsável;

II - planilha de custos demonstrando a equação inicial do contrato;

III - planilha de custos demonstrando a equação atual do contrato;

IV - documentação hábil demonstrando a ocorrência de fatos imprevisíveis, fatos previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do ajustado, ou, ainda, caso de força maior, caso fortuito ou fato do príncipe, que configurem álea econômica extraordinária e extracontratual;

V - ato do ordenador de despesa do órgão ou entidade que decidir pelo reconhecimento das circunstâncias que autorizam a revisão do contrato;

VI - pesquisa de preços praticados no mercado a fim verificar se o preço reequilibrado permanece atendendo o pressuposto fundamental da licitação, se for o caso.

18.5.12.4. Parágrafo único. A revisão será formalizada por meio de termo aditivo.

18.5.12.5. O prazo para resposta ao pedido de revisão para restabelecimento do equilíbrio econômico-financeiro, será de até 15 dias úteis, a contar do recebimento da solicitação.

18.6. **DA INEXECUÇÃO E DA RESCISÃO CONTRATUAL:**

18.6.1. As obrigações das partes, bem como os direitos e deveres da Contratante e da Contratada, estão estabelecidos no presente Termo e no contrato a ser firmado entre as partes, conforme os termos e condições descritas nos documentos que integram este procedimento licitatório.

18.6.2. A **Contratante** poderá, em qualquer momento, **extinguir o contrato**, **total ou parcialmente**, nas seguintes situações:

a) **Por conveniência administrativa**, caso entenda que o contrato não mais oferece vantagem ou interesse para a Administração, conforme o disposto no art. 106, inciso III da Lei nº 14.133/2021, observando-se o prazo e as condições estabelecidas na legislação;

b) **Por falta de créditos orçamentários**, quando a Administração não dispor dos recursos financeiros necessários para a continuidade do contrato, conforme também previsto no mencionado artigo da Lei nº 14.133/2021.

18.6.3. A rescisão ou extinção do contrato, conforme estabelecido na Lei nº 14.133/2021, será realizada mediante **notificação formal** à **Contratada**, respeitando os prazos e as condições de aviso prévio, quando aplicáveis, conforme estabelecido no **art. 106 da Lei nº 14.133/2021**.

18.6.4. O contrato poderá ser rescindido pela Contratante a qualquer tempo, no todo ou em parte, por conveniência administrativa, mediante notificação, através de ofício diretamente ou via postal com prova de recebimento, através de parecer fundamentado, assegurado, todavia os direitos adquiridos pela Contratada;

18.6.5. O inadimplemento de quaisquer das cláusulas e disposições deste instrumento, implicara na sua rescisão ou na sustação do pagamento relativo aos serviços já efetuados, a critério da Contratante, independentemente de qualquer procedimento judicial;

18.6.6. A inexecução total ou parcial do contrato enseja a sua rescisão, com as consequências contratuais e as previstas em lei ou regulamento.

18.6.7. Constituem motivo para rescisão de contrato:

I - O não cumprimento de cláusulas contratuais, especificações, projetos ou prazos.

II - O cumprimento irregular de cláusulas contratuais, especificações, projetos e prazos.

III - A lentidão do seu cumprimento, levando a Administração a comprovar a impossibilidade da conclusão do serviço ou do fornecimento, nos prazos estipulados.

IV - O atraso injustificado no início do serviço ou fornecimento.

V - A paralisação do serviço ou do fornecimento, sem justa causa e prévia comunicação à Administração.

18.7. **Prazo de Início da Vigencia do Contrato**

18.7.1. O prazo para início da vigência do contrato será contado a partir da última assinatura do contrato.

18.8. **Vigência Contratual**

18.8.1. O contrato terá um prazo de vigência de **01 (um) ano** a partir da data da última assinatura, podendo ser prorrogado até o limite previsto no art. 107 da Lei 14.133/21, de acordo com a necessidade e justificativa da CONTRATANTE e acordo entre as partes.

19. REQUISITOS DA CONTRATAÇÃO

19.1. A Contratação em tela deverá obedecer, no que couber, ao disposto na Lei Federal nº 14.133 de 1° de Abril de 2021 e suas alterações, bem como as seguintes normas:

a) Instrução Normativa nº 58, de 08 de agosto de 2022 - Ministério da Economia;

b) Decreto Estadual nº 28.874, de 25 de janeiro de 2024;

c) Lei Federal n° 13.709, de 14 de agosto de 2018.

19.2. **POSSÍVEIS IMPACTOS AMBIENTAIS e CRITÉRIOS SUSTENTABILIDADE**

19.2.1. Embora os impactos ambientais diretos de uma solução de segurança cibernética possam ser menores em comparação a outros tipos de contratações, é fundamental a inclusão de critérios ambientais nos requisitos de contratação, como a exigência de certificações verdes para data centers, a gestão responsável de resíduos eletrônicos e a preferência por fornecedores que adotem práticas sustentáveis, pode garantir que a contratação atenda aos princípios de sustentabilidade ambiental.

19.2.1.1. **Certificações Ambientais**

a) Certificações de Data Centers: Exigir que os fornecedores possuam certificações como LEED (Leadership in Energy and Environmental Design) ou ISO 14001, que atestam práticas de construção e operação ambientalmente responsáveis.

b) Certificações de Sustentabilidade: Preferir fornecedores que têm certificações de sustentabilidade reconhecidas, como o Energy Star, que garantem eficiência energética.

19.2.1.2. **Gestão de Resíduos Eletrônicos**

a) Reciclagem e Descarte Responsável: Exigir que os fornecedores adotem políticas claras de reciclagem e descarte de equipamentos eletrônicos, garantindo que eles não sejam enviados para aterros sanitários de forma inadequada.

b) Reutilização de Equipamentos: Incentivar a reutilização e a recuperação de equipamentos, promovendo práticas de economia circular.

19.2.1.3. **Eficiência Energética**

a) Uso de Fontes de Energia Renovável: Preferir fornecedores que utilizem energia renovável em suas operações, como solar ou eólica, e que apresentem planos para aumentar a proporção de energia limpa utilizada.

b) Otimização de Consumo Energético: Avaliar o consumo energético das soluções propostas e exigir relatórios sobre como os fornecedores planejam reduzir a pegada de carbono.

19.2.1.4. **Transparência e Relatórios**

a) Relatórios de Sustentabilidade: Solicitar que os fornecedores apresentem relatórios de sustentabilidade anuais que detalhem suas práticas ambientais e metas de redução de impactos.

b) Políticas de Sustentabilidade: Pedir uma declaração clara das políticas ambientais e sociais do fornecedor, incluindo objetivos e estratégias.

19.2.1.5. **Inovação e Desenvolvimento Sustentável**

a) Investimento em Tecnologias Verdes: Avaliar o comprometimento do fornecedor com inovações que minimizam o impacto ambiental, como soluções de segurança que exigem menos recursos computacionais.

b) Desenvolvimento de Produtos Sustentáveis: Incentivar o desenvolvimento de softwares e soluções que ajudem a otimizar recursos e reduzir o consumo de energia.

19.2.1.6. **Formação e Conscientização**

a) Treinamento em Sustentabilidade: Exigir que os fornecedores realizem treinamentos para suas equipes sobre práticas sustentáveis e a importância da responsabilidade ambiental.

b) Campanhas de Conscientização: Incentivar fornecedores a participar ou criar campanhas que promovam a sustentabilidade dentro e fora da organização.

19.3. **BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO**

19.3.1. **Solução de Proteção de Endpoints com Abordagem Proativa para Resposta Eficaz a Incidentes**

19.3.1.1. Resultados Esperados:

I - Proteção Aprimorada: Redução significativa do risco de malware, ransomware e outras ameaças.

II - Detecção Proativa: Identificação e mitigação de ameaças antes que causem danos significativos.

III - Resposta Rápida a Incidentes: Capacidade de isolar e remediar incidentes rapidamente, minimizando o impacto.

IV - Relatórios Detalhados: Fornecimento de análises detalhadas sobre eventos de segurança, facilitando a conformidade e a auditoria.

19.3.2. **Solução de Proteção de Servidores com Abordagem Proativa para Resposta Eficaz a Incidentes**

19.3.2.1. Resultados Esperados:

I - Segurança dos Dados: Proteção dos dados armazenados nos servidores contra acessos não autorizados e vazamentos.

II - Alta Disponibilidade: Manutenção da disponibilidade dos serviços, mesmo durante tentativas de ataque.

III - Detecção de Ameaças: Monitoramento contínuo e detecção de atividades suspeitas nos servidores.

IV - Remediação Automática: Implementação de ações automáticas para neutralizar ameaças detectadas.

19.3.3. **Solução de Segurança Avançada para Mitigação de Ameaças na Red**

19.3.3.1. Resultados Esperados:

I - Visibilidade Completa: Monitoramento em tempo real de todo o tráfego de rede, detectando atividades anômalas.

II - Resposta Imediata: Capacidade de bloquear e mitigar ameaças automaticamente.

III - Proteção Contínua: Defesa contínua contra ameaças conhecidas e desconhecidas através de análise comportamental.

IV - Integração com Outras Soluções: Operação coordenada com outras ferramentas de segurança para uma abordagem unificada.

19.3.4. **Solução de Prevenção de Intrusão de Próxima Geração (NGIPS)**

19.3.4.1. Resultados Esperados:

I - Prevenção de Intrusões: Identificação e bloqueio de tentativas de intrusão em tempo real.

II - Atualizações Frequentes: Atualizações constantes de assinaturas e algoritmos de detecção para lidar com novas ameaças.

III - Análise Profunda: Capacidade de analisar o tráfego de rede em profundidade para detectar ataques sofisticados.

IV - Redução de Falsos Positivos: Melhoria na precisão da detecção, minimizando alarmes falsos e reduzindo a carga de trabalho da equipe de segurança.

19.3.5. **Serviço de Suporte Proativo, Corretivo e para Resposta a Incidentes**

19.3.5.1. Resultados Esperados:

I - Manutenção Preventiva: Redução do número de incidentes através de atividades de manutenção preventiva.

II - Correção de Problemas: Resolução rápida e eficaz de problemas e falhas identificadas.

III - Resposta a Incidentes: Suporte especializado e rápido durante incidentes de segurança, minimizando o impacto.

IV - Documentação e Relatórios: Fornecimento de documentação detalhada e relatórios de todos os incidentes e atividades de suporte.

19.3.6. **Serviço de Implantação**

19.3.6.1. Resultados Esperados:

I - Configuração Ótima: Garantia de que todas as soluções sejam configuradas corretamente para máxima eficácia.

II - Integração Suave: Integração das novas soluções com as infraestruturas existentes sem interrupções significativas.

III - Teste e Validação: Realização de testes abrangentes para garantir que todas as soluções funcionem como esperado.

IV - Transferência de Conhecimento: Treinamento inicial para a equipe sobre as novas soluções implementadas.

19.3.7. **Serviço de Capacitação e Repasse de Conhecimento**

19.3.7.1. Resultados Esperados:

I - Treinamento da Equipe: Capacitação da equipe interna para operar e gerenciar as novas soluções de segurança.

II - Melhoria Contínua: Desenvolvimento de habilidades avançadas na equipe para identificar e responder a ameaças emergentes.

III - Documentação: Fornecimento de manuais e guias detalhados para referência futura.

IV - Autossuficiência: Aumentar a autonomia da equipe interna, reduzindo a dependência de suporte externo para tarefas rotineiras.

19.3.8. Cada um desses itens contribui para uma postura de segurança cibernética mais robusta e resiliente, reduzindo a vulnerabilidade da organização a incidentes de segurança e aumentando a eficiência operacional da equipe de Tecnologia da Informação.

19.3.9. Atrair o maior número de licitantes para a disputa.

19.3.10. Obter a proposta mais vantajosa para a Administração Pública.

20. DAS OBRIGAÇÕES

20.1. DA CONTRATADA:

20.1.1. Além daquelas exigidas na Lei Federal 14.133/2021, e, Lei Estadual 28.874/2024, deverá:

20.1.2. Responsabilizar-se integralmente pelos materiais adquiridos, nos termos da legislação vigente;

20.1.3. Entregar o objeto da aquisição nas especificações contidas neste Termo de Referência;

20.1.4. Entregar o objeto na forma e prazo estipulados neste Termo de Referência;

20.1.5. Entregar o objeto nas quantidades indicadas pelo órgão requisitante;

20.1.6. Os materiais que não atenderem exigências deste edital não serão aceitos e recebidos, devendo ser substituídos imediatamente.

20.1.7. Não promover substituição do produto empenhado, sem anuência expressa da contratante;

20.1.8. Entregar os produtos em embalagem íntegra, sob pena de rescisão do ajuste, independentemente das combinações legais cabíveis;

20.1.9. No Pregão Eletrônico não há quantidade mínima a ser adquirida, tampouco obrigatoriedade de

aquisição de todo o quantitativo licitado, e, em caso de eventuais contratos de fornecimento decorrentes da Aquisição, a Contratada se obriga a aceitar as supressões nas quantidades inicialmente previstas respeitando os limites da Lei 14.133/21 e os parâmetros da Lei 28.874/2024, tendo como base os preços constantes da(s) proposta(s) Contratada(s), diante de necessidade comprovada da Administração.

20.1.10. Responsabilizar-se pela substituição do produto entregue em desconformidade com este Termo de Referência, ou impossibilitados de uso devido, perda ou deterioração de suas características, devendo ser trocados no prazo máximo de 20 (vinte) dias uteis, contados a partir de comunicação formal do responsável. O ônus de todas as despesas decorrentes da efetivação da troca será da Contratada;

20.1.11. Manter durante toda execução da Ata, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

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

20.1.13. Considerar em todas as etapas de vinculação e arcar efetivamente com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas e todos os tributos incidentes, sem qualquer ônus à Contratante, devendo efetuar os respectivos pagamentos na forma e nos prazos previstos em Lei;

20.1.14. Indicar um preposto devidamente habilitado, com poderes para representá-lo em tudo o que se relacionar com o fornecimento objeto;

20.1.15. Ficarão a cargo da empresa vencedora os custos de frete, impostos, taxas e etc., que venham a incidir sobre a aquisição objeto deste Termo de Referência;

20.1.16. No momento da entrega a empresa deverá apresentar relação com o material entregue e nota fiscal, contendo marca, especificação e quantidade. Os preços propostos deverão incluir fretes e demais custos diretos e indiretos, inclusive os resultantes da incidência de quaisquer impostos, tributos, contribuições ou obrigações trabalhista, fiscais e previdenciárias a que estiver sujeito.

20.1.17. Garantir a qualidade dos produtos ofertados conforme este Termo de Referência e estipulado nas normas técnicas e regulamentações especializadas relacionadas ao objeto de fornecimento;

20.1.18. CUMPRIR E FAZER CUMPRIR, todas as diretrizes, normas, regulamentos impostas por este Termo de Referência e seus ANEXOS.

20.1.19. A contratada deverá reparar, corrigir, remover, reconstituir ou substituir, às suas expensas, os materiais que forem rejeitados, parcial ou totalmente, por apresentarem vícios, defeitos, incorreções, no prazo máximo de 20 (vinte) dias úteis a contar da data do recebimento da comunicação do fato.

20.1.20. A Contratada se obriga a aceitar acréscimos ou supressões nas quantidades inicialmente previstas respeitando os limites do artigo 125 da Lei 14.133/21 e suas alterações, tendo como base os preços constantes da(s) proposta(s) contratada(s), diante de necessidade comprovada da Administração.

20.1.21. É obrigação da Contratada manter durante toda execução do contrato compatibilidade com as obrigações por ela assumida, bem como todas as condições de habilitação e qualificação exigidas na licitação.

20.1.22. A futura contratada deverá cumprir as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social.

20.2. **DA CONTRATANTE:**

20.2.1. Além daquelas constantes no Termo de Referência e aquelas determinadas por leis, decretos, normas técnicas, regulamentos e demais dispositivos legais, a CONTRATANTE se obrigará:

20.2.2. Fiscalizar, acompanhar, conferir e avaliar o objeto deste Termo de Referência, através de representantes designados pela SESAU, conforme dispõe a Lei Nº 14.133/2021. Promover através da comissão nomeada, o acompanhamento e a fiscalização da entrega e recebimento dos produtos sob os aspectos quantitativo e qualitativo, anotando as inconformidades ou falhas detectadas e comunicando a Contratada as ocorrências de quaisquer fatos que, a seu critério, exijam medidas corretivas por parte daquela;

20.2.3. Garantir o cumprimento de todas as cláusulas contratuais ao bom desempenho do objeto desta contratação;

20.2.4. Aplicar as penalidades regulamentares cabíveis, quando for o caso;

20.2.5. Devolver o material caso não esteja dentro das especificações constantes do presente Termo de Referência, ou impossibilitados de uso devido por perda ou deterioração de suas características;

20.2.6. Efetuar o pagamento à contratada de acordo com as condições de preços e prazos estabelecidos

neste Termo de Referência.

20.2.7. Durante o processo licitatório a Contratante deverá verificar a conformidade das propostas em relação aos requisitos estabelecidos neste termo de referência e no edital.

20.2.8. A quantidade mínima a ser solicitada de cada item será de 10% do valor previsto para cada item. Não há obrigatoriedade de aquisição de todo o quantitativo licitado.

20.2.9. Serão considerados pela Contratante para o presente processo licitatório somente os requisitos da contratação indispensáveis, necessários e suficientes à escolha da melhor solução para a Administração Pública, observadas as leis e regulamentações específicas aplicáveis, bem como padrões mínimos de qualidade e desempenho.

21. DA GARANTIA CONTRATUAL

21.1. Para fiel execução dos compromissos aqui ajustados a CONTRATADA prestará prévia garantia de 5% (cinco por cento) do valor do valor inicial do contrato, como previsto no art. 98 da lei 14.133/2021;

21.2. A critério da autoridade competente, em cada caso, poderá ser exigida, mediante previsão no edital, prestação de garantia nas contratações de obras, serviços e fornecimentos.

21.3. A CONTRATADA poderá optar por uma das modalidades de garantia previstas no art. 96, § 1°, da Lei 14.133/2021;

21.4. A CONTRATADA terá o prazo de 10 (dez) dias, prorrogáveis por igual período, posteriores à assinatura do contrato, para apresentação da garantia contratual;

21.5. A garantia prestada pelo contratado será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, atualizada monetariamente, conforme art. 100 da Lei 14.133/2021.

22. DA SUBCONTRATAÇÃO

22.1. A subcontratação será necessária conforme Art. 42, XXIII, do Decreto 28.874/2024, adicionalmente, está em conformidade com o Art. 75, §1º, e Art. 124 da Lei nº 14.133/2021, que preveem condições específicas para subcontratação. Essas condições deverão incluir comprovação de capacidade técnica e alinhamento com os princípios da Administração Pública. Neste caso a subcontratação se faz devidamente fundamentada pelos seguintes motivos (ID SEI! 0055451477 e 0055727564):

a) Falta de Experiência Interna : Se sua equipe interna não tiver a experiência ou especialização necessária em cibersegurança, o subcontratado pode trazer acesso a profissionais especializados e especializados.

b) Recursos limitados : Quando há limitações de recursos, como pessoal, tempo ou orçamento, o subcontratado pode ser uma forma eficaz de obter o nível necessário de proteção sem sobrecarregar sua equipe interna.

c) Necessidade de Soluções Avançadas : Caso sua empresa precise de tecnologias avançadas e infraestrutura robusta que seriam caras de se implementar e manter internamente, a terceirização pode ser mais econômica.

d) Escalabilidade : Se seu negócio está crescendo rápido e sua infraestrutura de TI precisa escalar rapidamente, as empresas de cibersegurança podem ajudar a acompanhar esse crescimento de forma eficaz.

e) Monitoramento Contínuo : Para garantir vigilância e resposta a incidentes em tempo real, 24 horas por dia, sete dias por semana, subcontratando você garante que haja uma equipe dedicada a supervisionar e reagir rapidamente a ameaças.

22.2. Será admitida a subcontratação dos serviços de garantia e assistência técnica, desde que previamente autorizada por escrito pelo contratante, por empresa comprovadamente autorizada pelo fabricante dos equipamentos;

22.2.1. É permitida a subcontratação parcial do objeto, pela contratada à outra empresa, a cessão ou transferência parcial do objeto licitado, nos termos do art. 122 do §2º da Lei Nº 14.133/2021;

> "Art. 122. Na execução do contrato e sem prejuízo das responsabilidades contratuais e legais, o contratado poderá subcontratar partes da obra, do serviço ou do fornecimento até o limite autorizado, em cada caso, pela Administração.

§ 1º O contratado apresentará à Administração documentação que comprove a capacidade técnica do subcontratado, que será avaliada e juntada aos autos do processo correspondente.

§ 2º **Regulamento ou edital de licitação poderão vedar, restringir ou estabelecer condições para a subcontratação**. (...)".

22.2.2. Fica autorizada a subcontratação para os itens **05 - Serviço de suporte pro ativo, corretivo e para resposta a incidentes** e **06 - Serviço de implantação** no tópico 3. **Definição do Objeto c/c 3.2 descrição detalhada do objeto citados nesse Termo de referência**, nas seguintes condições:

22.2.3. É vedada a subcontratação total do objeto do contrato, sendo vedada a subcontratação dos serviços que foram utilizados na qualificação técnica da empresa Contratada, relativos às parcelas de maior relevância técnica e de valor significativo.

22.2.4. A subcontratação depende de autorização prévia por parte do Contratante, que deverá emitir anuência de forma expressa, a quem incumbe avaliar se o subcontratado cumpre os requisitos de qualificação técnica necessários para a execução do objeto.

22.2.5. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da Contratada pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades da subcontratada, bem como responder perante o Contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

22.2.6. É vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na contratação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau.

23. MODELO DE GESTÃO DE CONTRATO

23.1. A resolução N. 01/2024/SESAU-SC (0048586915) estabelece a necessidade de normatização da gestão e fiscalização dos contratos no âmbito da Secretaria de Estado da Saúde de Rondônia, em conformidade com a Lei nº 14.133, de 1º de abril de 2021.

23.2. Esta resolução impõe a obrigatoriedade de que a gestão e a fiscalização dos contratos sejam realizadas seguindo as diretrizes especificadas na própria resolução N. 01/2024/SESAU-SC.

RESOLVE:

Art. 1º – Aprovar o Manual de Gestão e Fiscalização de Contratos Administrativos (SEI nº 0047523841) elaborado pela comissão designada na Portaria 4150 (0041658066) de 11 de setembro de 2023.

Art. 2º – Instituir no Âmbito da Secretaria de Estado da Saúde a obrigatoriedade da utilização do Manual de Gestão e Fiscalização de Contratos Administrativos (0048122701) na Gestão e Fiscalização dos contratos.

Art. 3º – Deverão ser observados os procedimentos estabelecidos no Manual de forma cumulativa com os demais procedimentos previstos na legislação.

Art. 4º – Esta Resolução entrará em vigor a partir da data de sua publicação.

23.3. Desta forma, a gestão e a fiscalização dos contratos serão realizados conforme o Manual de Gestão e Fiscalização de Contratos Administrativos (0052173211), Anexo I deste Termo de Referência.

24. PAGAMENTO

24.1. O pagamento para o serviço será efetuado de forma INTEGRAL, conforme o serviço prestado/fornecido, mediante a apresentação de Nota Fiscal, emitidas pela Contratada, devidamente atestadas pela Administração.

24.2. Insta salientar que o pagamento seguirá conforme estipulado no Art. 188 do Decreto n.º 28.874/2024, ou seja:

Art. 188. As solicitações de pagamento deverão ser formalizadas pelo contratado por meio de pedido subscrito pelo seu representante legal, indicando o número do contrato administrativo e os dados para pagamento, instruído com os seguintes documentos:
I - nota fiscal, fatura ou documento equivalente que ateste o cumprimento do objeto, indicando o valor e o período da prestação do serviço ou do fornecimento;
II - certidão de regularidade fiscal perante a Fazenda Estadual;
III - certidão de regularidade previdenciária e trabalhista, além dos documentos comprobatórios do cumprimento das respectivas obrigações nos termos do art. 24 deste Decreto, nos casos de contrato de prestação de serviços contínuos com dedicação exclusiva (ou predominante) de mão de obra;

IV - comprovante de cumprimento de obrigações previdenciárias, nos casos de contratos de obra;
V - medição realizada pela fiscalização do contrato, nos casos de obra e serviços de engenharia, e de contratos submetidos ao referido regime de pagamento por medição;
VI - comprovante de atingimento de metas e respectivo impacto percentual no caso de remuneração variável;
VII - comprovante de percentual de economia produzida, nos casos de contratos de eficiência.
§ 1º Os documentos apresentados deverão ser atestados pela fiscalização do contrato que emitirá parecer conclusivo sobre a viabilidade do pagamento diante do cumprimento do objeto e efetiva correspondência com o valor cobrado, devendo ser autuado processo administrativo no qual serão incluídos cópia do contrato e eventuais termos aditivos, cópia da nota de empenho e mapa de controle de execução contratual.
§ 2º Atestado o cumprimento do objeto do contrato pela fiscalização e a correta instrução do processo, após autorização do ordenador, os autos deverão ser remetidos ao setor responsável pela liquidação da despesa e efetivação do pagamento.
§ 3º Em caso de não cumprimento do inciso II, o contratado deverá ser instado a se manifestar sobre a possibilidade de compensação do crédito com o débito existente, caso em que os autos deverão ser remetidos ao órgão fazendário para as providências cabíveis, com prévia oitiva da Procuradoria - Geral do Estado em caso de débito inscrito em dívida ativa.
§ 4º Em caso de não concordância com a compensação, imediatamente após o pagamento da contraprestação, os autos deverão ser remetidos à Procuradoria-Geral do Estado para adoção das providências cabíveis para recuperação do crédito estadual.
§ 5º Em caso de não cumprimento dos incisos III e IV, o pagamento deverá ser retido até a regularização, observadas as diretrizes fixadas neste Decreto.

24.3. Por conseguinte, a nota fiscal deverá ser emitida em favor do:

a) **Fundo Estadual de Saúde - RO.**

b) **CNPJ Nº: 00.733.062/0001-02.**

c) Endereço: Av. Farquar, 2986, Complexo Rio Madeira, Edifício Rio Machado (Entrada pela PIO XII) – Bairro: Pedrinhas – CEP: 76.801-470 - Porto Velho/RO.

24.4. No corpo da Nota Fiscal/Fatura deverá conter:

a) A descrição detalhada do item;

b) Valor unitário do objeto de acordo com a nota de empenho;

c) Identificação de Número do Processo e identificação da Nota de empenho;

d) Identificação do Banco (código), da Agência Bancária, do Número da Conta Bancária, para fins de pagamento, bem com, das correções fiscais e contábeis, se for o caso.

24.5. O pagamento será efetuado conforme recebimento e atesto dos seguintes documentos:

a) Nota Fiscal devidamente devidamente atestadas pela Administração, conforme disposto no no art. 140, inciso II, alíneas "a" e "b" da Lei 14.133/2021;

b) Comprovação da entrega do item com o termo de recebimento assinado pela comissão designada em portaria;

24.6. O pagamento decorrente de contratações públicas será feito após a habilitação para pagamento, no prazo máximo de **15 (quinze) dias úteis**, consoante o disposto no art. 190 do Decreto 28.874/2024.

24.7. No caso das Notas Fiscais apresentarem erros ou dúvidas quanto à exatidão, ou documentação, a Administração Pública poderá pagar apenas a parcela incontroversa no prazo fixado para pagamento, ressalvado o direito da empresa de representar para cobrança, as partes controvertidas com devidas justificativas, nestes casos, a Administração Pública terá o prazo de até 05 (cinco) dias úteis, a partir do recebimento, para efetuar análise e pagamento devidamente atestadas pela Administração.

24.8. Na hipótese da contratada não estar regular perante a Fazenda Estadual, o contratado será instado a se manifestar sobre a possibilidade de compensação do crédito com o débito existente, caso em que os autos serão remetidos ao órgão fazendário para as providências cabíveis, com prévia oitiva da Procuradoria - Geral do Estado em caso de débito inscrito em dívida ativa. Em caso de não concordância com a compensação, imediatamente após o pagamento da contraprestação, os autos serão remetidos à Procuradoria-Geral do Estado para adoção das providências cabíveis para recuperação do crédito estadual.

24.9. Em caso de descumprimento das obrigações trabalhistas e previdenciária, o pagamento será retido até a regularização, sem prejuízo das sanções cabíveis.

24.10. Não será efetuado qualquer pagamento, salvo as parcelas incontroversas, à (s) empresa (s) Contratada (s) enquanto houver pendência de liquidação da obrigação financeira em virtude de penalidade ou inadimplência contratual.

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

$I = \frac{(TX/100)}{365}$
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.

24.12. Ocorrendo erro no documento da cobrança, este será devolvido e o pagamento será sustado para que a Contratada tome as medidas necessárias, passando o prazo para o pagamento a ser contado a partir de data da reapresentação do mesmo. Caso se constate erro ou irregularidade na Nota Fiscal, a Administração, a seu critério, poderá devolvê-la, para as devidas correções, ou aceitá-las, com a glosa da parte que considerar indevida.

24.13. Na hipótese de devolução, a Nota Fiscal será considerada como não apresentada, para fins de atendimento das condições contratuais.

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

24.15. Conforme a Instrução Normativa RFB nº 1.234/2012, alterada pela Instrução Normativa RFB nº 2.145/2023, e com a Instrução Normativa nº 34/2023/SEFIN-COTES, será realizada a retenção na fonte do Imposto de Renda incidente sobre os valores pagos à CONTRATADA, nos casos legalmente previstos, incluindo rendimentos oriundos de fornecimento de bens ou prestação de serviços.

25. SANÇÕES ADMINISTRATIVAS

25.1. Considerando as **INFRAÇÕES E SANÇÕES ADMINISTRATIVAS** devem ser atendidos e preceituado como parâmetros os Art. 155 ao Art. 163 da Lei 14.133/2021 e arts. 184, 185, 186 e 187 Decreto Estadual Nº 28.874 de 25 de janeiro de 2024.

25.2. Sem prejuízo das sanções cominadas no art. 156, I, III e IV, da Lei nº 14.133 de 1º de abril de 2021, pela inexecução total ou parcial do contrato, a Administração poderá, garantida a prévia e ampla defesa, aplicar à Contratada multa de até 10% (dez por cento) sobre a parte inadimplida do contrato.

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

25.4. Ficará impedido de licitar e de contratar com o Estado de Rondônia e será descredenciado no SICAF, pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas em edital e no contrato e das demais cominações legais, garantido o direito à ampla defesa, o licitante que, convocado dentro do prazo de validade de sua proposta:

I - não assinar o contrato;

II - não entregar a documentação exigida no edital;

III - apresentar documentação falsa;

IV - causar o atraso na execução do objeto;

V - não mantiver a proposta;

VI - falhar na execução do contrato;

VII - fraudar a execução do contrato;

VIII - comportar-se de modo inidôneo;

IX - declarar informações falsas; e

X - cometer fraude fiscal.

25.4.1. As sanções descritas no item 25.3, também se aplicam aos integrantes do cadastro de reserva, em pregão para registro de preços que, convocados, não honrarem o compromisso assumido sem justificativa ou com justificativa recusada pela administração pública.

25.4.2. As sanções serão registradas e publicadas no SICAF e Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual - CAGEFIMP.

25.5. A multa descrita no quadro de infrações, eventualmente imposta à Contratada, será automaticamente descontada da fatura a que fizer jus, acrescida de juros moratórios de 1% (um por cento) ao mês. Caso a contratada não tenha nenhum valor a receber do Estado, ser-lhe-á concedido o prazo de 05 (cinco) dia úteis, contados de sua intimação, para efetuar o pagamento da multa. Após esse prazo, não sendo efetuado o pagamento, serão deduzidos da garantia. Mantendo-se o insucesso, seus dados serão encaminhados ao órgão competente para que seja inscrita na dívida ativa, podendo, ainda a Administração proceder à cobrança judicial.

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

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

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

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

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

ITEM	DESCRIÇÃO DA INFRAÇÃO	GRAU	MULTA
1.	Permitir situação que crie a possibilidade ou cause dano físico, lesão corporal ou consequências letais;	06	4,0% sobre o valor mensal do contrato.
2.	Usar indevidamente informações sigilosas a que teve acesso;	06	4,0% sobre o valor mensal do contrato

ITEM	DESCRIÇÃO DA INFRAÇÃO	GRAU	MULTA
3.	Suspender ou interromper, salvo por motivo de força maior ou caso fortuito, os serviços contratuais por dia e por unidade de atendimento	05	3,2% sobre o valor mensal do contrato
4.	Destruir ou danificar documentos por culpa ou dolo de seus agentes;	05	3,2% sobre o valor mensal do contrato
5.	Recusar-se a executar serviço determinado pela FISCALIZAÇÃO, sem motivo justificado;	04	1,6% sobre o valor mensal do contrato
6.	Executar serviço incompleto, paliativo substitutivo como por caráter permanente, ou deixar de providenciar recomposição complementar;	02	0,4% sobre o valor mensal do contrato
7.	Fornecer informação pérfida de serviço ou substituição de material;	02	0,4% sobre o valor mensal do contrato
Para os itens a seguir, deixar de:			
8.	Ressarcir o órgão por eventuais danos causados por sua culpa, em qualquer bem/material.	02	0,4% sobre o valor contratado
9.	Cumprir quaisquer dos itens do Edital e seus anexos, mesmo que não previstos nesta tabela de multas, após reincidência formalmente notificada pela FISCALIZAÇÃO;	03	0,8% sobre o valor mensal do contrato
10.	Refazer serviço não aceito pela FISCALIZAÇÃO, nos prazos estabelecidos no contrato ou determinado pela FISCALIZAÇÃO; por unidade de tempo definida para determinar o atraso	03	0,8% sobre o valor mensal do contrato
11.	Cumprir determinação formal ou instrução complementar da FISCALIZAÇÃO.	03	0,8% sobre o valor mensal do contrato
12.	Iniciar execução de serviço nos prazos estabelecidos pela FISCALIZAÇÃO, observados os limites mínimos estabelecidos por este Contrato; por serviço.	02	0,4% sobre o valor mensal do contrato
13.	Manter a documentação de habilitação atualizada;	01	0,2% sobre o valor mensal do contrato

Nota: Incidente sobre o valor da parcela do contrato.

25.11. As sanções aqui previstas poderão ser aplicadas concomitantemente, facultada a defesa prévia do interessado, no respectivo processo, no prazo de 05 (cinco) dias úteis.

25.12. Após 30 (trinta) dias da falta de execução do objeto, será considerada inexecução total do contrato, 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. As sanções previstas não poderão ser relevadas, salvo ficar comprovada a ocorrência de situações que se enquadrem no conceito jurídico de força maior ou casos fortuitos, devidos e formalmente justificados e comprovados, e sempre a critério da autoridade competente, conforme prejuízo auferido.

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

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

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

a) Tenham sofrido condenações definitivas por praticarem, por meio dolosos, fraude fiscal no recolhimento de tributos;

b) Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

c) Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

25.18. Sem prejuízo das sanções cominadas no Decreto nº 28874, de 25 de janeiro de 2024, conforme se segue:

> [...]
>
> Art. 185. A apuração de infração administrativa que enseja a imposição de advertência ou multa, isoladas ou cumulativamente, se dará mediante rito simplificado, observadas as garantias do administrado.
>
> Parágrafo único. 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.
>
> [...]

26. DIREITOS AUTORAIS

26.1. A forma de contratação do objeto não exige a previsão de direitos autorais, propriedade intelectual, nem tampouco sigilo e segurança de dados, conforme Art. 42, inciso XXVII, do Decreto Estadual No. 28.874/2024.

27. REQUISITOS PARA SERVIÇOS QUE ENVOLVAM SOLUÇÃO DE TIC

27.1. A empresa CONTRATADA deverá realizar o repasse de conhecimento aos funcionários da CONTRATANTE que atuarão, diretamente, com a solução de segurança adquirida, contemplando instalação, parametrização, monitoramento, melhores práticas e atuação de incidentes com carga horária mínima de 40 (quarenta) horas ministrado por profissional certificado pelo fabricante.

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

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

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

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

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

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

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

27.9. **Glossário de termos específicos de TIC:**

27.9.1. **Endpoint:** Dispositivo final que se conecta à rede de uma empresa, como computadores, laptops, smartphones ou tablets.

27.9.2. **Proteção de Endpoints:** Conjunto de medidas e ferramentas que visam proteger dispositivos de usuários contra ameaças, como malwares e ataques de phishing.

27.9.3. **Abordagem Proativa:** Estratégia que busca prevenir problemas e incidentes antes que eles ocorram, por meio de monitoramento contínuo e detecção antecipada de ameaças.

27.9.4. **Resposta a Incidentes:** Ações tomadas para mitigar os danos após a detecção de um evento de segurança, como uma invasão ou ataque cibernético.

27.9.5. **Proteção de Servidores:** Medidas de segurança destinadas a proteger servidores (locais ou em nuvem) contra ataques e violações de dados, assegurando a integridade e disponibilidade dos dados.

27.9.6. **Throughput de Dados:** Termo que define a capacidade de processamento de dados de uma rede ou dispositivo, medida pela quantidade de dados que pode ser transmitida em um período de tempo específico, geralmente em megabits ou gigabits por segundo.

27.9.7. **Solução de Segurança Avançada:** Ferramentas ou sistemas que utilizam tecnologias de ponta, como inteligência artificial e machine learning, para detectar e mitigar ameaças complexas e avançadas em redes corporativas.

27.9.8. **Mitigação de Ameaças:** Processo de redução ou eliminação dos riscos associados a ameaças de segurança, minimizando os impactos de potenciais ataques.

27.9.9. **NGIPS (Next-Generation Intrusion Prevention System):** Sistema de prevenção de intrusão de próxima geração, que vai além das funcionalidades tradicionais de firewalls e IDS (sistema de detecção de intrusão), usando técnicas avançadas para identificar e bloquear atividades maliciosas em redes.

27.9.10. **Firewall:** Ferramenta de segurança que monitora e controla o tráfego de rede de entrada e saída, agindo como uma barreira entre uma rede interna segura e outra externa potencialmente insegura.

27.9.11. **Sistema de Prevenção de Intrusão (IPS):** Tecnologia que monitora redes e sistemas em busca de atividades maliciosas ou violações de políticas de segurança, reagindo ativamente para bloquear ou impedir esses ataques.

27.9.12. **Suporte Proativo:** Serviço de suporte técnico que visa prevenir problemas antes que eles ocorram, realizando manutenções regulares, atualizações e monitoramento constante.

27.9.13. **Suporte Corretivo:** Serviço de suporte técnico que busca corrigir problemas ou falhas após a sua ocorrência, restaurando o funcionamento adequado da solução ou sistema.

27.9.14. **Implantação:** Processo de instalação e configuração de uma solução de software ou hardware, incluindo o ajuste da ferramenta ao ambiente corporativo específico.

27.9.15. **Capacitação:** Treinamento fornecido para preparar a equipe técnica e operacional na utilização eficaz da solução adquirida, com foco em melhorar o uso e a manutenção do sistema.

27.9.16. **Repasse de Conhecimento:** Processo de transferência de habilidades e conhecimentos técnicos de especialistas para a equipe da organização, garantindo autonomia para operar e manter a solução adquirida.

27.9.17. **Malware:** Software malicioso criado para danificar, invadir ou roubar informações de um sistema de computador. Exemplos incluem vírus, trojans, ransomware e spyware.

27.9.18. **Phishing:** Método de fraude digital que envolve enganar as pessoas para que forneçam informações pessoais ou confidenciais, como senhas ou números de cartão de crédito, por meio de mensagens falsas. Vulnerabilidade: Falha ou fraqueza em um sistema que pode ser explorada por ameaças cibernéticas para causar danos ou obter acesso não autorizado.

27.9.19. **Machine Learning (Aprendizado de Máquina):** Tecnologia que permite que sistemas de segurança "aprendam" com padrões de dados para identificar e prever ameaças de forma mais eficaz, evoluindo continuamente com base em novos dados.

27.9.20. **Resiliência:** Capacidade de um sistema ou rede de continuar operando ou se recuperar rapidamente após um ataque ou incidente de segurança.

27.9.21. **NOC (Network Operations Center):** Centro de Operações de Rede, onde equipes monitoram, gerenciam e controlam redes e sistemas para garantir o desempenho e a segurança.

27.9.22. **SOC (Security Operations Center):** Centro de Operações de Segurança, onde uma equipe de especialistas monitora e responde a incidentes de segurança cibernética, prevenindo e mitigando ameaças em tempo real.

27.9.23. Esses termos técnicos são comuns em processos de contratação de soluções de segurança e refletem as tecnologias e serviços necessários para proteger redes, endpoints e servidores corporativos de forma eficaz.

27.10. **Requisitos de manutenção e garantia**

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

27.10.2. A garantia deve incluir obrigatoriamente:

27.10.2.1. Atualização das versões dos softwares fornecidos, caso sejam disponibilizadas novas versões.

27.10.2.2. Atualização dos softwares fornecidos caso haja lançamento de novos softwares que substituam os fornecidos ou se ficar evidente a descontinuidade dos softwares fornecidos, mesmo que não se trate de substituição direta.

27.10.2.3. Correções dos softwares fornecidos, incluindo a aplicação de patches para corrigir eventuais falhas (bugs) de software que possam prejudicar o ambiente de produção ou vulnerabilidades que comprometam a segurança da solução.

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

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

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

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

28.1. Em observação às determinações constantes na lei 13.709/2018, o CONTRATANTE e a CONTRATADA se comprometem a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, relativos ao tratamento de dados pessoais, inclusive nos meios digitais, garantindo que:

a. O tratamento de dados pessoais dar-se-á de acordo com as bases legais previstas nas hipóteses dos Arts. 7º e/ou 11 da Lei 13.709/2018 às quais se submeterão os serviços, e para propósitos legítimos, específicos, explícitos e informados ao titular;

b. O tratamento seja limitado às atividades necessárias ao atingimento das finalidades de execução do objeto do contrato, utilizando-os, quando seja o caso, em cumprimento de obrigação legal ou regulatória, no exercício regular de direito, por determinação judicial ou por requisição da Autoridade Nacional de Proteção de Dados (ANPD); ou ainda em atividades à operadora da CONTRATADA;

c. Em caso de necessidade de coleta de dados pessoais indispensáveis à própria prestação do serviço/aquisição de bens, esta se dará para fins de cumprimento da execução do contratado. Os dados assim coletados só poderão ser utilizados na execução do objeto especificado neste contrato, ressalvado o tratamento para operações da Contratada, e quando o compartilhamento for necessário à atividade da CONTRATADA para fins da prestação do serviço, será exigido do terceiro o compromisso com a proteção de dados e privacidade.

d. Todas as informações obtidas pela CONTRATADA durante a execução dos serviços deverão ser tratadas como confidenciais, sendo vedada qualquer reprodução, utilização ou divulgação a terceiros, devendo zelar por seus representantes, empregados pela manutenção do sigilo absoluto de dados, informações, apresentações, documentos, códigos, especificações técnicas e demais artefatos que tenham conhecimento ou que sejam desenvolvidos em razão dos serviços executados;

e. A CONTRATADA deverá estar ciênte e respeitar a Política de Privacidade (ID SEI nº 0019610148) e a Política de Segurança da Informação (ID SEI nº 0018466170 da SETIC, quando do acesso a processos administrativos, e/ou tratamento de quaisquer dados de responsabilidade da Administração;

f. É expressamente proibida a divulgação, o repasse ou a utilização indevida de informações, bem como de documentos, imagens e gravações utilizadas durante a prestação dos serviços;

29. DEMAIS CONDIÇÕES

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

29.2. O objeto da aquisição ofertado pela CONTRATADA deverá atender ás exigências de qualidade, observados os padrões e normas preconizados pelos órgãos competentes de controle de qualidade industrial – ABTN, INMETRO, etc; atentando-se o proponente, principalmente para as prescrições contidas no art. 39, VIII, da Lei nº 8.078/90 (Código de Defesa do Consumidor).

29.3. As omissões, dúvidas e casos não previstos neste instrumento, serão resolvidos e decididos aplicando as regras contratuais e a Lei Federal nº 14.133 de 1° de Abril de 2021 e suas alterações.

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

29.5. Esta Secretaria de Estado da Saúde certifica que atende ao princípio da segregação de funções, conforme art. 7º, §1º, da Lei 14133/21 e art. 12 do Decreto 11246/22

29.6. Fica estabelecido, caso venha ocorrer algum fato não previsto neste termo de referência e seus anexos, os chamados casos omissos, estes serão dirimidos respeitado o objeto desse certame, por meio de aplicação da legislação e demais normas reguladoras da matéria, em especial a lei nº 14.133/2021, aplicando-se paralelamente, quando for o caso, supletivamente, os princípios da teoria geral dos contratos estabelecidos na legislação civil brasileira e as disposições de direito privado.

29.7. A administração utilizar-se à da aplicação de juízo arbitral para dirimir conflitos relativos a direitos patrimoniais disponíveis, conforme disposto na Lei Estadual 407 e Lei n. 9.307 , de 1996, alterada pela Lei Federal n. 13.129, de 2015. Tal medida visa o cumprimento ao Art. 11, do referido diploma legal.

29.8. Fica eleito o Foro da Comarca de Porto Velho/RO para dirimir os possíveis litígios que decorram do presente procedimento.

29.9. Nenhuma reivindicação adicional de pagamento ou reajustamento de preços será considerada.

29.10. Fica vedado a contratação de cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do órgão ou entidade contratante ou de agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, conforme Art. 48, Parágrafo Único, da Lei 14133/2021.

29.11. Fica vedado a intervenção indevida da Administração na gestão interna do contratado, conforme art. 48, VI, da Lei 14133/21.

29.12. Certifica-se que esta Secretária de Estado da Saúde atende ao princípio da segregação de funções, conforme art. 7º, §1º, da Lei 14133/21 e art. 12 do Decreto 11246/22.

29.13. Certifica-se para os fins previstos no inciso II, do Art. 16 da Lei Complementar n°101, de 04 de maio de 2000, que a despesa pública acima especificada tem adequação financeira com a lei orçamentária anual (LOA) e compatibilidade com o Plano Plurianual (PPA) e com a Lei de Diretrizes Orçamentária (LDO).

29.14. Certifica-se que esta Secretaria de Estado da Saúde fica comprometida a emitir a devida Nota de Empenho assim que liberado o crédito orçamentário pela Secretária de Estado de Planejamento Orçamento e Gestão (SEPOG), no presente exercício e próximo de acordo com a LOA 2026.

29.15. Certifica-se que está Secretaria de Estado da Saude cumpre o princípio compatibilidade da despesa estimada com a prevista nas leis orçamentárias. Art. 40, V, “c”, da Lei 14.133/21.

29.16. Certifica-se que está Secretaria de Estado da Saude atesta o cumprimento das disposições contidas no Plano de Contratações Anual (Decreto nº 10947/22), no Plano Diretor de Logística Sustentável e demais instrumentos de planejamento estabelecidos pela Instrução Normativa nº 81/2022 (Art. 7º), garantindo assim a otimização dos processos e a observância dos princípios da administração pública.

29.17. **DA LEI DE ACESSO A INFORMAÇÃO (12.527/2011)**

29.17.1. Cumpre destacar que o Sistema Eletrônico de Informações – SEI dispõe de mecanismos seguros e auditáveis para classificação documental e definição de níveis de acesso, em conformidade com a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) e demais normativos correlatos.

29.17.2. Em observância a essa legislação, a Secretaria de Estado da Saúde – SESAU/RO realiza a classificação e o tratamento das informações de forma criteriosa, observando as hipóteses legais de sigilo e garantindo a adequada conciliação entre os princípios da transparência, publicidade, proteção de dados e segurança da informação. Assim, assegura-se que todos os documentos e informações produzidos no âmbito deste processo sigam rigorosamente as disposições legais que regem o acesso à informação pública e a preservação de dados sigilosos.

30. PLANILHA DE COMPOSIÇÃO DE CUSTOS E FORMAÇÃO DE PREÇOS

30.1. O objeto da presente licitação e sua forma de contratação não exigem a confecção de planilha de composição de custos e formação de preços, conforme Art. 42, inciso XXX, do Decreto Estadual No. 28.874/2024.

31. SISTEMA DE REGISTRO DE PREÇOS

31.1. JUSTIFICATIVA PARA ESCOLHA DO SISTEMA DE REGISTRO DE PREÇO:

31.1.1. Sabe-se que o registro de preço é uma das modalidades de escolha para as aquisições públicas pelas características que se impõem através do Art. 40 da Lei 14.133/21.

> "Art. 40. O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:
>
> [...] II - processamento por meio de sistema de registro de preços, quando pertinente;"

31.1.2. O registro de preços é um sistema que visa a uma racionalização nos processos de contratação de compras públicas e de prestação de serviços. Sua finalidade precípua é maximizar o princípio da economicidade, permitindo à Administração Pública celebrar o contrato administrativo na exata medida e no momento de sua necessidade, sempre precedido de licitação, qualquer que seja o valor efetivo a ser praticado em cada situação específica.

31.1.3. Além disso, o art. 84 da Lei 14.133/21 e art. 42, §1º, IV, do Decreto Estadual n. 28.874, de 2024**,** estabelece que "o prazo de vigência da ata de registro de preços será de 1 (um) ano e poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso." Isso permite que a Administração Pública tenha flexibilidade na contratação, ajustando as aquisições conforme as necessidades e o orçamento disponíveis, sem comprometer a eficiência do gasto público.

31.1.4. Ou seja, a existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente motivada.

31.1.5. Visto que, no registro de preços não há quantidade mínima a ser adquirida, tampouco obrigatoriedade de aquisição de todo o quantitativo licitado. Os valores registrados não são exclusivos para determinadas secretarias ou entidades e podem ser compartilhados por toda a administração, dentro dos limites esculpidos pela legislação.

31.1.6. Com base nestes fundamentos, justifica-se a escolha pelo Sistema de Registro de Preços para a aquisição de servidores de hiperconvergência, serviços de instalação e assistência técnica, de forma a assegurar que a SESAU esteja equipada para responder às demandas operacionais de suas unidades de saúde, mantendo a qualidade e a continuidade dos serviços prestados à população.

31.1.7. A quantidade mínima a ser solicitada de cada item será de 10% do valor previsto para cada item.

31.1.8. No registro de preços não há obrigatoriedade de aquisição de todo o quantitativo licitado. Os valores registrados não são exclusivos para determinadas secretarias ou entidades e podem ser compartilhados por toda a administração, dentro dos limites esculpidos pela legislação.

31.1.9. Faz-se necessário o Registro de Preços, a fim de evitar a falta de estoque, proporcionando maior agilidade e qualidade nos serviços prestados a população.

31.1.10. Levando em conta as prerrogativas acima descritas JUSTIFICA-SE a necessidade do registro de preços para pretensa aquisição constante neste termo de referência conforme discriminação e quantitativos estabelecidos.

31.1.11. O órgão gerenciador da Ata de Registro de Preço será a Coordenadoria do Sistema de Registro de Preço-CRP/SUPEL/RO.

31.1.12. Além disso, o SRP promove:

a) Racionalização Administrativa e Eficiência Logística
O procedimento dispensa a repetição de licitações para itens recorrentes, otimizando recursos humanos e reduzindo os custos administrativos envolvidos nas contratações.

b) Aquisição Planejada e Sob Demanda
Permite que a SESAU adquira os equipamentos e serviços apenas quando necessário, evitando estoques desnecessários, desperdício de recursos públicos e obsolescência tecnológica.

c) Previsibilidade e Controle Orçamentário
A contratação sob demanda, aliada à prévia estimativa de consumo, facilita o planejamento financeiro da SESAU, alinhando-se ao princípio da responsabilidade fiscal e promovendo o uso racional dos recursos públicos.

d) Possibilidade de Compartilhamento entre Órgãos
Os itens registrados em ata podem ser utilizados por outros órgãos e entidades da Administração Pública Estadual, promovendo economia de escala e padronização tecnológica em todo o governo.

e) Segurança Jurídica e Transparência
O SRP está amparado em dispositivo legal específico, com rito formal e procedimentos regulados, conferindo segurança à contratação e ampla publicidade dos atos administrativos.

f) Redução de Tempo na Contratação
Uma vez registrada a ata, a contratação futura pode ser realizada com agilidade, o que é vital para áreas sensíveis como a saúde, onde a continuidade e a celeridade dos serviços são prioridades.

g) Adaptação a Demandas Emergenciais
Em casos de emergência ou aumento inesperado da demanda (ex.: surtos epidemiológicos ou sobrecarga de sistemas), a SESAU poderá lançar mão do SRP para obter os recursos tecnológicos com rapidez, sem necessidade de novo certame licitatório.

h) Vantajosidade Econômica
A ampla concorrência na fase de registro de preços tende a gerar condições mais favoráveis de contratação, como melhores preços unitários, garantias estendidas e escopo técnico mais completo.

i) Redução do Risco de Fracasso na Contratação
A possibilidade de registrar vários fornecedores para um mesmo item aumenta as chances de sucesso na aquisição, reduzindo a dependência de um único fornecedor e o risco de desabastecimento.

31.1.13. Essa modalidade, portanto, não apenas cumpre os princípios constitucionais da legalidade, eficiência, economicidade e isonomia, como também se mostra mais adequada à natureza e à dinâmica da demanda da SESAU, marcada por variações contínuas de uso, expansão de sistemas, necessidades emergenciais e exigências por alta disponibilidade e performance.

31.1.14. Com base nestes fundamentos, justifica-se a escolha pelo Sistema de Registro de Preços para a aquisição de servidores de hiperconvergência, serviços de instalação e assistência técnica, de forma a assegurar que a SESAU esteja equipada para responder às demandas operacionais de suas unidades de saúde, mantendo a qualidade e a continuidade dos serviços prestados à população.

31.2. REGISTRO DE PREÇOS

31.2.1. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente motivada.

31.2.2. Fica a Detentora ciente que a publicidade da ata de registro de preços na imprensa oficial terá efeito de compromisso nas condições ofertadas e pactuadas na proposta apresentada à licitação.

31.2.3. A Ata de Registro de Preços, os ajustes dela decorrentes, suas alterações e rescisões obedecerão a Lei Federal nº 14.133/21 demais normas complementares e disposições desta Ata e do Edital que a precedeu, aplicáveis à execução e especialmente aos casos omissos.

31.3. **GERENCIAMENTO DA ATA DE REGISTRO DE PREÇOS**

31.3.1. A Superintendência Estadual de Compras e Licitações – SUPEL, será o órgão responsável pelos atos de administração, controle e gerenciamento da Ata de Registro de Preços, conforme Art. 122 do Decreto Estadual nº. 28.874, de 25 de janeiro de 2024, conforme versa abaixo:

> Art. 122.Caberá ao órgão gerenciador, órgão competente para operacionalizar os procedimentos licitatórios no âmbito da Administração Pública, a prática de todos os atos de controle e administração do SRP, e ainda o seguinte:
>
> II - consolidar todas as informações relativas a estimativa individual e total de consumo encaminhadas pelos órgãos participantes para atender aos requisitos de padronização e racionalização;
>
> III - elaborar o projeto básico ou termo de referência do registro de preços fruto da intenção;
>
> IV - promover todos os atos necessários à instrução processual para a realização do procedimento licitatório de intenção de registro de preços;
>
> V - realizar levantamento de mercado e pesquisa de preço ampla e diversificada para elaboração da estimativa orçamentária, devendo zelar pela maior amplitude possível das fontes pesquisadas;
>
> VI - confirmar junto aos órgãos participantes a sua concordância com o objeto a ser licitado, inclusive quanto aos quantitativos e projeto básico;
>
> VII - realizar todo procedimento licitatório, bem como os atos dele decorrentes;
>
> VIII - gerenciar a ata de registro de preços, providenciando a indicação, sempre que solicitado, dos fornecedores, para atendimento às necessidades da Administração, obedecendo a ordem de classificação e os quantitativos de contratação definidos pelos órgãos participantes;
>
> IX - conduzir os procedimentos relativos a eventuais renegociações dos preços registrados e a aplicação de penalidades por descumprimento do pactuado na ata de registro de preços;
>
> X - analisar as solicitações de adesão formuladas pelos órgãos não participantes;
>
> XI - zelar pela observância dos limites individual e global para adesão;
>
> XII - divulgar o conteúdo do edital, da ata de registro de preços, os eventuais contratos e termos aditivos, na Imprensa Oficial, no sítio eletrônico do Estado e no Portal Nacional de Contratações Públicas, conforme as diretrizes da Lei Federal n° 14.133, de 2021.
>
> § 1°A análise das solicitações de adesão deverá ser precedida de levantamento de mercado e pesquisa de preço para aferição do valor do objeto registrado com base no quantitativo resultante da adesão, apresentado por ato próprio da unidade aderente.
>
> § 2°A constatação de preço mais vantajoso em decorrência da pesquisa referida no parágrafo anterior, identificada e informada pela unidade de origem, acarretará a necessidade de repactuação do preço registrado.
>
> § 3°Não havendo êxito nas negociações, o órgão gerenciador não autorizará a adesão.

31.4. **DA INTENÇÃO DE REGISTRO DE PREÇOS - IRP**

31.4.1. Não será adotada a etapa de Intenção de Registro de Preços (IRP) devido à natureza dos objetos se relacionarem exclusivamente ao órgão ou entidade responsável pelo certame, conforme disposição do art. 117, § 2°, I, do Decreto n° 28.874/2024

31.4.2. A Secretaria de Estado da Saúde é o único contratante interessado, uma vez que as atribuições relacionadas ao objeto são exclusivas e indelegáveis pelo órgão em âmbito Estadual.

31.4.3. A Superintendência Estadual de Compras e Licitações – SUPEL ficará responsável pela intenção de registro de preços, conforme preconiza o Art. 122 do Decreto Estadual 28.874/2024:

> Art. 122. Caberá ao órgão gerenciador, órgão competente para operacionalizar os procedimentos licitatórios no âmbito da Administração Pública, a prática de todos os atos de controle e administração do SRP, e ainda o seguinte:
>
> **I - realizar o procedimento de intenção de registro na forma do art. 124;**

31.5. **UTILIZAÇÃO DA ATA E DO FORNECIMENTO ADICIONAL "CARONAS"**

31.5.1. De acordo com o Artigo 124 do Decreto Estadual n° 28.874/24, durante a sua vigência, a utilização de ata de registro de preço por órgão não participante está sujeita à prévia autorização do órgão gerenciador. A autorização deverá levar em consideração a observância dos limites individual e global previstos neste decreto, além da necessidade de garantia da capacidade de fornecimento e observância da economia de escala.

31.5.2. **Conforme disposto no art. 121 do decreto estadual 28.874/2024, o limite individual da cada**

órgão ou entidade não participante será de um aumento de 50% do quantitativo registrado, ressalvado o disposto no ressalvado o disposto no art. 86, § 7°, da Lei Federal n° 14.133, de 2021.

31.5.3. **O conjunto de solicitações de adesão, independente do órgão ou entidade solicitante, não poderá exceder ao limite global de duas vezes o quantitativo registrado, conforme art. 121 do Decreto Estadual n° 28.874/24.**

31.5.4. É facultada aos órgãos ou entidades municipais, distritais ou estaduais a adesão à ata de registro de preços dos órgãos e entidades da União, dos Estados- Membros e do Distrito Federal, desde que os preços sejam compatíveis com os praticados no mercado e seja demonstrada a vantagem da adesão.

31.5.5. Caso haja adesão de itens individualizados, estes devem corresponder à proposta de menor valor, sob pena de inviabilidade da adesão

31.5.6. A utilização da ata de registro de preço por órgão não participante está sujeita a prévia autorização do órgão gerenciador.

31.5.7. O limite global de adesão á Ata de Registro de Preço não poderá exceder a quantidade total de cada item registrado para os órgãos participantes, independentemente do número de órgãos não participantes que aderirem.

31.5.8. A garantia da capacidade de fornecimento deverá ser demonstrada por meio de expressa autorização do fornecedor ou prestador de serviço registrado na qual esteja consignada o compromisso de não descontinuar ou prejudicar a concretização do quantitativo registrado a despeito da adesão solicitada.

31.5.9. As solicitações de adesão deverão ser formalizadas por meio de requerimento específico instruído em processo administrativo próprio com os seguintes documentos:

31.5.10. documento que ateste a equivalência do objeto registrado com a necessidade administrativa do órgão não participante;

31.5.11. nota de reserva orçamentária do recurso necessário a fazer face à despesa decorrente da adesão;

31.5.12. demonstração da vantajosidade dos preços registrados por meio da realização de pesquisa de mercado com amplitude e diversidade de fontes;

31.5.13. autorização expressa do órgão gerenciador;

31.5.14. autorização expressa do fornecedor ou prestador de serviço registrado nos moldes previstos no § 4° deste artigo.

31.5.15. A solicitação de adesão deverá estabelecer de forma clara o quantitativo do objeto que se pretende contratar, com base em técnicas estimativas que considerarão, quando possível, o histórico de consumo e a perspectiva de aumento ou redução da demanda.

31.5.16. A quantidade mínima a ser fornecida será o quantitativo total estabelecido como referência no item 3.2. deste Termo de Referência, conforme o art. 82, II e III da Lei nº 14.133/2021, atendendo ao princípio do art. 40, V, 'a' da padronização, considerando a compatibilidade das especificações estéticas, técnicas ou de desempenho.

31.5.17. A quantidade mínima para cada ordem de fornecimento, será de 10% do quantitativo registrado, conforme art. 121 do Decreto Estadual n° 28.874/24.

31.6. VIGÊNCIA DA ATA DE REGISTRO DE PREÇO

31.6.1. Os contratos decorrentes da Ata de Registro de Preços terão sua vigência conforme as disposições contidas no art. 84 da Lei 14.133/21.

31.6.2. Conforme art. 125 do Decreto Estadual n° 28.874/2024, o prazo de vigência da ata de registro de preços será de 1 (um) ano e poderá ser prorrogado, por igual período, desde que comprovada a vantajosidade do preço registrado, mediante pesquisa de mercado que leve em consideração os parâmetros fixados no art. 51, do mesmo decreto.

31.7. ALTERAÇÃO DA ATA DE REGISTRO DE PREÇOS

31.7.1. Os preços registrados poderão ser revistos em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos serviços ou bens registrados, cabendo ao órgão gerenciador promover as negociações junto aos fornecedores, observadas as disposições contidas na alínea "d"

do inciso II do caput do artigo 124 da Lei 14.133/21.

31.7.2. Quando o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão gerenciador convocará os fornecedores para negociarem a redução dos preços aos valores praticados pelo mercado.

31.7.3. Os fornecedores que não aceitarem reduzir seus preços aos valores praticados pelo mercado serão liberados do compromisso assumido, sem aplicação de penalidade.

31.7.4. A ordem de classificação dos fornecedores que aceitarem reduzir seus preços aos valores de mercado observará a classificação original.

31.7.5. Quando o preço de mercado tornar-se superior aos preços registrados, e o fornecedor não puder cumprir o compromisso, o órgão gerenciador poderá:

31.7.6. Liberar o fornecedor do compromisso assumido, caso a comunicação ocorra antes do pedido de fornecimento, sem aplicação de penalidade se confirmada à veracidade dos motivos e comprovantes.

31.7.7. Convocar os demais fornecedores para assegurar igual oportunidade de negociação.

31.7.8. Não havendo êxito nas negociações, o órgão gerenciador deverá proceder à revogação do item da ata de registro de preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

31.7.9. Art. 132 do Decreto Estadual n. 28.874/2024 , as eventuais alterações da ata de registro de preços não poderão acarretar aumento dos quantitativos registrados, inclusive, nas hipóteses previstas no art. 124 da Lei Federal n° 14.133, de 2021. (Redação do parágrafo dada pelo Decreto Nº 28.874 de 25/01/2024).

31.7.10. Com relação às supressões, conforme previsto no § 1°, do Art. 124, da Lei Federal nº. 14.133/21, o objeto da presente licitação poderá sofrer supressões.

31.8. DO CANCELAMENTO DO REGISTRO

31.8.1. Os preços registrados poderão ser revisto em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução tal como pactuado, observada a instrução processual respectiva, cabendo ao órgão gerenciador promover as negociações junto aos fornecedores, conforme disposto no art. 133 do Decreto Estadual n° 28.874 de 25 de janeiro de 2024.

31.8.2. Os preços registrados serão mantidos inalterados por todo o período de vigência da Ata de Registro de Preços - ARP, admitida sua revisão para majorar ou minorar os preços registrados em casos excepcionais, nas hipóteses legais e considerando os preços vigentes de mercado.

31.8.3. A revisão de preços precederá de requerimento: I - do detentor da ata, que deverá fazê-la antes do pedido de fornecimento e, instruindo seu pedido com documentação probatória de majoração de preço do mercado e a oneração de custos; ou II - pelo órgão participante ou órgão interessado, comprovando por meio de pesquisas de preços que há minoração do valor originalmente registrado.

31.8.4. Quando o preço inicialmente registrado, por motivo superveniente, tornar-se superior ao preço praticado no mercado o órgão gerenciador convocará o fornecedor visando a negociação para redução de preços e sua adequação ao praticado pelo mercado e, caso este não aceite a redução dos seus preços aos valores praticados pelo mercado será liberado dos compromissos assumidos, sem aplicação de penalidades administrativas, nos termo do art. 134, § 1º do Decreto Estadual n° 28.874/2024.

31.8.5. Se não houver prova efetiva da desatualização dos preços registrados e da existência de fato superveniente, o fornecedor continuará obrigado a cumprir os compromissos pelo valor registrado na ata, sob pena de cancelamento do registro de preços e de aplicação das penalidades administrativas previstas em lei e no edital, nos termos do art. 135, § 2º do Decreto Estadual n° 28.874/2024.

31.8.6. Na hipótese do cancelamento do registro de preços prevista no art. 135, § 2º do Decreto Estadual n° 28.874/2024, o órgão gerenciador poderá convocar os demais fornecedores integrantes do cadastro de reserva para que manifestem interesse em assumir o fornecimento dos bens, a execução das obras ou dos serviços, pelo preço registrado na ata.

31.8.7. Caso comprovada a desatualização dos preços registrados decorrente de fato superveniente que prejudique o cumprimento da ata, poderá ser efetuada a atualização do preço registrado, adequando-o aos valores praticados no mercado.

31.8.8. O órgão gerenciador, em alternativa à atualização prevista no item 5.6 desta Ata de Registro de Preços, poderá liberar o fornecedor do compromisso sem aplicação de penalidades, convocando, posteriormente,

os licitantes remanescentes, na ordem de classificação, para negociação e assinatura da ata no máximo nas condições ofertadas por estes, desde que o valor seja igual ou inferior ao orçamento estimado para a contratação, inclusive quanto aos preços atualizados, nos termos do instrumento convocatório.

31.8.9. A redução do preço registrado será comunicada pelo órgão gerenciador aos órgãos que tiverem formalizado contratos com fundamento no respectivo registro, para que avaliem a necessidade de efetuar a revisão dos preços contratados.

31.8.10. O cancelamento do preço registrado, em conformidade com o artigo 136 do Decreto Estadual n° 28.874/2024, poderá ocorrer por fato superveniente decorrente de caso fortuito ou força maior que prejudique o cumprimento da ata, devidamente comprovados e justificados, por razão de interesse público ou a pedido do fornecedor.

31.8.11. O preço registrado, em atenção ao estabelecido pelo art. 136, inc. I a V do Decreto Estadual n° 28.874/2024, também poderá ser cancelado quando o fornecedor descumprir total ou parcialmente as condições previstas na Ata de Registro de Preços, não retirar a nota de empenho ou instrumento equivalente no prazo estabelecido pela Administração, não aceitar reduzir o seu preço registrado na hipótese deste se tornar superior aqueles praticados no mercado ou sofrer sanção prevista na forma do Decreto Estadual n° 28.874/2024 em seu Capítulo VIII.

31.9. REGISTRO DE MAIS DE UM FORNECEDOR

31.9.1. A possibilidade de registro de mais de um fornecedor ou prestador de serviço, desde que aceitem cotar o objeto em preço igual ao do licitante vencedor, assegurada a preferência de contratação de acordo com a ordem de classificação

31.9.2. Para atender ao disposto no art. 82, VII, da Lei Federal nº 14.133, de 2021, fica estabelecida a possibilidade de registro de mais de um fornecedor na ata de registro de preços, conforme as seguintes condições:

31.9.3. Diversidade de Fornecedores: O registro poderá contemplar diferentes fornecedores que apresentem propostas dentro das especificações técnicas e condições de preço estabelecidas neste Termo de Referência.

31.9.4. Critérios de Seleção: A seleção dos fornecedores será realizada com base em critérios de habilitação e classificação, levando em consideração a melhor proposta apresentada em termos de preço e qualidade.

31.9.5. Acesso aos Fornecedores: Todos os fornecedores registrados poderão ser convocados para atender às demandas dos órgãos/entidades participantes, conforme a necessidade de aquisição e o cumprimento das condições da ata.

31.9.6. Os detalhes sobre o número máximo de fornecedores a serem registrados e as condições para convocação serão especificados na fase de execução da ata.

31.10. OBRIGAÇÕES DA DETENTORA DA ATA

31.10.1. Em conformidade com o disposto no art. 42, §1º, VII, do Decreto Estadual nº 28.874, de 2024, a detentora da ata de registro de preços deverá:

> Art. 42.O termo de referência é documento obrigatório para todos os processos licitatórios e contratações diretas destinados a aquisições de bens e contratação de serviços, inclusive serviços comuns de engenharia, quando possível, devendo os demais casos observar a obrigatoriedade de elaboração de projeto básico, excetuando-se a hipótese prevista no § 1º do artigo anterior devendo conter, no que couber, os seguintes parâmetros e elementos descritivos, dentre outros que se fizerem necessários:
>
> I - justificativa para escolha do sistema de registro de preços, informando o dispositivo legal no qual o caso específico se enquadra;
>
> II - indicação do órgão ou entidade gerenciador da ata;
>
> III - indicação dos órgãos ou entidades participantes da ata;
>
> IV - prazo de vigência da ata e sua possibilidade de prorrogação;
>
> V - previsão e justificativa da possibilidade de adesão por órgãos e entidades não participantes, bem como as condições para esta adesão, exceto quando corresponderem àquelas previstas em instrumentos padronizados a serem utilizados na licitação, hipótese em que deverão ser descritas apenas as condições específicas relativas ao caso concreto;
>
> VI - obrigações do órgão gerenciador da ata, exceto quando corresponderem àquelas previstas em

instrumentos padronizados a serem utilizados na licitação, hipótese em que deverão ser descritas apenas as obrigações específicas relativas ao objeto pretendido; e

VII - obrigações da detentora da ata, exceto quando corresponderem àquelas previstas em instrumentos padronizados a serem utilizados na licitação, hipótese em que deverão ser descritas apenas as obrigações específicas relativas ao objeto pretendido.

§ 2° Nos processos de contratação em que for realizada análise de riscos, o TR deve contemplar, quando aplicável, as medidas de tratamento necessárias para mitigá-los, conforme regulamento próprio

§ 3° Para o caso do inciso IV do § 1° deste artigo, a publicação da Ata de Registro de Preços na Imprensa Oficial terá efeito de compromisso nas condições ofertadas e pactuadas na proposta apresentada à licitação, independentemente da assinatura do licitante.

31.10.2. Cumprir os prazos de entrega dos itens contratados, conforme estabelecido na ata e no Termo de Referência.

31.10.3. Manter a qualidade e as especificações dos produtos/serviços, conforme previamente acordado e detalhado no edital e na ata.

31.10.4. Apresentar relatórios de fornecimento e desempenho sempre que solicitado pelos órgãos/entidades participantes.

31.10.5. Notificar imediatamente os órgãos/entidades participantes sobre quaisquer dificuldades que possam comprometer o cumprimento das obrigações assumidas.

31.10.6. Atender às demandas dos órgãos/entidades participantes, conforme a necessidade de aquisição, respeitando as condições e limites estabelecidos.

31.10.7. O não cumprimento das obrigações aqui estabelecidas poderá acarretar penalidades, conforme a legislação vigente e as disposições do Termo de Referência.

31.10.8. Órgão ou entidade participante participa dos procedimentos iniciais da contratação para registro de preços e integra a ata de registro de preços;

31.11. **ÓRGÃO GERENCIADOR DA ATA;**

31.11.1. Órgão gerenciador é o responsável pela condução do conjunto de procedimentos para registro de preços e pelo gerenciamento da ata de registro de preços dele decorrente;

31.11.2. O órgão gerenciador da Ata de Registro de Preço será a Coordenadoria do Sistema de Registro de Preço-CRP/SUPEL/RO.

31.12. **DOS ÓRGÃOS E ENTIDADES PARTICIPANTES**

31.12.1. Faz parte desta Ata de Registro de Preços a Secretaria de Estado da Saúde - SESAU.

32. **ANEXOS**

32.1. Integram este Termo de Referência, para todos os fins e efeitos, os seguintes anexos:

Anexo I - Manual de Gestão e Fiscalização de Contratos Administrativos (0053828787)

Anexo II - Modelo de Minuta de Contrato

Anexo III - Mapa de Risco (0051897532)

Anexo IV - Adendo Matriz de Riscos (0051893000)

ANEXO V - Tabela Suporte Técnico

Elaborado por:
ALLAN JUNIOR ALVES SIQUEIRA
Assessor NSC/CECOMP/CAD

Revisado por:
JOELMA DA SILVA TELES
Responsável Núcleo de Serviços Continuados - SESAU-NSC

Revisado por:
ALYSSON ANTONIO DE MELLO CARVALHO

Revisado por:
COORDENADORIA DE INOVAÇÃO E TECNOLOGIA DA INFORMAÇÃO (SESAU-CITI)

Autorizo Na Forma da Lei, *Autorizo o presente Termo de Referência e SAMS* , declaro e dou fé destes.

ROSELAINE DE SOUZA CHAGA
Secretária Executiva de Estado da Saúde

SESAU Secretaria de Estado da Saúde — RONDÔNIA Governo do Estado

ANEXO I

MANUAL DE GESTÃO E FISCALIZAÇÃO DE CONTRATOS ADMINISTRATIVOS (0053828787)

ANEXO II

CONTRATANTE: O ESTADO DE RONDÔNIA, por intermédio da (ÓRGÃO CONTRATANTE), inscrita no CNPJ/MF sob o n° (00.000.000/0001-00), com sede na Rua Farquar, n° 2986, Complexo Rio Madeira, Bairro Pedrinhas, nesta cidade de Porto Velho-RO, representada pelo (CARGO DO REPRESENTANTE), o Sr. ou Sr(a) (REPRESENTANTE DO ÓRGÃO), portador(a) do CPF/MF nº (000.000.000-00).

CONTRATADA: (NOME DA EMPRESA), inscrita no CNPJ/MF sob n° (00.000.000/0001-00), com endereço na Rua (ENDEREÇO EMPRESARIAL), aqui representada por seu (CARGO), o Sr. ou Sr(a) (REPRESENTANTE EMPRESARIAL), portador(a) do CPF/MF n° (000.000.000-00), de acordo com a representação legal que lhe é outorgada.

Os Contratantes celebram, por força do presente instrumento, CONTRATO DE (DESCRIÇÃO DO SERVIÇO), o qual se regerá pelas disposições da Lei nº 14.133/21 e demais normas pertinentes, licitado através da (MODALIDADE DE LICITAÇÃO), vinculando-se aos termos do Processo Administrativo n° (NÚMERO DO PROCESSO), e à proposta da CONTRATADA, mediante as seguintes cláusulas:

1. CLÁUSULA PRIMEIRA – DO OBJETO

1.1. O objeto do presente instrumento é a (DESCRIÇÃO DO OBJETO), nas condições estabelecidas no Termo de Referência, Edital e seus anexos.

1.2. **Da Vinculação**:
1.2.1. Integram este Contrato além do Termo de Referência, as normas do Edital de Licitação (MODALIDADE DE LICITAÇÃO), e a proposta da CONTRATADA, independentemente de transcrição.

2. CLÁUSULA SEGUNDA – DO DETALHAMENTO DO OBJETO

2.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

3. CLÁUSULA TERCEIRA – DA EXECUÇÃO DO SERVIÇO

3.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

4. CLÁUSULA QUARTA – DAS CONDIÇÕES DE RECEBIMENTO DO OBJETO

4.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

5. CLÁUSULA QUINTA – DA GARANTIA

5.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador

de despesa do órgão requerente.

6. CLÁUSULA SEXTA – DA VIGÊNCIA

6.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

7. CLÁUSULA SÉTIMA – DO VALOR E DOTAÇÃO ORÇAMENTÁRIA

7.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

8. CLÁUSULA OITAVA – DAS CONDIÇÕES DE PAGAMENTO

8.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

8.2 – Da Retenção do Imposto de Renda na Fonte

8.2.1. Em conformidade com o disposto na Instrução Normativa RFB nº 1.234/2012, alterada pela Instrução Normativa RFB nº 2.145/2023, bem como com a Instrução Normativa nº 34/2023/SEFIN-COTES, a CONTRATANTE efetuará a retenção na fonte do Imposto de Renda incidente sobre os valores pagos à CONTRATADA, nos casos legalmente previstos, incluindo rendimentos oriundos de fornecimento de bens ou da prestação de serviços.

8.2.2. A base de cálculo para a retenção corresponderá ao valor bruto constante da Nota Fiscal/Fatura, deduzidos os descontos incondicionais e abatimentos, aplicando-se as alíquotas vigentes conforme a natureza do serviço prestado, nos termos da legislação federal pertinente.

8.2.3. O valor retido será recolhido pela CONTRATANTE aos cofres públicos, em nome da CONTRATADA, constando na documentação fiscal o respectivo destaque da retenção, de modo a possibilitar a compensação ou dedução futura pela CONTRATADA, conforme a legislação tributária.

8.2.4. A retenção do Imposto de Renda na fonte não exclui nem substitui as demais obrigações tributárias da CONTRATADA, inclusive aquelas de natureza municipal, estadual, previdenciária ou trabalhista, devendo esta manter-se regular perante todos os órgãos competentes, sob pena de suspensão do pagamento até a regularização.

8.2.5. Na hipótese de a CONTRATADA se enquadrar em situação de imunidade, isenção ou regime especial que a desobrigue da retenção do Imposto de Renda, deverá apresentar, antes da emissão da primeira nota fiscal, a documentação comprobatória emitida por autoridade competente, sob pena de ser realizada a retenção conforme as normas gerais.

8.2.6. O não atendimento às disposições desta cláusula poderá ensejar a retenção dos valores correspondentes, até a devida regularização fiscal, sem prejuízo das sanções administrativas cabíveis previstas na legislação e neste Contrato.

9. CLÁUSULA NONA – DA FISCALIZAÇÃO

9.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

10. CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES DA CONTRATADA

10.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

11. CLÁUSULA DÉCIMA PRIMEIRA – DAS OBRIGAÇÕES DA CONTRATANTE

11.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

12. CLÁUSULA DÉCIMA SEGUNDA – DAS SANÇÕES E PENALIDADES

12.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

13. CLÁUSULA DÉCIMA TERCEIRA – DO REAJUSTE, ACRÉSCIMO E SUPRESSÃO (SE HOUVER)

13.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

14. CLÁUSULA DÉCIMA QUARTA – DA RESCISÃO CONTRATUAL

14.1 A inexecução total ou parcial do contrato enseja a sua rescisão, com as consequências contratuais e as previstas em lei ou regulamento.

14.2 Constituem motivo para rescisão de contrato:

I - O não cumprimento de cláusulas contratuais, especificações, projetos ou prazos.

II - O cumprimento irregular de cláusulas contratuais, especificações, projetos e prazos.

III - A lentidão do seu cumprimento, levando a Administração a comprovar a impossibilidade da conclusão do serviço ou do fornecimento, nos prazos estipulados.

IV - O atraso injustificado no início do serviço ou fornecimento.

V - A paralisação do serviço ou do fornecimento, sem justa causa e prévia comunicação à Administração.

14.3 Poderão ser motivos de rescisão contratual, as hipóteses descritas no art. 137 da Lei 14.133/2021, podendo a mesma ser unilateral, consensual, ou determinada por decisão arbitral, nos termos e condições do art. 138, incisos I, II e III, da referida lei.

14.4 A CONTRATADA reconhece os direitos da CONTRATANTE nos casos do Art. 138, § 2º, I, II e II da Lei 14.133/2021.

14.5 Concluída a licitação, a contratante tem a prerrogativa de resolver o contrato (Acórdão 3474/2018-Segunda Câmara do TCU), mediante prévia notificação com antecedência mínima de 30 (trinta) dias.

15. CLÁUSULA DÉCIMA QUINTA – MATRIZ DE RISCOS

15.1 - Na hipótese de ocorrência de um dos eventos listados no Anexo - Matriz de Riscos deste Contrato, a CONTRATADA deverá, no prazo de 01 (um) dia útil, informar a SESAU/RO sobre o ocorrido, contendo as seguintes informações mínimas:

a) Detalhamento do evento ocorrido, incluindo sua natureza, a data da ocorrência e sua duração estimada;

b) As medidas que estavam em vigor para mitigar o risco de materialização do evento, quando houver;

c) As medidas que irá tomar para fazer cessar os efeitos do evento e o prazo estimado para que esses efeitos cessem;

d) As obrigações contratuais que não foram cumpridas ou que não irão ser cumpridas em razão do evento; e,

e) Outras informações relevantes.

15.1.1 - Após a notificação, a SESAU/RO decidirá quanto ao ocorrido ou poderá solicitar esclarecimentos adicionais a CONTRATADA. Em sua decisão a SESAU/RO poderá isentar temporariamente a CONTRATADA do cumprimento das obrigações contratuais afetadas pelo Evento.

15.1.2 - A concessão de qualquer isenção não exclui a possibilidade de aplicação das sanções previstas na Cláusula contratual respectiva.

15.1.3 - O reconhecimento pela SESAU/RO dos eventos descritos na Matriz de Riscos deste Contrato que afetem o cumprimento das obrigações contratuais, com responsabilidade indicada exclusivamente a CONTRATADA, não dará ensejo a recomposição do equilíbrio econômico financeiro do Contrato, devendo o risco ser suportado exclusivamente pela CONTRATADA.

15.2 - As obrigações contratuais afetadas por caso fortuito, fato do príncipe ou força maior deverão ser comunicadas pelas partes em até 01 (um) dia útil, contados da data da ocorrência do evento.

15.2.1 - As partes deverão acordar a forma e o prazo para resolução do ocorrido.

15.2.2 - As partes não serão consideradas inadimplentes em razão do descumprimento contratual decorrente de caso fortuito, fato do príncipe ou força maior.

15.2.3 - Avaliada a gravidade do evento, as partes, mediante acordo, decidirão quanto a recomposição do equilíbrio econômico financeiro do Contrato, salvo se as consequências do evento sejam cobertas por Seguro, se houver.

15.2.3.1 - O Contrato poderá ser rescindido, quando demonstrado que todas as medidas para sanar os efeitos foram tomadas e mesmo assim a manutenção do contrato se tornar impossível ou inviável nas condições existentes ou é excessivamente onerosa.

15.2.4 - As partes se comprometem a empregar todas as medidas e ações necessárias a fim de minimizar os efeitos advindos dos eventos de caso fortuito, fato do príncipe ou força maior.

15.3 - Os fatos imprevisíveis, ou previsíveis, porém de consequências incalculáveis, retardadores ou impeditivos da execução do contrato, não previstos na Matriz de Riscos, serão decididos mediante acordo entre as partes, no que diz respeito à recomposição do equilíbrio econômico financeiro do contrato.

16. CLÁUSULA DÉCIMA SEXTA - DA FRAUDE E CORRUPÇÃO

16.1. A CONTRATADA deverá observar os mais altos padrões éticos durante a execução do Contrato, estando sujeitas às sanções previstas na legislação em caso de inobservância.

17. CLÁUSULA DÉCIMA SÉTIMA – DOS CASOS OMISSOS

17.1. As omissões, dúvidas e casos não previstos neste instrumento, serão resolvidos e decididos aplicando-se as regras da Lei nº 14.133/21 e suas alterações, bem como demais ordenamentos jurídicos correlatos, levando-se sempre em consideração os princípios que regem a administração pública.

18. CLÁUSULA DÉCIMA OITAVA – DA PUBLICAÇÃO

18.1. Incumbirá à CONTRATANTE, através da Procuradoria Geral do Estado, providenciar a publicação deste instrumento, por extrato, no Diário Oficial do Estado de Rondônia, no prazo previsto na Lei nº 14.133/21.

19. CLÁUSULA DÉCIMA NONA – DO FORO

19.1. Fica eleito pelas partes o Foro da Comarca de Porto Velho, Capital do Estado de Rondônia, para dirimir todas e quaisquer questões oriundas do presente ajuste, inclusive às questões entre a CONTRATADA e a CONTRATANTE, decorrentes da execução deste CONTRATO, com renúncia expressa de qualquer outro, por mais privilegiado que seja.

20. CLÁUSULA VIGÉSIMA - DAS DISPOSIÇÕES GERAIS

20.1. Ficam aquelas estabelecidas no Termo de Referência, as quais foram devidamente aprovadas pelo ordenador de despesa do órgão requerente.

Para firmeza e como prova do acordado, é lavrado o presente Contrato, o qual, depois de lido e achado conforme, vai assinado pelas partes, dele sendo extraídas as cópias que se fizerem necessárias para sua publicação e execução, devidamente certificadas pela Procuradoria Geral do Estado.

Porto Velho/RO, _____de_____ de 202_.

_____

Titular da Contratante

_____

Titular da contratada

_____

Procurador do Estado de Rondônia

Anexo III - Mapa de Risco (0051897532)

Risco	Descrição	Possíveis Causas	Fase	Nível	Ações Preventivas	Controle de Contingência	Responsável
Impugnação do edital de licitação	Impugnação do edital por participantes, atrasando o processo licitatório.	Edital mal redigido, cláusulas ambíguas.	Licitação	Alto	Revisar o edital detalhadamente antes da publicação, consulta pública prévia.	Responder prontamente às impugnações e corrigir o edital se necessário.	SUPEL
Falta de propostas qualificadas	Poucas ou nenhuma proposta que atendam aos requisitos da licitação.	Divulgação insuficiente, requisitos muito restritivos.	Licitação	Alto	Divulgação ampla da licitação, reuniões de esclarecimento com possíveis interessados.	Realizar nova licitação com ajustes nos requisitos.	Unidade requisitante / GECOMP
Problemas na análise de propostas	Erros ou falhas na análise das propostas recebidas, levando a recursos e atrasos.	Falta de capacitação da comissão, critérios de avaliação mal definidos.	Licitação	Médio	Treinamento da comissão de licitação, estabelecimento de critérios claros de avaliação.	Revisão das propostas por uma equipe secundária, se necessário.	SUPEL

Risco	Descrição	Possíveis Causas	Fase	Nível	Ações Preventivas	Controle de Contingência	Responsável
Recursos administrativos	Interposição de recursos administrativos pelos participantes, atrasando o processo.	Falta de transparência, erros na análise.	Licitação	Médio	Garantir transparência e clareza no processo licitatório.	Responder rapidamente aos recursos e corrigir possíveis falhas.	SUPEL
Irregularidades na documentação dos proponentes	Documentação incompleta ou irregular dos participantes da licitação.	Falta de verificação detalhada.	Licitação	Médio	Verificação rigorosa da documentação durante a fase de habilitação.	Dar prazo para regularização e verificar novamente.	SUPEL
Fraude ou conluio entre participantes	Tentativas de manipulação do processo licitatório por conluio entre os participantes.	Falta de monitoramento e auditoria.	Licitação	Alto	Monitoramento contínuo e auditoria do processo licitatório.	Denúncia às autoridades competentes, cancelamento da licitação.	SUPEL
Problemas de comunicação entre as partes	Falhas na comunicação entre SESAU e a empresa contratada.	Falta de canais de comunicação definidos, reuniões insuficientes.	Execução	Médio	Estabelecer canais de comunicação claros, reuniões regulares de acompanhamento.	Implementação de sistema de gestão de comunicação.	Fiscal de contrato / Gerência de contratos
Atraso	Atraso na entrega das soluções	Problemas logísticos; Fornecedor enfrenta dificuldades operacionais	Execução	Médio	Cronograma claro e monitoramento constante do progresso; Penalidades contratuais por atrasos	Negociação com a contratada para resolução rápida; Escalonamento para gerência de contratos	Fiscal de contrato / Gerência de contratos
Dificuldade em atender aos requisitos	Dificuldade em atender aos requisitos regulatórios de segurança	Mudanças nas regulamentações; Falta de atualização das soluções	Execução	Médio	Acompanhamento contínuo das regulamentações aplicáveis; Reuniões periódicas com a contratada para alinhamento	Implementação de soluções complementares; Revisão do contrato para inclusão de novas exigências	Unidade requisitante, Fiscal de contrato

Anexo IV - Adendo Matriz de Riscos (0051893000)

Risco	Descrição	Alocação de Risco		
		Contratante	Contratada	Compartilhada
Aumento de Volume de Dados	Expansão no volume de dados trafegados e armazenados, exigindo maior capacidade de processamento e armazenamento pela solução.			X
Evolução Tecnológica Rápida	Surgimento de novas tecnologias ou técnicas de ataque que possam exigir a atualização ou substituição antecipada da solução contratada.		X	

Risco	Descrição	Alocação de Risco		
Alteração de Normativas	Mudança em regulamentações de segurança da informação que exijam adaptações ou complementos à solução contratada.			X
Variação Cambial	Oscilações no valor da moeda que impactem o custo de licenças e equipamentos importados, afetando o equilíbrio econômico-financeiro do contrato.	X		
Indisponibilidade de Insumos	Falta de componentes ou equipamentos necessários para a implementação ou manutenção da solução de segurança.		X	
Incidente de Segurança Crítico	Ocorrência de um incidente de segurança que exija uma resposta imediata e possivelmente fora do escopo contratual.			X
Atraso na Entrega de Equipamentos	Problemas logísticos que causem atraso na entrega de hardware ou software necessários para a solução de segurança.		X	
Aumento na Demanda por Suporte Técnico	Crescimento inesperado na demanda por suporte técnico devido a falhas recorrentes ou aumento de incidentes de segurança.			X
Falha no Repasse de Conhecimento	Problemas na transferência de conhecimento para a equipe interna da Secretaria, resultando em dificuldades operacionais.		X	
Mudanças no Cenário de Ameaças	Evolução ou surgimento de novas ameaças cibernéticas que exijam ajustes na estratégia de segurança inicialmente planejada.			X
Obsolescência Tecnológica	Acelerada obsolescência dos componentes tecnológicos utilizados na solução, requerendo substituições ou upgrades não previstos.		X	
Interrupção de Suporte pelo Fabricante	Descontinuidade do suporte por parte do fabricante de algum dos softwares ou hardware utilizados na solução contratada.		X	
Mudanças no Perfil de Uso	Alterações significativas no perfil de uso dos sistemas da Secretaria, como aumento de acesso remoto ou novas aplicações, que possam impactar a eficácia da solução de segurança contratada.			X

ANEXO V -Suporte Técnico

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

Severidade 3 **Criticidade**	negócio. Exemplo: Ocorrência de erro que causou impacto negativo limitado na operações.	**Prazo Máximo de Atendimento**	**Prazo Máximo de Restauração de Serviço**	**Glosa (por evento) para eventual descumprimento** 5%
		Em até 6 horas um Engenheiro de Suporte do fabricante entra em contato	Entrega da Solução pelo fabricante em até 15 dias ou na próxima atualização do Software.	
Severidade 4 (Baixa)	O problema é pequeno, ou de documentação. Exemplos:O problema não afetou as operações da contratante negativamente; Encaminhamento de solicitações e ou sugestões para novos	Em até 12 horas um técnico do fornecedor entra em contato.	Em até 12 horas um técnico do fornecedor entra em contato.	2%

Documento assinado eletronicamente por **Allan Junior Alves Siqueira**, **Assessor(a)**, em 14/05/2026, às 14:38, 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 **Joelma Da Silva Teles**, **Assessor(a)**, em 14/05/2026, às 15:04, 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 **ALYSSON ANTONIO DE MELLO CARVALHO** , **Gerente**, em 15/05/2026, às 14:49, 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 **Roselaine de Souza Chaga**, **Secretário(a) Executivo(a)**, em 15/05/2026, às 17:15, 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 **Patrick Hebert da Silva**, **Coordenador(a)**, em 18/05/2026, às 11:05, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **70923055** e o código CRC **6BFBB389**.

GOVERNO DO ESTADO DE RONDÔNIA
Secretaria de Estado da Saúde - SESAU
NÚCLEO DE PROCEDIMENTOS ACESSÓRIOS - SESAU-NPA

RELATÓRIO

RELATÓRIO DE PESQUISA DE PREÇOS

Instrução Normativa nº 01/2024/SUPEL-CPEAP

(Processo Administrativo nº 0036.028242/2024-36)

1. DESCRIÇÃO DO OBJETO A SER CONTRATADO (art. 3º, inc. I)

Objeto: O Relatório da Pesquisa de Preços foi elaborada em atenção ao Art. 51 do Decreto Estadual nº 28.874/2024 e Art. 23 da Lei Federal nº 14.133/2024 . Destaca-se que a Pesquisa de preços foi elaborada por este agente tecnicamente capaz de definir quantitativa e qualitativamente as necessidades do objeto, visando Registro de Preços para contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da Secretaria de Estado da Saúde - SESAU/RO, por um período de 3 (três) anos. , conforme descrito no Documento de Oficialização de Demanda - DOD (0054733868) de justificativa id. 0049992803., conforme Art. 106 da Lei Federal nº 14.133 de 1° de abril de 2021.

Esta Justificativa, como ressaltado pelo Professor Ulysses Jacoby, transcende a mera aceitação do preço imposto pelo contratado, demandando uma análise ampla da compatibilidade do valor contratado com o mercado, aferida por meio de métodos que assegurem a economicidade e a adequação aos parâmetros legais. Nesse contexto, a presente justificativa busca fornecer esclarecimentos consistentes e embasados para dissipar quaisquer dúvidas quanto à idoneidade e coerência do processo de contratação em questão, alinhando-se aos princípios basilares que regem as contratações públicas.

2. METODOLOGIA APLICADA

Assim, no presente processo será considerado a metodologia de ordem sub-sequencial constante no art. 23 da Lei Federal nº 14.133/2021, vejamos:

Art. 1º O valor previamente estimada da contratação deverá ser compatível com os valores praticados pelo mercado, considerados os preços constantes de banco de dados públicos e as quantidades a serem contratadas, observadas a potencial economia de escala e as peculiaridades do local de execução do objeto.

Parágrafo único. No processo licitatório para aquisição de bens e contratação de serviços em geral, conforme regulamento, o valor estimado será definido com base no melhor preço aferido por meio da utilização dos seguintes parâmetros, adotados de forma combinada ou não:

I - composição de custos unitários menores ou iguais à mediana do item correspondente no painel para consulta de preços ou no banco de preços em saúde disponíveis no Portal Nacional de Contratações Públicas (PNCP);

II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;

III - utilização de dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que contenham a data e hora de acesso;

IV - pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital;

V - pesquisa na base nacional de notas fiscais eletrônicas, na forma de regulamento.

Em análise ao Decreto Estadual nº 28.874/2024 que regulamenta licitações no âmbito do Governo do estado de Rondônia, percebe-se que a fonte preferencial a ser adotada nas estimativas de preços é banco ou painel de preços, vejamos:

Art. 2º pesquisa de preços deverá ser realizada da forma mais ampla possível e de acordo com o regramento do art. 23, da Lei Federal n° 14.133, de 2021.

Parágrafo único. como fonte preferencial para elaboração de estimativa de valor de veículos oficiais de divulgação de valores referenciais, tais como bancos ou painéis de preços.

Para definição do valor de referência, poderá ser aplicada a metodologia estatística prevista no art. 6º da **IN nº 01/2024/SUPEL-CPEAP**:

Mediana: quando o Coeficiente de Variação (CV) foi superior a 25,99%.

Média: quando o CV foi inferior a 25,99%.

Menor Preço: nos casos de mercado restrito, com poucos fornecedores ou único fabricante, conforme o **Acórdão nº 1850/2020 do TCU**.

Antes da escolha do método, os preços foram ordenados e submetidos à medida saneadora, com aplicação do **desvio padrão de 25%**, visando eliminar valores excessivos ou inexequíveis (**outliers**).

(**outliers**).

I - Painel de Preços (SEI nº 68241097)

No processo em análise, a busca por parâmetros de definição de preço incluiu a verificação da existência de contratações comparáveis no painel de preços conforme preconizado pela legislação pertinente. Não Fora encontrado resultado para o objeto em questão conforme consta no relatório (SEI nº 68241097) por problemas no site.

II - Banco de Preços (SEI nº 68241045)

Em análise ao banco de preços (68241045) foram localizados valores de balizamento para o Registro de Preços para contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da Secretaria de Estado da Saúde - SESAU/RO, por um período de 3 (três) anos, conforme descrito no Documento de Oficialização de Demanda - DOD (0054733868) de justificativa id. 0049992803., conforme Art. 106 da Lei Federal nº 14.133 de 1° de abril de 2021.

Em análise mais detalhada dos valores, verifica-se que o objeto dos contratos se assemelha ao pretendido na contratação, sendo possível assim a utilização dos valores constantes no Relatório Banco de Preços.

III - Banco de Preços em saúde.

O dispositivo de Banco de Preços em Saúde disponível não se aplica a presente contratação, visto que a Contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da Secretaria de Estado da Saúde - SESAU/RO, por um período de 3 (três) anos e o portal citado é com finalidade de registro de medicamentos e dispositivos médicos:

O Banco de Preços em Saúde - BPS é um sistema de registro de informações de compras públicas e privadas de medicamentos e dispositivos médicos que existe desde 1998. Sua principal finalidade é possibilitar o uso de informações de compras públicas e privadas de medicamentos e dispositivos médicos, a fim de subsidiar a compra pública mais eficiente no setor saúde, pelos entes federados e instituições de saúde.

IV - Portal Nacional de Contratações Públicas (68241084).

No intuito de atender ao preceito normativo que preconiza a busca por contratações similares realizadas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, buscou-se diligentemente informações que pudessem subsidiar a análise e definição de preços para o presente processo.

Em busca pormenorizada de contratações similares, foram localizadas Contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da Secretaria de Estado da Saúde - SESAU/RO, por um período de 3 (três) anos.

V - Utilização de dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo.

Em conformidade com o disposto no Decreto Estadual nº 28.874/2024, que regulamenta as contratações públicas no âmbito do Governo do Estado de Rondônia, a pesquisa de preços deve observar, preferencialmente, as fontes estabelecidas no referido normativo, buscando garantir a fidedignidade dos valores estimados e a seleção da proposta mais vantajosa à Administração.

No entanto, a utilização de dados provenientes de mídia especializada, tabelas de referência formalmente aprovadas pelo Poder Executivo Federal ou de sítios eletrônicos especializados ou de domínio amplo não se mostrou adequada para a presente estimativa, pelos seguintes motivos:

1. **Incompatibilidade técnica e especificações distintas** – As informações disponíveis nas referidas fontes não contemplam as especificações técnicas exatas dos itens demandados, apresentando variações de marca, modelo, configuração ou características que poderiam comprometer a exatidão da estimativa.

2. **Desatualização ou ausência de dados regionais** – As tabelas e mídias consultadas não apresentam valores atualizados ou não refletem a realidade de mercado local, especialmente no contexto regional do Estado de Rondônia, podendo gerar distorções na formação do preço estimado.

3. **Falta de representatividade comercial** – As mídias e sítios eletrônicos consultados não possuem abrangência suficiente para retratar as condições comerciais efetivamente praticadas por fornecedores que atuam na localidade, o que inviabiliza a adoção de seus valores como base comparativa.

4. **Predominância de fontes mais aderentes** – Optou-se por adotar, de forma fundamentada, outras fontes de pesquisa de preços mais adequadas e fidedignas, tais como cotações diretas junto a fornecedores do ramo, atas de registro de preços vigentes ou contratações recentes realizadas por órgãos públicos, que demonstraram maior conformidade com o objeto e com o mercado local.

Dessa forma, a não utilização das referidas fontes se justifica pela necessidade de assegurar a precisão e a confiabilidade da estimativa de preços, em observância aos princípios da economicidade, da razoabilidade e da eficiência previstos no Decreto Estadual nº 28.874/2024 e na Lei Federal nº 14.133/2021.

VI - Pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital.

A utilização de pesquisa direta com fornecedores locais deve ser observada com cautela pela Administração Pública durante a elaboração da estimativa, de forma que possa aferir que de fato os valores refletem a realidade do mercado. A Instrução Normativa/SEGES-ME nº 65 de 07 de julho de 2021 estabeleceu que a Lei 14.133/2021 dispõe que os cinco parâmetros citados podem ser adotados de forma combinada ou não, **acrescenta que deverão ser priorizados os dois primeiros parâmetros, ou seja, o módulo integrado para pesquisa de preços no sistema Compras.gov.br; e as contratações similares feitas pela Administração Pública.** As demais fontes devem ser utilizadas de forma complementar ou subsidiária, com as devidas justificativas, **devendo ser evitada a cotação somente junto a potenciais fornecedores,** vejamos:

Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição de bens e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:

I - composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou banco de preços em saúde, observado o índice de atualização de preços correspondente;

II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;

III - dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso;

IV - pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; ou

V - pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data de divulgação do edital, conforme disposto no Caderno de Logística, elaborado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.

§ 1º Deverão ser priorizados os parâmetros estabelecidos nos incisos I e II, devendo, em caso de impossibilidade, apresentar justificativa nos autos. (grifo nosso)

O Decreto Estadual nº 28.874/2024, através do art. 51 regulamentou as formas de pesquisa de preços previstas no art. 23 da Lei Federal nº 14.133/2021, e definiu-se como base preferencial para os preços os valores de veículos oficiais, tais como bancos ou painéis de preços, bem como ainda exigindo a justificativa quando a pesquisa realizada somente por meio de pesquisa de mercado:

Art. 51.A pesquisa de preços deverá ser realizada da forma mais ampla possível e de acordo com o regramento do art. 23, da Lei Federal n° 14.133, de 2021.

§ 1°Adotar-se-á como fonte preferencial para elaboração de estimativa de valor de veículos oficiais de divulgação de valores referenciais, tais como bancos ou painéis de preços.

§ 2°A realização de estimativa de valor exclusivamente por meio de pesquisa de mercado somente será admitida em caso de expressa justificativa do setor responsável, devendo ser observada a pluralidade e atualidade das propostas com a correspondente justificativa de escolha dos agentes econômicos pesquisados.

O Tribunal de Contas da União através do Acórdão nº 1.875/2021-Plenário já definiu que os valores deverão ser baseados em cestas de preços, sendo preferencialmente os preços públicos oriundos de outros certames e somente utilizado pesquisa junto a fornecedores em caso de ausência extrema de preços públicos, vejamos:

9.5.1. as pesquisas de preços para estimativa de valor de objetos a serem licitados devem ser baseadas em uma "cesta de preços", devendo dar preferência para preços públicos, oriundos de outros certames;

9.5.2. a pesquisa de preços feita exclusivamente junto a fornecedores deve ser utilizada em último caso, **na extrema ausência de preços públicos ou cestas de preços referenciais;**

Diante disso, percebe-se que não existiu necessidade no processo a realização de pesquisa com fornecedores locais, considerando a existência de preços públicos que possibilitem a realização da cesta de preços e estimativa necessária.

3. SÉRIE DE PREÇOS COLETADOS (art. 3º, inc. IV)

ITEM	ESPECIFICAÇÃO	UNIDADE	QUANTIDADE	EMPRESA ITPROTECT	PNCP 1	PNCP 2	BANCO DE PREÇOS 1	BANCO DE PREÇOS 2	BANCO DE PREÇOS 3	MENOR VALOR	VALOR MEDIANO	VALOR MÉDIA	DESVIO PADRÃO	COEFICIENTE DE VARIAÇÃO	PARÂMETRO UTILIZADO	VALOR TOTAL
01	Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes	Por Endpoint	2150	R$ 483,21	R$ 539,25	R$ 832,55	R$ 800,00	R$ 693,10	N/C	R$ 483,21	R$ 693,10	**R$ 669,62**	R$ 154,79	23,12%	MÉDIA	**R$ 1.439.683,00**

02	Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes	Por Servidor	139	R$ 4.390,00	R$ 4.200,00	R$ 5.037,50	R$ 4.200,00	R$ 5.000,00	R$ 5.700,00	R$ 4.200,00	R$ 4.695,00	**R$ 4.754,58**	R$ 597,01	12,56%	MÉDIA	**R$ 660.886,62**
03	Solução de segurança avançada para mitigação de ameaças na rede	Por Throughput de dados	2	R$ 3.600.000,00	R$ 3.996.162,02	R$ 4.295.547,05	R$ 3.295.000,00	R$ 3.901.534,00	R$ 3.640.000,00	R$ 3.295.000,00	R$ 3.770.767,00	**R$ 3.778.040,51**	R$ 350.463,23	9,25%	MÉDIA	**R$ 7.576.081,02**
04	Solução de prevenção de intrusão de próxima geração (NGIPS)	Por Throughput de dados	4	R$ 2.025.000,00	R$ 2.648.300,11	R$ 2.849.774,40	R$ 2.648.300,11	R$ 1.750.000,00	R$ 2.846.016,00	R$ 1.750.000,00	R$ 2.648.300,11	**R$ 2.461.231,77**	R$ 461.554,37	18,75%	MÉDIA	**R$ 9.844.927,08**
05	Serviço de suporte pro ativo, corretivo e para resposta a incidentes	Por Solução	4	R$ 401.500,00	R$ 582.000,00	R$ 430.000,00	R$ 581.790,63	R$ 430.000,00	R$ 450.000,00	R$ 401.500,00	R$ 440.000,00	**R$ 479.215,11**	R$ 81.023,31	16,91%	MÉDIA	**R$ 1.916.860,44**
06	Serviço de implantação	Por Solução	4	R$ 45.000,00	R$ 39.088,92	R$ 35.000,00	R$ 36.000,00	R$ 32.575,00	R$ 35.000,00	R$ 32.575,00	R$ 35.500,00	**R$ 37.110,65**	R$ 4.401,61	11,86%	MÉDIA	**R$ 148.442,60**
07	Serviço de capacitação e repasse de conhecimento	40 Horas	2	R$ 35.000,00	R$ 42.500,00	R$ 30.000,00	R$ 42.500,00	R$ 30.000,00	R$ 40.200,00	R$ 30.000,00	R$ 37.600,00	**R$ 36.700,00**	R$ 5.868,56	15,99%	MÉDIA	**R$ 73.400,00**
															VALOR TOTAL ANUAL	**R$ 21.660.280,76**

VALOR ESTIMADO ANUAL DA CONTRATAÇÃO R$ 21.660.280,76 (vinte e um milhões seiscentos e sessenta mil duzentos e oitenta reais e setenta e seis centavos).

4. DA ANÁLISE DOS VALORES OBTIDOS E DEFINIÇÃO DE VALOR DE REFERÊNCIA

Diante do exposto, considerando que o Decreto Estadual nº 28.874/24 define em seu Art. 53:

Art. 3º resultado da pesquisa de preços será a **média, mediana ou o menor dos preços obtidos**, observados os seguintes parâmetros:

I - para a obtenção do resultado da pesquisa de preços, deverá ser realizada análise crítica dos preços pesquisados, a fim de verificar eventuais propostas cujos preços possam ser considerados inexequíveis ou excessivamente elevados e, ainda, verificar a similaridade com o objeto, especificações, qualidade, prazos e garantias definidos pela Administração;

II - o responsável deverá fazer um balizamento entre o resultado obtido e os preços praticados no âmbito dos órgãos e entidades da Administração Pública, através da análise de contratos recentes ou vigentes, Atas de Registro de Preços e outros meios para verificar se o resultado apresenta o preço praticado no mercado.

Sugere-se no presente processo, a utilização do critério média de preço para a definição do Registro de Preços para contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da Secretaria de Estado da Saúde - SESAU/RO, por um período de 3 (três) anos. , conforme descrito no Documento de Oficialização de Demanda - DOD (0054733868) de justificativa id. 0049992803., conforme Art. 106 da Lei Federal nº 14.133 de 1° de abril de 2021.

Os documentos que deram suporte para justificar o tratamento dado aos preços coletados, bem como a metodologia que foi aplicada encontram-se anexos aos autos, conforme pesquisas de Preços (68216967) Portal Nacional de Contratações Públicas (68241084), Banco de Preços (68241045), Painel de Preços Negativo (68241097) e **Orçamento da Empresa ITPROTECT (68238823)**, os quais contemplam os preços praticados no âmbito dos órgãos e entidades da Administração Pública.

5. CONCLUSÃO

Em conclusão, ratificamos que a pesquisa de preços realizada para embasar o presente certame seguiu criteriosamente os preceitos estabelecidos na legislação vigente. O parâmetro estabelecido no art. 51, §8º do Decreto Estadual nº 28.874/2024 foi cuidadosamente cumprido e obtido preço através de ampla cesta de preços utilizada para estimativa do valor do plantão e definição da planilha de custo, demonstrando a diligência da administração na busca por referências adequadas para a definição dos valores estimados.

Visto isso e considerando o caso concreto, diante da conformidade com os dispositivos legais e da adequada justificação dos parâmetros utilizados, o presente processo demonstra o compromisso da administração em conduzir uma pesquisa de preços idônea e alinhada aos princípios da Administração Pública, assegurando, dessa forma, a lisura e a legalidade do procedimento de contratação, atendendo ainda o princípio da economicidade pública, tendo o processo o valor estimado de **R$ 21.660.280,76 (vinte e um milhões seiscentos e sessenta mil duzentos e oitenta reais e setenta e seis centavos).**

Porto Velho/RO, data e hora do sistema.

MARCOS EDUARDO IGNÁCIO REGO
NÚCLEO DE PROCEDIMENTOS ACESSÓRIOS - SESAU-NPA

JUNIOR SANTANA DE ARAUJO
CHEFE DE NÚCLEO - SESAU/NPA

SESAU RO GOV

Documento assinado eletronicamente por **Junior Santana de Araujo**, **Chefe de Núcleo**, em 15/01/2026, às 11:27, 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 **Marcos Eduardo Ignacio Rego**, **Assessor(a)**, em 15/01/2026, às 11:48, 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 **68244109** e o código CRC **AF01FF54**.

GOVERNO DO ESTADO DE RONDÔNIA

Secretaria de Estado da Saúde - SESAU

NÚCLEO DE SERVIÇOS CONTINUADOS - SESAU-NSC

SAMS

Solicitação de Aquisição de Materiais/Serviços – SAMS

DESCRIÇÃO DA DESPESA	
Registro de Preços para contratação de empresa para fornecimento, sob demanda, de solução de segurança para proteção de e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da Secretaria de Estado da Saúde - SESAU/RO, por um período de 1 (um) anos, conforme descrito no Documento de Oficialização de Demanda - DOD (0054733868) de justificativa id. 0049992803., conforme Art. 107 da Lei Federal nº 14.133 de 1° de abril de 2021.	
Resposta ao:	Memorando 1123 (0050620201)

PROGRAMA DE TRABALHO	UNIDADE ATENDIDA	FONTE DE RECURSO	NATUREZA DA DESPESA
17.012.10.126.1015.2064 - PROMOVER A GESTÃO DE T.I	Coordenadoria de Inovação e Tecnologia da Informação - CITI	1.500.0.01002 - Recursos não vinculados de impostos - Saúde 2.500.0.01002 - Recursos não vinculados de impostos do exercício anterior - Saúde .	3.3.90.39 - Outros Serviços de Terceiros - PJ 3.3.90.40 - Serviços de Tecnologia da Informação e Comunicação - Pessoa Jurídica

GRUPO ÚNICO	ITEM	ESPECIFICAÇÃO	UND	QTD	VALOR UNITÁRIO R$	VALOR TOTAL R$
01	01	Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes	Por Endpoint	2150		
	02	Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes	Por Servidor	139		
	03	Solução de segurança avançada para mitigação de ameaças na rede	Por Throughput de dados	2		
	04	Solução de prevenção de intrusão de próxima geração (NGIPS)	Por Throughput de dados	4		
	05	Serviço de suporte pro ativo, corretivo e para resposta a incidentes	Por Solução	4		
	06	Serviço de implantação	Por Solução	4		
	07	Serviço de capacitação e repasse de conhecimento	40 Horas	2		
VALOR TOTAL:						

<table>
<tr><td rowspan="3">Carimbo do CNPJ/CPF-ME:</td><td>Local:</td><td>Responsável pela cotação da Empresa:</td><td rowspan="3">USO EXCLUSIVO DA SUPEL</td><td>Valor da Proposta: R$</td></tr>
<tr><td>Data:</td><td>Fone:</td><td rowspan="2">Validade Proposta: 90 (Noventa) dias</td></tr>
<tr><td>Banco:
Agência:
C/C:</td><td>Assinatura:</td><td>Prazo de Entrega:</td></tr>
</table>

Porto Velho, data e hora certificada.

Elaborado por:

ALLAN JUNIOR ALVES SIQUEIRA
Assessor NSC/CECOMP/CAD

Revisado por:
JOELMA DA SILVA TELES
Responsável Núcleo de Serviços Continuados - SESAU-NSC

Revisado por:
ALYSSON ANTONIO DE MELLO CARVALHO
Gerência de Compras - CECOMP/CAD

Revisado por:
COORDENADORIA DE INOVAÇÃO E TECNOLOGIA DA INFORMAÇÃO (SESAU-CITI)

Autorizo Na Forma da Lei, *Autorizo o presente Termo de Referência e SAMS* , declaro e dou fé destes.

ROSELAINE DE SOUZA CHAGA
Secretária Executiva de Estado da Saúde

SESAU Secretaria de Estado da Saúde — RONDÔNIA Governo do Estado

Documento assinado eletronicamente por **Joelma Da Silva Teles**, **Assessor(a)**, em 13/05/2026, às 14:47, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

Documento assinado eletronicamente por **Allan Junior Alves Siqueira**, **Assessor(a)**, em 14/05/2026, às 14:38, 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 **ALYSSON ANTONIO DE MELLO CARVALHO**, **Gerente**, em 14/05/2026, às 15:01, 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 **Roselaine de Souza Chaga**, **Secretário(a) Executivo(a)**, em 15/05/2026, às 17:15, 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 **Patrick Hebert da Silva**, **Coordenador(a)**, em 18/05/2026, às 11:05, conforme horário oficial de Brasília, com fundamento no artigo 18 caput e seus §§ 1º e 2º, do Decreto nº 21.794, de 5 Abril de 2017.

A autenticidade deste documento pode ser conferida no site portal do SEI, informando o código verificador **71034668** e o código CRC **3FEE15BB**.

Referência: Caso responda este(a) SAMS, indicar expressamente o Processo nº 0036.028242/2024-36 SEI nº 71034668

SESAU
SECRETARIA DE ESTADO DE SAÚDE

RONDÔNIA
Governo do Estado

MANUAL DE GESTÃO E FISCALIZAÇÃO DE CONTRATOS

Edição 2024
Porto Velho,
Rondônia, 2024.

MANUAL DE GESTÃO E FISCALIZAÇÃO DE CONTRATOS

1ª Edição

Porto Velho/RO

Secretaria de Estado de Saúde 2024

Governador do Estado de Rondônia
MARCOS JOSÉ ROCHA DOS SANTOS

Secretário de Estado da Saúde
JEFFERSON RIBEIRO DA ROCHA

Secretário Executivo de Estado da Saúde
ADRIANO FLORES MESSIAS DA SILVA

Secretário Adjunto de Estado da Saúde
ELCIO BARONY DE OLIVEIRA

Texto de
Tamara Cunha de Oliveira
Regiane da Silva Gomes
Luciano Petisco
Ida Maria Dalboni Gonzaga

Revisão
Ernani Marques de Almeida
Maiara Marcelia Lima Santos
Fernando Velasques Gonçalves

Secretaria de Estado da Saúde – SESAU
CNPJ/MF nº 04.287.520/0001-88, com sede na Avenida Farquar, 2.986 – Complexo do Palácio Rio Madeiras (Prédio Rio Machado), Bairro Pedrinhas - Porto Velho/RO

MENSAGEM AO SERVIDOR

Prezados Servidores,

Este Manual Normativo de Acompanhamento dos Contratos Administrativos é um documento do tipo “Manual Normativo”, com o qual se pretende elevar a maturidade administrativa da SESAU, com vistas à harmonização, por meio de diretrizes, procedimentos e normas específicas que deverão ser seguidos, para a consecução de processos adequadamente instruídos.

As diretrizes, procedimentos e normas específicas estabelecidas neste “Manual Normativo”, orientam a gestão e fiscalização de contratos eficaz e eficiente no âmbito da SESAU. Os procedimentos adotados visam fornecer uma estrutura clara e consistente para o acompanhamento, execução e fiscalização de contratos administrativos, promovendo transparência, otimização dos recursos e garantindo a conformidade com as cláusulas contratuais, regulamentações e normas pertinentes.

A legislação e as melhores experiências administrativas evoluem com o tempo, e o presente documento sempre será uma peça em aperfeiçoamento, na sua proposta de orientação aos seus usuários. Desta forma, abre-se um espaço para eventuais atualizações e a discricionariedade pessoal de cada profissional que exerça as atividades aqui descritas.

O aprimoramento contínuo dos processos de trabalho envolvidos nas atividades de contratações públicas realizadas pela Secretaria de Estado de Saúde também é um destaque e o acompanhamento de contratos administrativos, possui conexão transversal com todas as áreas da SESAU e, portanto, trará grandes benefícios para todos.

Enfim, não podemos nos esquecer de que o propósito aqui é atingir as melhores práticas nas questões de controle, integridade, de transparência, de compliance e na prestação de contas à sociedade. E, automaticamente, resguardando a instituição e seus gestores, nas suas diversas atribuições nas contratações públicas.

Face ao exposto, este Manual Normativo tem como objetivo central estabelecer diretrizes, procedimentos e normas específicas, sob a premissa de orientar os responsáveis pela fiscalização dos contratos no âmbito administrativo.

Secretário de Estado da Saúde
JEFFERSON RIBEIRO DA ROCHA

Secretário Executivo de Estado da Saúde
ADRIANO FLORES MESSIAS DA SILVA

SUMÁRIO

1. FUNDAMENTAÇÃO LEGAL..... 7
1.2. Termos e definições.....9
2. MACROPROCESSO.....15
2.1. Planejamento.....15
2.2. Seleção e Contratação..... 15
2.3. Gerenciamento e Fiscalização do Contrato..... 16
2.4. Gerenciamento de Riscos do Processo de Contratações Públicas..... 16
3.GESTÃO CONTRATUAL.....16
3.1. Gestor do Contrato..... 17
3.2. Das Garantias.....20
3.3. Alterações nos Contratos..... 22
3.4. Paralisação e Reinício para Contratos de Obras..... 24
3.5. Reajuste..... 24
3.6. Revisão - Reequilíbrio Econômico-Financeiro..... 25
3.7. Repactuação..... 26
3.8. Acréscimo/Supressão Contratual.....26
4. FISCALIZAÇÃO CONTRATUAL..... 27
4.1. Fiscalização Técnica..... 28
4.1.1. Fiscalização Técnica de Obras e Serviços de Engenharia..... 30
4.2. Fiscalização Administrativa..... 30
4.2.1. Critérios para Elaboração dos Relatórios Administrativos..... 32
4.2.2. Critérios para Elaboração dos Relatórios com Dedicação Exclusiva.....32
4.2.3. Descumprimento das Obrigações Trabalhistas.....33
4.3. Fiscalização Setorial.....34
4.4. Fiscalização pelo Público Usuário.....35
4.5.1. Designação da Comissão de Fiscalização.....36
4.5.2. Conhecimento Técnico.....37
4.5.3. Acúmulo de Funções.....37
4.5.4. Preposto da Empresa.....38
4.5.5. Inicialização da Fiscalização..... 38
4.5.6. Fiscalização Contratual Técnica Periódica.....40
4.5.7. Fiscalização Contratual Administrativa Mensal.....42
4.5.8. Verificação Quanto ao Cumprimento Contratual.....42
4.5.9. Verificação de Regularidades Fiscais, Sociais e Trabalhistas..... 44
4.5.10. Pesquisa de Situação dos Sócios e da Empresa.....45
4.5.11. Das Penalidades.....47
4.5.12. Verificação da Necessidade de Análise de Riscos..... 48
4.5.13. Preparação e Instrução do Processo para fins de Pagamento ao Fornecedor. 49
5. GESTÃO E FISCALIZAÇÃO DE CONTRATOS ESPECÍFICOS DE SAÚDE.....52

5.1. Do Monitoramento e Avaliação dos Serviços.....52
5.2. Do Reajustamento ao Contrato de Saúde..... 52
5.3. Pagamento - Contrato de Saúde.....53
6. DA COMPETÊNCIA DOS SETORES E PRAZOS..... 54
7. ANEXOS..... 55
8. REFERÊNCIAS.....60

APRESENTAÇÃO

A contratação pública, procedimento para o Estado suprir as suas necessidades de recursos para atender ao interesse público, com a sua complexidade e importância, é processo fundamental para o atendimento da finalidade pública, que consiste em trabalhar para se atender ao interesse público, agindo conforme os princípios constitucionais da legalidade, impessoalidade, moralidade, publicidade, eficiência.

A eficiência de um processo licitatório e do contrato depende do atendimento concreto e efetivo do interesse público, e esta depende da execução do contrato, momento em que é possível mensurar se o interesse público realmente foi atendido. Assim, é de extrema importância a etapa de execução e fiscalização de contratos administrativos é dever da administração, conforme caput do art. 115 e 117 da lei 14.133/21 c/c art. 104 inciso III.

O processo de fiscalização de contratos aborda três etapas distintas: (I) Designação da Comissão de Fiscalização do contrato aos servidores; (II) Inicialização da fiscalização do contrato; (III) Acompanhamento das fiscalizações dos contratos, denominada “Fiscalização Técnica Periódica”; e “Fiscalização Administrativa”, incluindo a gestão de riscos do processo.

Neste contexto, apresenta-se este **Manual de Gestão e Fiscalização de Contratos** da Secretaria de Estado de Saúde de Rondônia (SESAU/RO), doravante denominado Manual, contendo as orientações e os procedimentos para a gestão e fiscalização de contratos, com o propósito de consolidar um conjunto de procedimentos, rotinas, orientações e modelos que facilitem a gestão e fiscalização dos contratos.

Estará a cargo da Secretaria de Estado de Saúde - Coordenação Administrativa (Gerência de Contratos), a manutenção da atualização deste Manual.

Espera-se obter com a implementação bem-sucedida do Manual:

- Assegurar os servidores designados como gestores e fiscais (e substitutos) quanto ao cumprimento das cláusulas contratuais, especificações técnicas e a conformidade legal regulamentar;
- Padronizar os procedimentos de fiscalização de contratos e obter indicadores qualitativos da gestão e fiscalização de contratos na SESAU/RO;
- Aumentar a eficiência e o controle sobre os contratos sob responsabilidade das unidades executoras;
- Aumentar a eficiência na execução dos contratos: obter plena realização de seus objetivos; Maior adequação à legislação;
- Disseminar com maior eficácia as recomendações e determinações emitidas pelos órgãos de controle interno e externo.

Na elaboração deste Manual foram considerados a legislação vigente, além dos impactos de novos fatores no processo de contratações públicas em Rondônia, dos quais se destacam:

- Para nortear os processos de contratação há um grande número de normativos, que se encontram estabelecidos em normativos diversos. Entendemos que a centralização dos normativos e procedimentos relativos às contratações em um manual otimiza tempo e recursos para a realização dos procedimentos relacionados ao processo de contratação;
- A publicação da Lei Federal nº 14.133, de 1º de abril de 2021, conhecida atualmente como a "Nova Lei de Licitações e Contratos", editada para substituir a Lei Federal nº 8.666/93, em fase de implementação no Governo de Rondônia, com as mudanças nas contratações, como, por exemplo, a nova modalidade de contratação, os novos critérios de julgamento, e de outras mudanças em andamento, como adequações em sistemas.

1. FUNDAMENTAÇÃO LEGAL

Inicialmente, cumpre-se destacar que Manual, está em consonância com as referências legais descritas abaixo:

- Lei Federal nº 4.320, de 17 março de 1964, que estatui Normas Gerais de Direito Financeiro para elaboração e controle dos orçamentos e balanços da União, dos Estados, dos Municípios e do Distrito Federal;
- Lei Federal nº 8.666, de 21 de junho de 1993, Lei de Licitações e Contratos da Administração Pública, criada para regular a realização de licitações e o fechamento de contratos da Administração Pública, que estabelece no art. 2º que "As obras, serviços, inclusive de publicidade, compras, alienações, concessões, permissões e locações da Administração Pública, quando contratadas com terceiros, serão necessariamente precedidas de licitação, ressalvadas as hipóteses previstas nesta Lei.";
- Lei Federal nº 10.520, de 17 de julho de 2002, que instituiu no âmbito da União, Estados, Distrito Federal e Municípios, nos termos do art. 37, inciso XXI da Constituição Federal, a modalidade de licitação denominada pregão, para a aquisição de bens e serviços comuns;
- Lei Federal nº 14.133, de 1º de abril de 2021, conhecida como a "Nova Lei de Licitações e Contratos Administrativos", alterando a Lei nº 8.666/93 e a Lei Federal nº 10.520/02, e o seu art. 194, que prevê que "Esta Lei entra em vigor na data de sua publicação", e no art. 193, inciso II que "a Lei nº 8.666, de 21 de junho de 1993, a Lei nº 10.520, de 17 de julho de 2002, e os arts. 1º a 47-A da Lei nº 12.462, de 4 de agosto de 2011, após decorridos 2 (dois) anos a publicação oficial desta Lei.";
- Lei n° 3.830, de 27 de junho de 2016, que regula o processo administrativo no âmbito da Administração Pública do Estado de Rondônia" – Alterada pela Lei n° 5.509, de 21 de dezembro de 2022 (§ 4° do artigo 40 da Lei n° 3.830);
- Decreto nº 16.089, de 28 de julho de 2011 que dispõe sobre o Cadastro Geral de Fornecedores - CAGEFOR, previsto no artigo 34 da Lei Federal nº 8.666, de 21 de junho de 1993, e regulamenta a Lei nº 2.414, de 18 de fevereiro de

2011, que institui o Cadastro de Fornecedores Impedidos de Licitar e Contratar com a Administração Pública Estadual – CAGEFIMP.

- Decreto n° 26.182, de 24 de junho de 2021, que regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia e dispõe sobre o uso da dispensa eletrônica, no âmbito do Poder Executivo do Estado de Rondônia e revoga o Decreto n° 12.205, de 30 de maio de 2006.
- Decreto nº 21.794, de 5 de abril de 2017, que dispõe sobre o uso do Sistema Eletrônico de Informações para realização do processo administrativo no âmbito do Poder Executivo incluindo os Órgãos e as Entidades da Administração Pública Estadual Direta e Indireta e dá outras providências.
- Decreto n° 26.051, de 3 de maio de 2021, que dispõe sobre o conflito de interesses no exercício de cargo ou emprego do Poder Executivo Estadual, os requisitos e restrições a ocupantes de cargo ou emprego que tenham acesso a informações privilegiadas, os impedimentos posteriores ao exercício do cargo ou emprego e as competências para fiscalização, avaliação e prevenção de conflitos de interesses.
- Decreto n° 26.238, de 19 de julho de 2021, que Institui o Programa de Integridade na Administração direta e indireta vinculadas ao Poder Executivo Estadual e dá outras providências.
- Decreto n° 27.382, de 3 de agosto de 2022, que altera, acresce e revoga dispositivos do Decreto n° 16.901, de 9 de julho de 2012 (“Dispõe sobre os critérios para pagamento em ordem cronológica das obrigações decorrentes de contratos regidos pelas Leis Federais n° 14.133/21, n° 8.666/93 e n° 4.320/64, no âmbito da Administração Pública Estadual”);
- Resolução nº 01/2020/CGE-GAB, que dispõe sobre orientações para procedimentos de consultoria em gestão de riscos nas contratações emergenciais do COVID-19 - quando demandado pela alta administração de cada unidade, conforme o art. 3º da Portaria n. 63, de 20 de março 2020;
- Instrução Normativa nº 04 da Secretaria de Logística e Tecnologia da Informação (Órgão Federal), de 11 de setembro de 2014, que dispões sobre o processo de contratação de Soluções de Tecnologia da Informação pelos órgãos integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação – SISP do Poder Executivo Federal;
- Instrução Normativa nº 05 da Controladoria Geral da União (CGU), de 25 de maio de 2017, que dispõe sobre as regras e diretrizes do procedimento de contratação de serviços sob o regime de execução indireta no âmbito da Administração Pública Federal direta, autárquica e fundacional;
- Instrução Normativa nº 73, de 5 de agosto de 2020, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para a aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional;

- Instrução Normativa nº 01/2020/CGE-GAP, que estabelece normas acerca das atribuições de gestores e fiscais de contratos de obras e serviços de engenharia, e dá outras providências;
- Instrução Normativa n° 025/TCE-R0-2009, que disciplina a disponibilização por meio eletrônico de editais de licitação, para fins da análise prévia de que trata o artigo 113, § 2º, da Lei Federal nº 8.666/93.
- Decreto nº 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.

1.2. Termos e definições

A seguir será explicitado os principais termos e suas definições, utilizados em aquisições públicas, extraídos de normativos legais e manuais utilizados na Administração Pública:

Adimplemento Contratual - É o cumprimento de todas as obrigações ajustadas pelas partes, conforme a previsão contratual.

Aditamento Contratual - São alterações do contrato administrativos para melhor adequar às finalidades de interesse público, respeitados os direitos do contratado quer seja por vontade da administração ou por acordo entre as partes.

Apostilamento - É a anotação ou registro administrativo de modificações contratuais que não alteram a essência da avença ou que não modifiquem as bases contratuais. Segundo a Lei nº 14.133/21, artigo 136, a apostila pode ser utilizada nos seguintes casos: Variação do valor contratual para fazer face ao reajuste ou à repactuação de preços previstos no próprio contrato; Atualizações, compensações ou penalizações financeiras decorrentes das condições de pagamento previstas no contrato; Alterações na razão ou na denominação social do contratado; Empenho de dotações orçamentárias.

Área gestora dos contratos - Unidade responsável que realiza todas as atividades administrativas necessárias para a formalização, aditamentos, atualizações, apenações e encerramento contratual. De acordo com a estrutura do órgão ou da unidade contratante, uma ou mais unidades administrativas poderão exercer as atribuições para a gestão dos contratos.

Área requisitante - Trata-se da unidade, que solicita os bens e serviços a serem contratados, e as que irão utilizar após a contratação.

Termo circunstanciado para serviços e obras - Aceitação formal de entrega de bens e/ou serviços realizada pela comissão de recebimento, afirmando estar em conformidade, de acordo com especificação no Termo de Referência e contrato.

Compra - Aquisição de bens e/ou serviços, de forma remunerada, podendo ser entregue de imediato ou parceladamente, prevista no Inciso III, art. 6º, Lei Federal nº 8.666/93, e art. 6º, inciso X da Lei Federal nº 14.133/2021.

Compra direta - Aquisição de bens e/ou serviços, realizada pelas modalidades de dispensa e inexigibilidade de licitação, conforme previsão nos arts. 24 e 25 da Lei nº 8.666/93, de 21 de junho de 1993, e art. 72 a 75 da Lei Federal nº 14.133/2021.

Contrato Administrativo - São ajustes firmados entre a Administração Pública e o fornecedor, que independe da sua denominação, havendo um acordo de vontades formando-se um vínculo, e são estipuladas nele obrigações recíprocas. Podem ser realizados por meio de instrumentos como termo de contrato, carta-contrato, nota de empenho de despesa, autorização de compra ou ordem de execução de serviço. Previsto no art. 62 da Lei Federal nº 8.666/93 e art. 95 da Lei Federal nº 14.133/2021.

Declaração de adequação financeira (DAF) - Documento que atesta a existência de recurso orçamentário e financeiro previsto para cobertura da despesa, e especifica a origem deste recurso.

Estudo Técnico Preliminar - Documento constitutivo da primeira etapa do planejamento de uma contratação que caracteriza o interesse público envolvido e a sua melhor solução e dá base ao anteprojeto, ao termo de referência ou ao projeto básico a serem elaborados caso se conclua pela viabilidade da contratação que servirá de base para a elaboração do Termo de Referência ou Projeto Básico.

Fiscalização do contrato - É o acompanhamento da execução do contrato, e tem por finalidade, verificar o cumprimento das disposições contratuais técnicas, operacionais, administrativas, legais e tributárias, com a verificação e implementação de controles. Bem como, aborda o gerenciamento de riscos. Que por sua vez, será conduzida e realizada pelo contratante (Administração Pública) e seus representantes, por meio de um acompanhamento minucioso e desvelado, nas etapas/fases da execução contratual. Assegurando que a contratada estará respeitando a legislação vigente e cumprindo as suas obrigações contratuais.

Gestão de Contrato - Atividade administrativa que consiste em condutas e procedimentos minuciosos e zelosos a serem aplicados pelo agente público para acompanhamento, controle dos contratos e condução da gestão de riscos. Abrange desde o planejamento da contratação, os demais procedimentos necessários para a sua formalização, como as alterações e a aplicação de penalidades, até o seu encerramento.

Gestão de Riscos - Processo lógico e sistemático que pode ser utilizado para estabelecer base confiável para a tomada de decisões a fim de melhorar a eficácia e a eficiência do desempenho. A gestão de riscos constitui mais que uma estratégia da

organização, mas a política responsável pela definição das diretrizes norteadoras do gerenciamento do risco, entre as quais se insere a definição do apetite ao risco, ou seja, o risco que a organização se dispõe a aceitar para alcançar seus objetivos e metas estratégicas.

Glosa - Trata-se do procedimento destinado a restringir parte do valor indicado em uma fatura, reduzindo-se o preço a ser pago. O valor glosado poderá ser liberado posteriormente, se a retenção teve por objetivo apenas obrigar o contratado a corrigir uma irregularidade, ou não ser mais pago, quando, por exemplo, o serviço não tiver sido realizado integralmente. No primeiro caso, tem-se a glosa com finalidade cautelar, no segundo, definitiva.

Licitação - É um procedimento administrativo isonômico, realizado pela Administração Pública para selecionar melhor proposta, dentro dos preceitos de qualidade, é aquela que for mais vantajosa, e menos onerosa, para a contratação de um serviço, mão de obra, alienação, locação ou aquisição de um produto, devendo ser feito de forma obrigatória para as contratações de bens ou serviços de terceiros. Quanto às hipóteses de dispensa e inexigibilidade da licitação, encontram-se previstas nos parágrafos 2º e 4º do art. 17 e art. 24 e 25 da Lei nº 8.666/93, art. 75, 74 e parágrafos 3º e 6º do art. 76, da Lei nº 14.133/2021.

Licitante - Trata-se de pessoa física ou jurídica, ou para os casos de consórcio de pessoas jurídicas, que manifesta a intenção de participar do processo licitatório, sendo-lhe equiparável, para os fins das leis acima referenciadas, o fornecedor ou o prestador de serviço que, em atendimento à solicitação da Administração, oferece proposta.

Empenho - Ato emanado de autoridade competente (Secretário Executivo) que cria para o Estado obrigação de pagamento pendente ou não de implemento de condição. Documento extraído a cada empenho (corresponde à sua materialização) que indica o nome do credor, a representação e a importância da despesa, e a dedução do saldo da dotação própria. É a comprovação do registro do empenho. Nota de Empenho pode substituir o termo de contrato, conforme previsto no art. 62, § 4.º da Lei nº 8.666/93 e art. 95 da Lei nº 14.133/2021.

Liquidação - Consiste no segundo estágio da despesa, efetuado também pela unidade contratante, em que se verifica o direito adquirido pelo credor que envolve todos os atos de verificação e conferência, desde a entrada do material ou da prestação do serviço, até o reconhecimento da despesa, baseado em títulos e documentos comprobatórios do respectivo crédito, inclusive a verificação da regularidade fiscal do fornecedor. A finalidade é a verificação de apurar o quê, quanto e a quem pagar, e terá como base o contrato, ajuste ou acordo respectivo, a nota de empenho, e os comprovantes de entrega do material ou da prestação efetiva do serviço.

Pagamento - É o último estágio da despesa pública. Ocorre com a entrega do numerário ao fornecedor/credor, e é efetuado após a regular liquidação da despesa, por meio de despacho exarado pela autoridade competente, determinando sua execução.

Oficialização da Demanda - É o documento que contém o detalhamento da necessidade da área requisitante de contratação, assinado por ela.

Ordenador de Despesas - Autoridade administrativa (Secretário, Secretário Adjunto e Secretário Executivo) detentora de competência para ordenar a execução de despesas orçamentárias como a emissão de notas de empenho e a autorização para liquidação de despesas.

Parecer Jurídico - É a manifestação da Procuradoria Geral do Estado, por meio da qual expressa opinião sobre o pedido do autor, com base no que a lei dispõe sobre aquele assunto. Objetiva trazer clareza sobre um determinado assunto ou processo, e pode expressar opinião favorável ou contrária à proposição à qual se refere. Seu escopo de ação é abrangente, e pode ter relação com a documentação do processo que antecede à contratação, alterações ou encerramentos contratuais

Planejamento da Contratação - É a fase que recebe como insumo uma necessidade de negócio e gera como saída um edital completo, incluindo-se o termo de referência (TR) ou projeto básico (PB) para a contratação. Aplica-se nas contratações diretas e adesões a atas de registro de preços, nos quais são precedidas de um planejamento adequado, formalizado no processo de contratação, incluindo a elaboração da matriz de riscos, incorporado no Termo de Referência ou no Projeto Básico, quando for o caso.

Reajuste - Forma de manutenção do equilíbrio econômico-financeiro de contrato consistente na aplicação do índice de correção monetária previsto no contrato, que deve retratar a variação efetiva do custo de produção, admitida a adoção de índices específicos ou setoriais (Lei 14.133/2021).

Recebimento Provisório - O recebimento provisório, consiste na certificação formal de que os serviços foram prestados ou de que os bens foram recebidos para posterior análise de conformidade e qualidade, baseadas nos critérios de aceitação definidos no instrumento convocatório. A emissão do Termo de Recebimento Provisório não acarreta, em princípio, a aceitação total do objeto para fins de liquidação e pagamento.

Recebimento Definitivo - O recebimento definitivo é a aceitação do bem ou serviço por parte da Administração, por estar em conformidade com as especificações descritas na Nota de Empenho ou Termo de Referência do processo de aquisição. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança da obra ou serviço, nem a responsabilidade ético-profissional pela

perfeita execução do contrato, nos limites estabelecidos pela lei ou pelo contrato, conforme art. 140 da Lei nº 14.133/2021.

Equilíbrio Econômico-Financeiro - É a igualdade formada, de um lado, pelas obrigações assumidas pelo contratante no momento do ajuste e, do outro lado, pela compensação econômica que lhe corresponderá. Os procedimentos e/ou instrumentos utilizados para a manutenção do equilíbrio econômico- financeiro dos contratos são o reajuste, repactuação e reequilíbrio econômico-financeiro.

Registro de Ocorrências - É um documento, podendo ser livro, arquivo eletrônico, caderno ou folhas, onde o fiscal do contrato anota todas as ocorrências relacionadas com a execução contratual.

Seleção do Fornecedor - É a fase que recebe como insumo o edital completo, e gera como saída o contrato assinado e tornado público, por meio da publicação do extrato do contrato.

Serviço Executado de Forma Contínua - São os serviços auxiliares, necessários para a Administração para o desempenho de suas atribuições, e que, se interrompidos, podem comprometer a continuidade das suas atividades finalísticas, e cuja contratação deva estender-se por mais de um exercício financeiro. Exemplos: limpeza e conservação, manutenção predial, vigilância etc.

Termo de Contrato - É instrumento de ajuste que a Administração celebra com pessoas físicas ou jurídicas, públicas ou privadas, para a consecução de fins públicos, segundo regime jurídico de direito público. É obrigatório nas contratações por tomada de preços, concorrência e toda contratação (dispensa e inexigibilidade) cujo valor seja acima do estabelecido para a tomada de preços (art. 62, Lei nº 8.666/93 e art. 95 da Lei nº 14.133/21). Exceção: aquisição de bens com entrega única que não demande obrigações futuras (ex: assistência técnica), (§4º, art. 62, Lei nº 8.666/93 e art. 95, inciso II da Lei nº 14.133/21).

Termo de Referência ou Projeto Básico - É instrumento elaborado a partir dos estudos técnicos e preliminares, obrigatório para toda contratação, que reúne os elementos necessários e suficientes e nível de precisão adequado para caracterizar o objeto da licitação. Contém minimamente a descrição técnica, detalhamento do objeto a ser contratado, justificativa (motivação) da contratação, as condições de fornecimento ou prestação do serviço (prazo e local de entrega, validade dos produtos, garantia dos serviços, forma de acondicionamento etc.), obrigação das partes envolvidas (contratada e contratante), sendo vedadas especificações excessivas, irrelevantes ou desnecessárias que limitem a competição ou direcionem a aquisição.

Vigência do Contrato - Consiste no período durante o qual o contrato administrativo se apresenta como obrigatório para as partes, sendo submetidas aos direitos e

obrigações dele decorrentes, com início na data de sua assinatura ou outra posterior devidamente determinada. Compreende a etapa de execução do objeto, e o seu recebimento.

Assessoria Jurídica - Examinar as hipóteses de exceção das regras de exigibilidade de licitação (dispensa ou inexigibilidade), a emissão de pareceres jurídicos pontuais acerca da licitação, examinar e aprovar as minutas de editais de licitação, bem como as dos contratos, acordos, convênios ou ajustes.

Coordenação Administrativa - Unidade administrativa da Secretaria de Estado da Saúde de Rondônia (SESAU/RO) que tem como competência, dentre outras, garantir a eficácia e a eficiência do gerenciamento administrativo, com atribuições de planejar, coordenar, orientar e executar as atividades de gestão de aquisições e contratações públicas, além de implementar ações que promovam a qualidade do gasto público no âmbito da SESAU/RO".

Unidade Demandante - Solicitar a demanda de contratação, justificar, fundamentadamente, a sua necessidade, indicar a finalidade e o interesse público a ser atendido, bem como descrever o contexto da demanda nas unidades organizacionais interessadas, incluindo os riscos possíveis decorrentes da não realização da contratação solicitada.

Setor de Contratos - Realiza a gestão dos contratos tanto da área administrativa quanto dos serviços de saúde. Coordena as atividades relacionadas à fiscalização técnica, administrativa, setorial e pelo público usuário, bem como os atos preparatórios para formalização dos procedimentos que envolvam a prorrogação, alteração, reequilíbrio, pagamento, eventual aplicação de sanções, extinção dos contratos, dentre outros;

Fiscal do Contrato - Ao fiscal de contrato, compete realizar acompanhamento do contrato, tendo como objeto, avaliar suas execução, seguindo os ritos previsto para contratação e, se for o caso, analisar/julgar se a quantidade qualidade, tempo, e o modo da prestação ou execução do objeto estão em consonância s com os indicadores estabelecidos no edital, para fins de pagamento, conforme o resultado pretendido pela administração;

Unidade Gestora - É a unidade, responsável por realizar os procedimentos relativos ao ordenamento das despesas, em todas as fases, tais como empenho, liquidação e ordem de pagamento, executados pelo Fundo Estadual de Saúde.

2. MACROPROCESSO

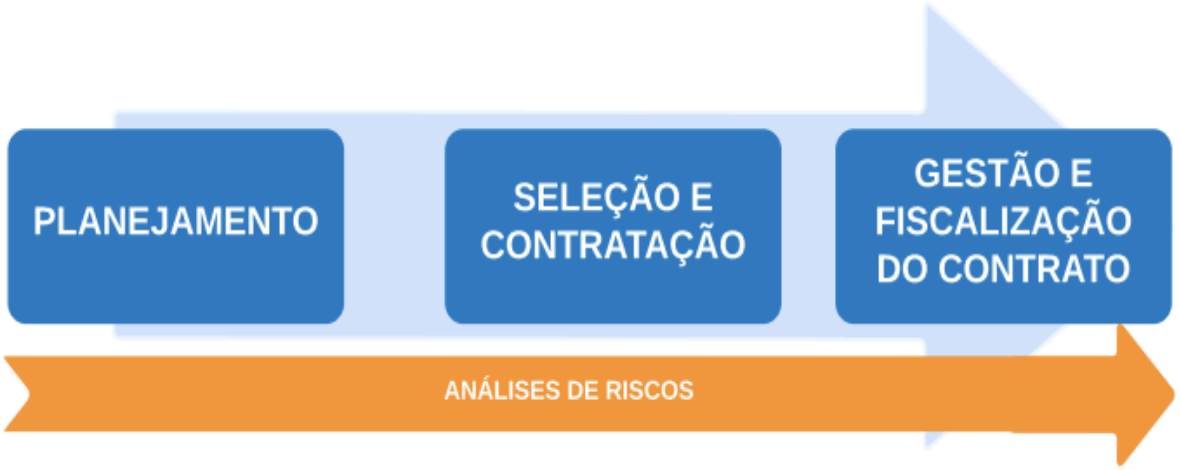


Figura 01 - Macroprocesso

O macroprocesso foi concebido no entendimento de três grandes fases, sendo elas: o planejamento, seleção, contratação ,gerenciamento e fiscalização do contrato.

No que concerne à gestão , esta por sua vez, permeia-se em todas as fases. Possibilitando aos atores envolvidos, uma melhor compreensão de cada fase, e a importância do gerenciamento de riscos, dentro do processo licitatório de forma contínua.

2.1. Planejamento

Fase em que se inicia a concepção do processo licitatório, conduzida pelo agente de contratação, os membros da comissão de contratação, equipe de apoio e da equipe de planejamento, tendo como principais atividades a elaboração dos seguintes estudos: mapa de riscos, projetos e anteprojetos, termos de referência, pesquisas de preço, Estudos de viabilidade, Estudo técnico preliminar, minutas de editais.

2.2. Seleção e Contratação

Fase na qual ocorre todo o processo relativo à seleção do fornecedor (ou aprovação nos casos de dispensa ou inexigibilidade de licitação) até a publicação do

contrato, e tem como principais atividades a Seleção do fornecedor, publicação do instrumento contratual e a Nomeação do Gestor e Fiscais do Contrato.

2.3. Gerenciamento e Fiscalização do Contrato

O Gerenciamento e Fiscalização do contrato têm um papel muito importante no que se refere a aplicação de controles, monitoramento, aferição dos resultados acordados, verificação das regularidades obrigatórias, sejam elas fiscais, previdenciárias, trabalhistas, sociais, dentre outras, observando a análise de riscos em todas as fases do macroprocesso de contratações públicas.

2.4. Gerenciamento de Riscos do Processo de Contratações Públicas

A implementação da gestão de riscos e controles internos dos processos licitatórios e dos respectivos contratos está prevista na nova Lei de Licitações (Lei nº 14.133/2021), no parágrafo único do art. 11, e art. 169, que tratam das diretrizes para a implementação de práticas contínuas e permanentes de gestão de riscos e controle preventivo, de responsabilidade da alta administração e integrantes das três linhas de defesa do órgão.

3.GESTÃO CONTRATUAL

Gestão de contrato é o gerenciamento das atividades relacionadas à execução, sob a forma: fiscalização técnica do contrato, administrativa, setorial e pelo público usuário. Bem como dos atos necessários à formalização do contrato, da prorrogação, repactuação, reequilíbrio econômico financeiro, da alteração, do acréscimo, da supressão, do pagamento, da aplicação de sanções, da extinção dos contratos, entre outros.

A gestão e fiscalização dos contratos, envolve servidores públicos, que representam a Secretaria de Estado da Saúde - SESAU, designado para a atribuição por meio de portaria emitida pela autoridade máxima (Secretário Executivo) do órgão ou entidade, sendo vedada a designação para a atribuição de servidor que integre ou esteja vinculado à unidade ou setor responsável pela elaboração de estimativa do valor da contratação ou pela realização do certame licitatório.

Quando a contratação tiver por escopo obra ou serviço de engenharia, a gestão e fiscalização do contrato será realizada por, no mínimo, um servidor público com formação nas áreas de engenharia ou arquitetura, designado por portaria da autoridade máxima do órgão, observada a vedação prevista no parágrafo anterior.

Para o exercício da função, o gestor e os fiscais deverão ser cientificados, expressamente, da indicação e respectivas atribuições antes da formalização do ato de designação, ao acompanhamento e ao pagamento do objeto contratual adimplido.

Quanto aos servidores públicos, designados para integrar a comissão de fiscalização do contrato administrativo, estes por sua vez, deverão possuir qualificação técnica adequada para desenvolvimento da atribuição, de acordo com os atos normativos editados pelos respectivos conselhos profissionais.

As eventuais necessidades de desenvolvimento de competências de agentes para fins de fiscalização e gestão contratual deverão ser evidenciadas no Estudo Técnico Preliminar, e deverão ser sanadas, se for o caso, previamente à celebração do contrato, conforme dispõe o inciso X do § 1º do art. 18 da Lei Federal n° 14.133, de 2021.

Quando da designação do gestor e do fiscal de contrato, a autoridade máxima do órgão deverá manter de maneira equânime o número de contratos que serão submetidos à fiscalização de um mesmo servidor.

3.1. Gestor do Contrato

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

Cabendo ao gestor do contrato, ser responsável por coordenar, comandar e acompanhar a execução do contrato. Devendo agir de forma proativa e preventiva, observar o cumprimento das regras previstas no instrumento contratual e buscar os resultados esperados pela Administração, baseando-se em indicadores objetivamente definidos, sempre que aplicável

É vedado à autoridade máxima do órgão ou entidade o exercício da função de gestor de contrato, salvo nos casos de desligamento extemporâneo e definitivo do gestor e de seus substitutos e não poderá perdurar por mais de 60 (sessenta) dias, sob pena de responsabilização funcional.

Considerando que o gestor do contrato nem sempre participa das fases de Planejamento e Licitação, é importante que leia atentamente o Memorial Descritivo, o Projeto Executivo (quando for o caso) e o contrato, prestando especial atenção às cláusulas que descrevem as especificações do objeto, as condições de execução, os procedimentos de fiscalização e as penalidades aplicáveis à Contratada. Cabe ao Gestor, principalmente, as seguintes atribuições:

- instruir o processo com os documentos necessários às alterações contratuais, inclusive controlando os limites aplicáveis, e encaminhá-lo à autoridade superior para decisão;
- encaminhar o requerimento de prorrogação do prazo de execução do objeto ou da vigência do contrato à autoridade competente, instruindo o processo com manifestação conclusiva e dados que comprovem o impedimento do cumprimento do prazo pela contratada;
- controlar o prazo de vigência do contrato e de execução do objeto, assim como de suas etapas e demais prazos contratuais, recomendando, com antecedência razoável, à autoridade competente, quando for o caso, a deflagração de novo procedimento licitatório ou a prorrogação do prazo, instruindo o processo com a documentação necessária;
- prover o fiscal do contrato das informações e dos meios necessários ao exercício das atividades de fiscalização e supervisionar as atividades relacionadas ao adimplemento do objeto contratado;
- comunicar à autoridade competente as irregularidades cometidas pela contratada, sugerindo, quando for o caso, a imposição de sanções contratuais e/ou administrativas, conforme previsão contida no edital e/ou instrumento contratual ou na legislação de regência;
- adotar as medidas preparatórias para a aplicação de sanções e de rescisão contratual, conforme previsão contida no edital e/ou instrumento contratual ou na legislação de regência, cabendo à autoridade competente a deflagração do respectivo procedimento, a notificação da contratada para a apresentação de defesa e a decisão final;

- promover o controle das garantias contratuais, inclusive no que se refere à juntada de comprovante de recolhimento e adequação da sua vigência e do seu valor;
- propor, formalmente, à autoridade competente, a liberação da garantia contratual em favor da contratada nos prazos regulamentares;
- receber as notas fiscais atestadas pelo(s) fiscal(is) do contrato e encaminhá-las para o setor responsável pelo pagamento, após conferência dos respectivos documentos;
- manter controle atualizado dos pagamentos efetuados, em ordem cronológica;
- documentar nos autos todos os fatos dignos de interesse administrativo;
- registrar as informações necessárias nos sistemas informatizados utilizados pelo Poder Executivo do Estado de Rondônia, inclusive inserindo os dados referentes aos contratos administrativos no Portal Nacional de Contratações Públicas- PNCP, e mantê- los atualizados;
- diligenciar para o acompanhamento de situações que possam impactar nos preços contratados, como a criação, alteração ou extinção de tributos ou encargos legais ou a superveniência de disposições legais que repercutam no contrato, na forma do art. 134 da Lei Federal n° 14.133, de 2021;
- elaborar o relatório final de que trata a alínea “d” do inciso VI do § 3º do art. 174 da Lei Federal n° 14.133, de 2021, com as informações obtidas durante a execução do contrato;
- tomar providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei Federal n° 14.133, de 2021, ou pelo agente ou pelo setor competente para tal, conforme o caso;
- realizar o recebimento definitivo do objeto do contrato mediante termo detalhado que comprove o atendimento das exigências contratuais;
- receber os pedidos de reajuste, repactuação e revisão de contratos, devendo emitir parecer quanto ao cabimento.
- convocar e coordenar a reunião inicial, registrada em ata que posteriormente é incorporada ao Processo de Acompanhamento e Fiscalização do Contrato. A reunião contará preferencialmente com a equipe técnica responsável pela elaboração do Termo de Referência, além dos Fiscais e do Preposto;

- emitir ordem inicial de serviço e autorizar implantação do contrato no sistema de controle de contratos, ou planilha de controle;

Quando a Contratada manifestar interesse na alteração de alguma cláusula contratual, como exemplo a prorrogação do prazo, o Gestor deve solicitar apresentação de justificativas e comprovações necessárias à Fiscalização, que deve analisar a legalidade e conveniência da alteração contratual, observando o disposto no art. 124 da Lei de Licitações (14.133/2021). Em havendo grande complexidade técnica do objeto, o Gestor deverá solicitar pareceres ou relatórios elaborados por servidores da área ou por profissionais contratados para auxiliá-lo.

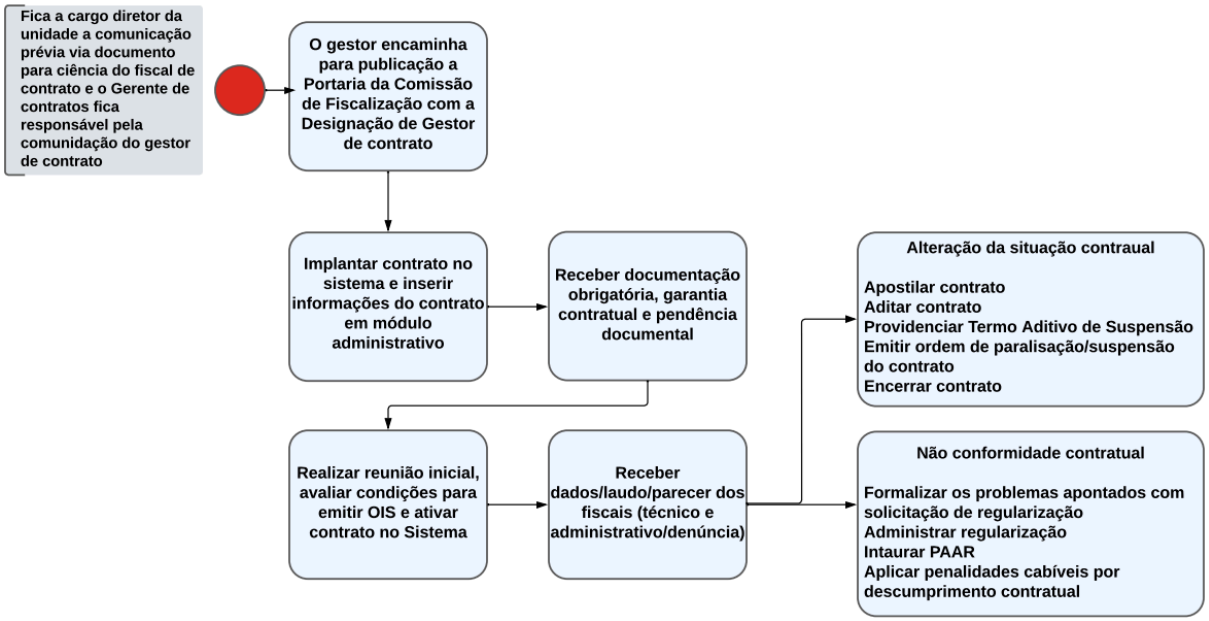


Figura 02 - Responsabilidades do Gestor do Contrato, disponível também em PDF, no processo SEI nº 0036.041279/2023-79 (ID: 0047309666).

O Gestor deverá solicitar que as empresas contratadas apresentem periodicamente, no mínimo uma vez ao ano, Termo de Quitação Geral Anual, nos termos do Art. 507-B da CLT.

As decisões e providências que ultrapassarem a competência/atribuição do gestor deverão ser encaminhadas aos seus superiores (Gerente de contratos) em tempo hábil, para a adoção das medidas devidas.

3.2. Das Garantias

As garantias visam dar margem razoável de segurança ao fiel cumprimento das obrigações assumidas por parte da contratada, conforme prevê o Art. 96, da Lei

14.133/93, portanto, caberá ao contratado optar por uma das seguintes modalidades de garantia:

- caução em dinheiro ou em títulos da dívida pública emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados por seus valores econômicos, conforme definido pelo Ministério da Economia;
- seguro-garantia;
- fiança bancária emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil;
- título de capitalização custeado por pagamento único, com resgate pelo valor total. (Incluído pela Lei nº 14.770, de 2023).

No que concerne à gestão de seguros e garantias do contrato, esta por sua vez, é de atribuição do Gestor de Contratos, incluindo a sua contratação e reclamação. E diante da contratação do seguro, deve-se analisar as cláusulas da apólice e compará-las com os requisitos definidos no edital. Caso as cláusulas não estejam compatíveis, deve-se notificar a contratada para retificar a apólice junto à seguradora.

Além disso, é responsável por notificar a contratada e a seguradora de qualquer expectativa de sinistro e reclamar o seguro, caso tal expectativa se concretize (§8º, Art. 5º, da IN 06/2019).

A Unidade Gestora deve verificar as situações abaixo relacionadas antes de notificar a seguradora da expectativa de sinistro ou reclamar o seguro:

- O envio à contratada da notificação solicitando o cumprimento da obrigação num prazo determinado, com cópia à seguradora, comunicando através desta a expectativa de sinistro, com documentação dos itens não cumpridos do contrato;
- O aviso à seguradora de qualquer mudança pela contratada no escopo e/ou prazo de execução do contrato (termos aditivos de qualquer natureza);
- A apresentação, pela contratada, de endosso da apólice referente aos termos aditivos;
- O aviso à seguradora da abertura de Processo Administrativo de Apuração de Responsabilidade – PAAR;

- A comprovação de inadimplência da contratada que possa gerar prejuízo a SESAU;
- O envio de documentos necessários à realização de expectativa/reclamação do sinistro de acordo com o especificado na apólice e;
- Verificar se a garantia está dentro do prazo prescricional (1 ano a partir da ciência do fato gerador da pretensão, art. 206 do Código Civil).

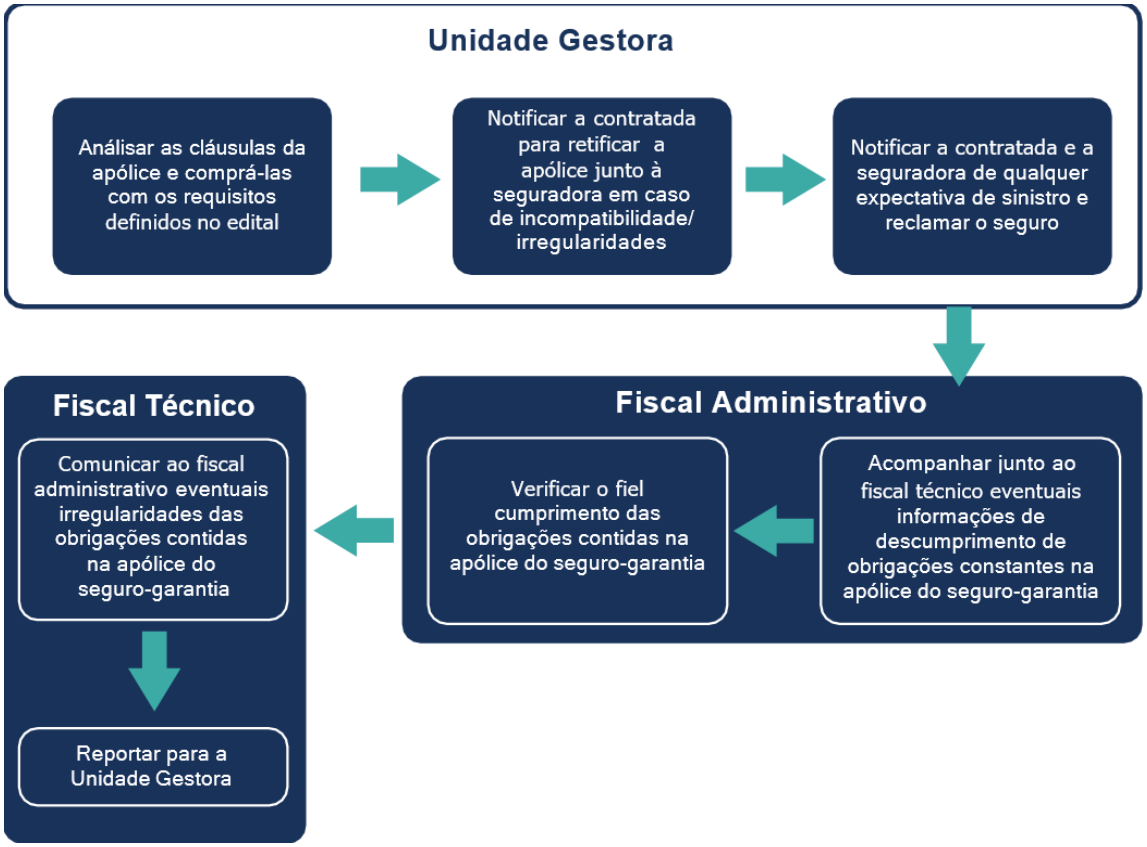


Figura 03 - Responsabilidades dos agentes em relação ao Seguro-Garantia

3.3. Alterações nos Contratos

As alterações contratuais, conforme os ditames no art. 124 da Lei n° 14.133/21, devem ser realizadas durante o período de vigência do contrato, conforme o art. 106 da Lei n° 14.133/21, devendo ser formalizadas por meio da celebração do Termo Aditivo do contrato, nos casos de prorrogação de prazo, acréscimos e supressões.

Quanto a outras modificações que possam ser caracterizadas como alterações do contrato, também são admitidas em lei, tais como: alteração do nome

ou denominação empresarial da contratada; alteração do endereço da contratada; retificação de cláusula contratual e retificação de dados (CNPJ) da empresa contratada.

Oportuno esclarecer que nem toda alteração contratual deverá ocorrer mediante a formulação de Termo Aditivo, podendo ser formalizados por Apostila. São os casos enumerados pela a Lei nº 14.133/21 em seu art. 136:

- variação do valor contratual para fazer face ao reajuste ou à repactuação de preços previstos no próprio contrato;
- atualizações, compensações ou penalizações financeiras decorrentes das condições de pagamento previstas no contrato;
- Alterações na razão ou na denominação social do contrato ou do contratado;
- empenho de dotações orçamentárias.

Em suma, o Termo de Apostilamento pode ser definido como um registro, que pode ser realizado no próprio contrato ou em outro documento oficial, enquanto o Termo Aditivo é um instrumento realizado separadamente que segue toda formalidade inerente ao contrato, devendo, inclusive, obediência à obrigatoriedade de publicação na Imprensa Oficial. Portanto, cabe ao Gestor e ao Fiscal do contrato observarem quando caberá a formulação desses instrumentos durante a vigência contratual.

Todas as tratativas realizadas junto à Contratada durante o processo de aditamento contratual deverão ser formalizadas e registradas.

No caso de contratação integrada, o Art. 9º, § 4º da Lei nº 12.462 de agosto de 2011, delibera que seja vedada a celebração de termos aditivos, exceto nos seguintes casos:

- Para recomposição do equilíbrio econômico-financeiro decorrente de caso fortuito ou força maior;
- Por necessidade de alteração do projeto ou das especificações para melhor adequação técnica aos objetivos da contratação, a pedido da administração pública, desde que não decorrentes de erros ou omissões por parte do contratado, observados os limites previstos no § 1º do art. 65 da Lei no 8.666/93.

No caso de contratação por meio do Sistema de Registro de Preços no RDC não poderão sofrer acréscimo de quantitativos, conforme Decreto nº 7.581/11.

3.4. Paralisação e Reinício para Contratos de Obras

No caso de paralisação do contrato, caberá ao Gestor e Fiscais observar que a suspensão do prazo de execução contratual terá como marco inicial a data de expedição da ordem de paralisação da execução do contrato.

As paralisações podem ser parciais ou totais, sendo que a total suspende as medições, devendo ser alterada a situação cadastral no sistema de controle de contratos; enquanto a paralisação parcial pode ocorrer em trechos específicos de uma obra, por exemplo, não havendo paralisação do prazo de execução, nem necessitando de alteração no sistema de controle de contratos.

ATENÇÃO

Prazo de vigência é diferente de prazo de execução.

Prazo de vigência é o prazo do contrato, enquanto o prazo de execução é o tempo fixado para a execução do objeto.

Prorrogação do prazo de vigência é ato de competência exclusiva do gestor.

Após expedida a Ordem de paralisação, ela já se encontra apta a produzir seus efeitos próprios, dentre os quais o de obrigar o contratado a paralisar a obra ou o serviço. Mesmo que o contrato esteja paralisado, a vigência contratual continua a mesma. O que sofre a remissão de data é o período de execução. O registro da efetiva paralisação da obra ou do serviço será feito por apostilamento.

Quando identificada a necessidade de paralisação do contrato, os fiscais devem comunicar ao Gestor, apresentando as justificativas pertinentes em até 48 horas a partir da emissão da Ordem de Paralisação.

A suspensão deve-se dar por ordem escrita da Administração, que deverá ser fundamentada e a decisão formalmente comunicada à contratada. Recomenda-se que a Contratada seja consultada e se manifeste dando anuência para suspensão contratual, observando o disposto no art. 78 da Lei nº 8.666/93.

3.5. Reajuste

O reajuste tem por finalidade a recomposição do equilíbrio financeiro do contrato em razão da variação normal do custo de produção decorrente da inflação. Para tanto, pode-se utilizar índices específicos ou setoriais, desde que oficiais. Os

dispositivos legais que tratam do reajuste contratual são: art. 40, inciso XI, art. 55, inciso III, ambos da Lei nº 8.666/93, e art. 124 a 136 da Lei 14.133/2021.

Este procedimento é realizado em periodicidade igual ou superior a um ano, contado a partir da data limite para apresentação da proposta ou do orçamento a que essa se referir, segundo a Lei nº 10.192/01.

O critério de reajuste é item obrigatório na composição do edital da licitação, bem como do contrato administrativo, devendo conter ainda a data-base e a periodicidade do reajustamento de preços (vide art. 1º e 2º da Lei 10.192/01).

Este instrumento é regulado por vários dispositivos legais, pela Lei nº 10.192/01, que dispõe em seu art. 3º temos que:

> "Os contratos em que seja parte órgão ou entidade da Administração Pública direta (...) serão reajustados ou corrigidos monetariamente de acordo com as disposições desta Lei, e, no que com ela não conflitarem, da Lei no 8.666/93. § 1º A periodicidade anual nos contratos de que trata o caput deste art. será contada a partir da data limite para apresentação da proposta ou do orçamento a que essa se referir".

Para realizar o cálculo do reajuste, a Fiscalização deve observar os índices descritos na contratação, e caso tenham sido extintos, levar à diretoria setorial responsável pela deliberação.

3.6. Revisão - Reequilíbrio Econômico-Financeiro

O Reequilíbrio Econômico-Financeiro desvincula-se de quaisquer índices de variação inflacionária, pois tem por objetivo a correção das distorções geradas por ocorrências extraordinárias e imprevisíveis ou previsíveis.

A revisão contratual deve ser fundamentada, ou seja, deve haver a motivação do ato por pelo menos uma das partes contratantes. A motivação deverá demonstrar de forma clara a incidência de onerosidade excessiva ocasionada por acontecimentos supervenientes, sendo indispensável que tais fatos sejam exaustivamente comprovados no processo administrativo regular.

Considerando tratar-se de situação de caráter excepcional, em que o grande desequilíbrio e a imprevisibilidade estão relacionados à teoria da imprevisão, esta revisão poderá ocorrer antes do período mínimo de um ano da vigência contratual, desde que verificadas as exigências enumeradas na alínea “d” do inc. II do art. 124, da Lei nº 14.133, de 1º de abril de 2021.

3.7. Repactuação

É dever do contratado provocar a Administração para exercer seu direito à repactuação contratual. Este pedido deve ocorrer a partir da data da homologação da convenção ou acordo coletivo, que venha fixar o novo salário normativo da categoria profissional abrangida pelo contrato administrativo, devendo ser repactuado até a data da prorrogação contratual subsequente.

Caso o contratado não manifeste seu pedido de forma tempestiva, e a prorrogação do contrato ocorrer sem sua respectiva repactuação, haverá a preclusão do seu direito a repactuar, este direito também preclui se houver expiração do prazo de vigência do contrato.

A repactuação tem por finalidade promover o reajuste dos contratos de serviços de prestação continuada.

3.8. Acréscimo/Supressão Contratual

A Administração poderá alterar o contrato realizando acréscimos ou supressões, respeitados os limites dispostos na legislação, e apresentados na tabela a seguir:

		Reforma de edifício ou equipamento		Demais casos	
	Tipo de Alteração	**Unilateral**	**Consensual**	**Unilateral**	**Consensual**
Acréscimo	qualitativa	50%	*	25%	*
	quantitativa	50%	50%	25%	25%

Supressões	qualitativa	50%	não há limite	25%	não há limite
	quantitativa	50%	não há limite	25%	não há limite

Tabela - Limites para acréscimo e supressão

4. FISCALIZAÇÃO CONTRATUAL

A fiscalização contratual é o conjunto de atividades exercidas pela Administração para controle, tendo o papel de acompanhar, avaliar e conferir a execução do objeto nos moldes contratados nos aspectos técnicos, administrativo e operacional para efeito de pagamento. Em que configura-se como o monitoramento do cumprimento das obrigações estabelecidas em contrato, com o fim de assegurar a execução do objeto contratado e o respeito às normas vigentes.

Portanto, é de dever realizar o registrar sempre uma ocorrência no caso de detecção de algum incidente, e por auxiliar o gestor do contrato, aplicando os controles e revisando os riscos pertinentes à execução.

As funções da fiscalização do contrato compreendem diversos procedimentos de verificação de natureza técnica e administrativa, estabelecidos neste Manual e na etapa do Planejamento da Fiscalização do contrato, observados os normativos legais, a natureza e complexidade do objeto contratado, as boas práticas e a gestão de risco.

As atividades de fiscalização da execução contratual devem ser realizadas de forma preventiva, rotineira e sistemática, preferencialmente por servidor efetivo ou empregado público dos quadros permanentes da Administração Pública designado pela autoridade signatária do contrato.

A fiscalização deverá ser realizada in loco, com o propósito de avaliar a execução do objeto contratado e aferir a qualidade, quantidade, tempo e modo da prestação do serviço/fornecimento.

Conforme o art. 117 da Lei Federal nº 14.133/2021, é permitida a contratação de terceiros para assistir e subsidiar os fiscais do contrato com informações pertinentes a tais atribuições.

4.1. Fiscalização Técnica

A fiscalização técnica consiste no acompanhamento e avaliação da execução do objeto nos moldes contratados, visando aferir a qualidade, quantidade, tempo e

modo de execução, bem como assegurar a qualidade da prestação dos serviços, e se estão compatíveis com os indicadores de níveis mínimos de desempenho estipulados no ato convocatório.

A função de fiscal técnico de contrato deve ser atribuída a servidor com experiência e conhecimento na área relativa ao objeto contratado, designado para auxiliar o gestor do contrato quanto à fiscalização dos aspectos técnicos do contrato.

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

a) participar das reuniões inicial, de trabalho e de conclusão da execução contratual;

b) anotar em registro próprio todas as ocorrências relacionadas com a execução e determinará o que for necessário à regularização de falhas ou defeitos observados.

c) conhecer o termo de contrato e todos os seus Anexos, especialmente o Projeto Básico ou o Termo de Referência, certificando-se de que a contratada está cumprindo todas as obrigações assumidas;

d) verificar se, na entrega de material, na execução de obra ou na prestação de serviço, a especificação, o valor unitário ou total, a quantidade e os prazos de entrega estão de acordo com o estabelecido no instrumento contratual;

d) Verificar e confrontar os preços e quantidades constantes da nota fiscal com os estabelecidos no contrato;

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

f) anotar, em processo específico, quando autuado para esse fim, todas as ocorrências relativas à execução do contrato, com a indicação do que for necessário à regularização das faltas ou defeitos observados. A fim de produzir um histórico de gerenciamento do contrato, todas as ocorrências relacionadas à execução do contrato.

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

h)monitorar constantemente o nível de qualidade dos serviços para evitar eventuais incorreções, devendo intervir para requerer à contratada a correção das faltas, falhas e irregularidades constatadas;

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

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

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

m) registrar e informar ao gestor as atividades desempenhadas e todas as pendências constatadas na execução do contrato, comunicando ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual;

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

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

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

q) verificar se estão sendo atendidas as especificações contidas nos planos, projetos, planilhas, memoriais descritivos, especificações técnicas, projeto básico, termo de referência, assim como os prazos de execução e de conclusão, devendo solicitar ao preposto da contratada a correção de imperfeições detectadas;

r) verificar a execução do objeto contratual, proceder a sua medição e recebê-lo, pela formalização da atestação;

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

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

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

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

x) confrontar os preços e quantidades constantes da nota fiscal com os estabelecidos no contrato;

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

4.1.1. Fiscalização Técnica de Obras e Serviços de Engenharia

No caso de obras e serviços de engenharia, a fiscalização será exercida por um servidor com formação nas áreas de engenharia ou arquitetura, da Secretaria de Estado de Obras e Serviços Públicos - SEOSP podendo ser mais de um engenheiro

a critério do gestor, crumpre ainda aos fiscais de obras e prestação de serviços de engenharia:

1) fazer constar todas as ocorrências no Diário de Obras, com vistas a compor o processo documental, de modo a contribuir para dirimir dúvidas e embasar informações acerca de eventuais reivindicações futuras, tomando as providências que estejam sob sua alçada e dando ciência ao gestor quando excederem as suas competências;
2) zelar pela fiel execução da obra, sobretudo no que concerne à qualidade dos materiais utilizados e dos serviços prestados, bem como quanto aos aspectos ambientais;
3) atestar o funcionamento de equipamentos e registrar a conformidade em documento
4) acompanhar e analisar os testes, ensaios, exames e provas necessários ao controle de qualidade dos materiais, serviços e equipamentos a serem aplicados na execução do objeto contratado, quando houver;
5) informar ao gestor ocorrências que possam gerar dificuldades à conclusão da obra ou em relação a terceiros; e
6) proceder, conforme cronograma físico-financeiro, às medições dos serviços executados, conforme disposto em contrato.

ATENÇÃO:

É admitida a contratação de terceiros para assistir e subsidiar a fiscalização pelos agentes estaduais, quando as peculiaridades técnicas do objeto assim justificarem, sendo vedado, em qualquer hipótese, terceiro exercer função própria e exclusiva do fiscal de contrato, nos termos do parágrafo 4º, inc. I, art. 117, da Lei Federal n° 14.133, de 2021

A fiscalização não exclui nem reduz a responsabilidade da contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com os arts. 119 e 120 da Lei Federal n° 14.133, de 2021.

4.2. Fiscalização Administrativa

Consiste no acompanhamento dos aspectos administrativos contratuais É o acompanhamento quanto as obrigações previdenciárias, fiscais e trabalhistas, sendo necessária nos contratos de prestação de serviços de regime de dedicação exclusiva de mão de obra.

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

a) prestar apoio técnico e operacional ao gestor do contrato, com a realização das tarefas relacionadas ao controle dos prazos relacionados ao contrato e à formalização de apostilamentos e de termos aditivos, ao acompanhamento do empenho e do pagamento e ao acompanhamento de garantias e glosas;
b) certificar-se de que a contratada mantém, durante toda execução do contrato, as condições de habilitação e qualificação exigidas na licitação e/ou na contratação, solicitando os documentos necessários a esta constatação, com especial atenção para a regularidade trabalhista e previdenciária nos casos de obras e serviços com dedicação exclusiva (ou predominante) de mão de obra;
c) examinar a regularidade no recolhimento das contribuições fiscais, trabalhistas e previdenciárias;
d) atuar tempestivamente na solução de eventuais problemas relacionados ao descumprimento das obrigações contratuais e reportar ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência;
e) participar da atualização do relatório de riscos durante a fase de gestão do contrato, em conjunto com o fiscal técnico e com o setorial, sob coordenação do gestor do contrato;
f) auxiliar o gestor do contrato com as informações necessárias, na elaboração do documento comprobatório da avaliação realizada na fiscalização do cumprimento de obrigações assumidas pelo contratado;
g) realizar o recebimento provisório do objeto do contrato, mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo;
h) receber e conferir a nota fiscal emitida pela contratada, atestando a efetiva realização do objeto contratado, na quantidade e qualidade contratada, para fins de pagamento das faturas correspondentes;
i) nos casos de requerimento de revisão contratual, exigir a comprovação dos custos suportados pelo contratado através de notas fiscais, realizando análise crítica da compatibilidade dos preços com a realidade de mercado constatada junto a outras fontes;
j) receber todos os documentos necessários, contratualmente estabelecidos, para a liquidação da despesa e encaminhá-los, juntamente com a nota fiscal;
k) para o gestor do contrato que, após conferência, remeterá a documentação ao setor responsável pelo pagamento, em tempo hábil, de modo que o pagamento seja efetuado no prazo adequado;
l) verificar o cumprimento das normas trabalhistas por parte da contratada, inclusive no que se refere à utilização pelos empregados da empresa dos equipamentos de proteção individual exigidos pela legislação pertinente, a fim de evitar acidentes com agentes administrativos, terceiros e empregados da contratada, e, na hipótese de descumprimento, comunicar ao gestor para impulsionar o procedimento tendente à notificação da contratada para o cumprimento das normas trabalhistas e instauração de processo administrativo para aplicação de sanção administrativa;

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

4.2.1. Critérios para Elaboração dos Relatórios Administrativos

Quanto aos relatórios elaborados pela fiscalização do contrato administrativo deverão abordar os seguintes pontos:

a) cumprimento do cronograma e das diretrizes fixadas no termo de referência ou no projeto básico;
b) observância do cronograma físico-financeiro da obra ou do serviço, nos casos de contratação com escopo definido;
c) atingimento das metas e dos índices de qualidade fixados no termo de referência, projeto básico e contrato;
d) atendimento dos critérios de habilitação durante o curso da execução por meio da apresentação de certidões atualizadas;
e) cumprimento das obrigações trabalhistas, inclusive, FGTS, no caso de contratos que tenham por objeto a prestação de serviços contínuos com dedicação exclusiva (ou predominante) de mão de obra;
f) avaliação do desempenho contratual do fornecedor.

ATENÇÃO

A fiscalização dos contratos deverá ser realizada por meio de vistorias, observando-se a periodicidade e as diretrizes fixadas no contrato, devendo ser realizada, no mínimo, uma vistoria a cada mês de execução.

Todos os atos emitidos pela fiscalização do contrato deverão ser anexados ao processo administrativo respectivo.

4.2.2. Critérios para Elaboração dos Relatórios com Dedicação Exclusiva

No caso de contratos que tenham por objeto a prestação de serviços contínuos com dedicação exclusiva (ou predominante) de mão de obra, a comprovação do cumprimento das obrigações trabalhistas, além da apresentação de certidão atualizada de regularidade trabalhista, será realizada por meio da apresentação dos seguintes documentos:

a)cópia da folha de pagamento analítica do mês da prestação dos serviços, em que conste como tomador o órgão ou entidade contratante;

b)cópia dos contracheques dos empregados, relativos ao mês da prestação dos serviços;

c)recibos de pagamento ou guias de depósitos bancários da remuneração dos empregados vinculados ao contrato no mês da prestação do serviço;

d) guia de recolhimento da Previdência Social - GPS, junto ao Instituto Nacional do Seguro Social - INSS, da contratada e Informações à Previdência Social, GFIP - SEFIP/GRF, onde conste a Relação de Trabalhadores vinculados ao contrato no mês da prestação dos serviços;

e) guias de recolhimento de FGTS dos empregados vinculados ao contrato, relativas ao mês da prestação dos serviços;

f) registros de horário de trabalho (cartões-ponto ou folha-ponto), relativos ao mês da prestação dos serviços;

g)comprovantes de entrega de benefícios suplementares (vale-transporte, vale alimentação, entre outros), a que estiver obrigada por força de lei ou de convenção ou acordo coletivo de trabalho, relativos ao mês da prestação dos serviços e de todos os empregados;

h) avisos e recibos de férias, recibos de 13º salário, Relação Anual de Informações Sociais - RAIS, ficha de registro de empregado, autorização para descontos salariais; e

i) termos de rescisão dos contratos de trabalho dos empregados, devidamente homologados pelo sindicato da categoria quando exigível; guias de recolhimento da contribuição previdenciária e do FGTS, referentes às rescisões contratuais, extratos dos depósitos efetuados nas contas vinculadas individuais do FGTS de cada empregado(a) dispensado(a); e exames médicos demissionais dos empregados dispensados.

4.2.3. Descumprimento das Obrigações Trabalhistas

Caso inobservado ou descontinuado o cumprimento das obrigações trabalhistas, a fiscalização do contrato deverá aplicar sanção de advertência ao contratado fixando prazo máximo para restabelecimento da regularidade.

Persistindo a irregularidade, pagamentos pendentes deverão ser retidos até a efetiva regularização, observadas as seguintes diretrizes:

1. a retenção integral do pagamento em aberto é temporária, devendo ser adstrita, assim que possível, ao valor devido pelo contratado acrescida das multas trabalhistas e contratuais;
2. caso o contratado não providencie a regularização com a apresentação dos comprovantes e certidões respectivas até o último dia da competência seguinte à data de entrada da solicitação relativa ao pagamento pendente, a Administração contratante realizará o depósito em conta vinculada aberta para tal finalidade específica, em nome do Estado, devendo centralizar todos os depósitos realizados independentemente do órgão ou entidade responsável pela contratação, devendo ser resguardada a impenhorabilidade dos recursos.

3. Caso o órgão ou entidade responsável entenda conveniente e razoável, a providência poderá ser substituída pelo pagamento direto aos empregados do contratado.
4. A realização de depósitos na conta vinculada deverá ser comunicada ao Ministério Público do Trabalho e à entidade sindical representante dos empregados.
5. Os valores depositados somente serão liberados após a comprovação da regularidade pelo contratado ou em caso de determinação judicial.
6. na fiscalização do cumprimento das obrigações trabalhistas e sociais nas contratações continuadas com dedicação exclusiva ou predominante, a fiscalização do contrato deverá realizar entrevistas, a partir de seleção por amostragem, com os trabalhadores da contratada para verificar as anotações contidas em CTPS, devendo ser observadas, entre outras questões, a data de início do contrato de trabalho, função exercida, a remuneração, gozo de férias, horas extras, eventuais alterações dos contratos de trabalho e, se necessário, fiscalizar no local de trabalho do empregado.
7. A constatação de irregularidade quanto ao pagamento de contribuições previdenciárias no caso de contratos administrativos que tenham por objeto a realização de obras ensejará a retenção de eventuais pagamentos pendentes até que seja sanada a irregularidade;

Acompanhamento das obrigações trabalhistas e sociais em contratos de terceirização de mão de obra. No primeiro mês da prestação dos serviços, Fiscal Administrativo deverá solicitar em meio eletrônico à contratada a relação dos empregados terceirizados de todo contrato administrativo, com nome completo, número de CPF, função exercida, salário, adicionais, gratificações, benefícios recebidos (quantidade e valor: vale-transporte, auxílio-alimentação, dentre outros) e horário do posto de trabalho.

Deverá ser realizada fiscalização periódica e constante da execução dos contratos, principalmente no que se refere ao cumprimento das obrigações previdenciárias e trabalhistas, em especial: pagamento do FGTS, da GPS, dos salários até o 5º dia útil do mês seguinte; notificações à empresa terceirizada por descumprimento de cláusulas contratuais; sanções aplicadas à empresa que descumpra suas obrigações contratuais, entre outros.

As ocorrências observadas na execução contratual deverão ser registradas durante toda a vigência da prestação dos serviços.

4.3. Fiscalização Setorial

A fiscalização setorial tem por objetivo ser um braço do órgão em todas as suas unidades, especialmente as desconcentradas. Pode abranger tanto os aspectos técnicos quanto os administrativos, garantindo uma maior eficiência nos contratos em que há descentralização de sua execução em diferentes unidades.

4.4. Fiscalização pelo Público Usuário

A fiscalização pelo público usuário realizada por quem de fato faz uso ou é beneficiário dos serviços, a exemplo dos servidores, de modo que é recomendável que a sua efetivação se realize por intermédio de avaliações qualitativas relativas aos serviços e materiais disponibilizados pela contratada, bem como pela manutenção de canais de comunicação para recebimento de reclamações.

Nota: O recebimento provisório ficará a cargo do fiscal técnico, administrativo ou setorial e o recebimento definitivo, a cargo do gestor do contrato, conforme art. 20. inciso XVI, e art. 23. inciso X, do Decreto Estadual n. 28.874/2024, RO.

4.5. Das Fases do Processo de Fiscalização

O macroprocesso de fiscalização é contemplado por quatro processos interligados, e de muita importância para se assegurar as melhores práticas e aplicações de controles, a fim de mitigar os riscos, minimizando as possíveis consequências durante a fase de execução contratual.

Dentro dos processos apresentados na Figura 04, a seguir, são apresentados os subprocessos, iniciando pela “Designação da Comissão de Fiscalização”, por ato do titular da unidade administrativa (ou o representante da Administração pública responsável pela contratação), que posteriormente irá conduzir o segundo subprocesso, de “Inicialização da Fiscalização”. Em seguida, se torna possível o efetivo monitoramento do contrato, de forma periódica, conduzida pelo fiscal técnico de forma contínua, dentro de uma periodicidade previamente determinada no planejamento denominada “Fiscalização Técnica Periódica”. Finalmente, tem-se a “Fiscalização Administrativa”, com foco nos documentos administrativos relativos às obrigações trabalhistas, sociais, tributárias e contratuais, para fins de pagamento ao fornecedor e revisão da análise de riscos.

A Administração deve manter permanentemente, de forma eletrônica ou física, registro apropriado para anotações relacionadas com a execução e fiscalização do contrato.

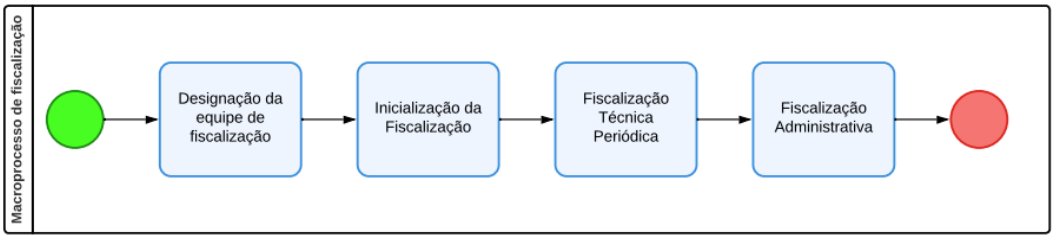


Figura 04 - Macroprocesso da fiscalização

4.5.1. Designação da Comissão de Fiscalização

A designação da Comissão de Fiscalização ocorrerá por nomeação de servidores, no caso do fiscal pelos diretores/coordenadores das unidades administrativas, e o gestor será designado pelo gerente de contratos, conforme Figura 05, mediante Portaria, para acompanhar e fiscalizar a execução dos contratos administrativos no âmbito de sua abrangência, de forma diligente, zelosa e minuciosa.

A Portaria será expedida até a data da publicação do contrato e divulgada oficialmente.

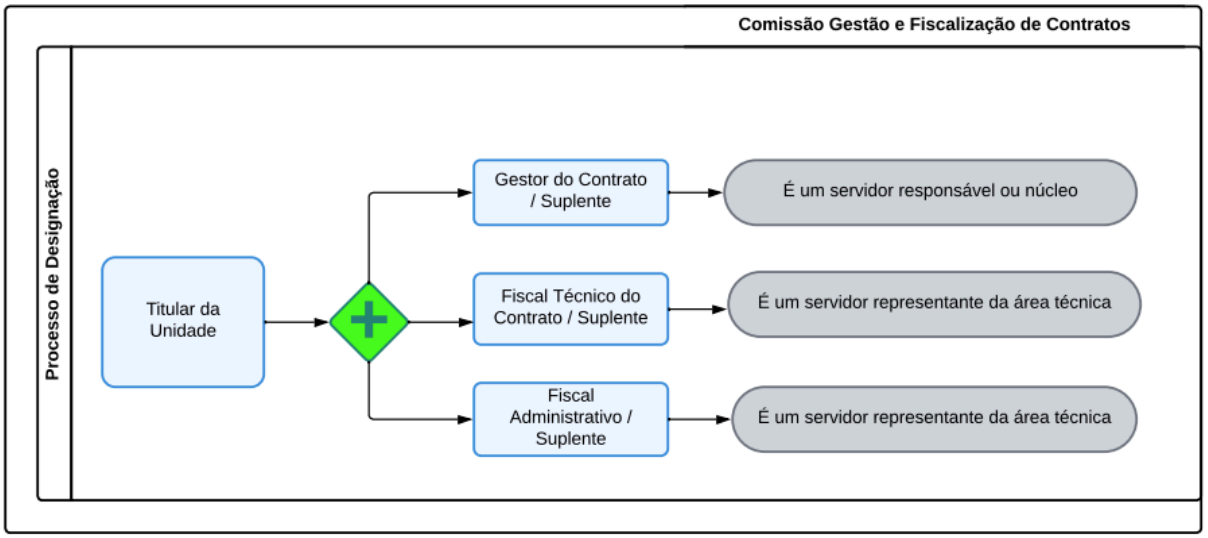


Figura 05 - Designação da Comissão de Fiscalização

A Comissão de Fiscalização composta pelo gestor, fiscais e seus suplentes deverá ser cientificada, expressamente, da indicação e respectivas atribuições, antes da formalização do ato de designação.

Na indicação do servidor devem ser considerados a compatibilidade com as atribuições do cargo, a complexidade da fiscalização, o quantitativo de contratos por servidor e a sua capacidade para o desempenho das suas atividades.

Nos casos de atraso ou falta de indicação, de desligamento ou afastamento, extemporâneo e definitivo, do gestor ou fiscais e seus suplentes, até que seja providenciada a indicação, o exercício de suas atribuições caberá ao responsável pela indicação.

Os servidores designados como fiscais e seus suplentes deverão manter vigilância constante acerca de cláusulas contratuais que julguem merecer maior atenção e, com o cuidado de sempre, fiscalizar a qualidade dos produtos fornecidos, e se as entregas estão ocorrendo de forma oportuna. Deverão verificar se o quantitativo dos recursos utilizados é o adequado, evitando acréscimos desnecessários; zelar pela qualidade do serviço, e acompanhar o tempestivo atendimento das ocorrências apresentadas à contratada.

4.5.2. Conhecimento Técnico

A fiscalização da execução do contrato deve ser realizada por servidores com conhecimento técnico compatível com o objeto contratado, os quais serão escolhidos com fundamento na sua qualificação, conhecimento e capacidade técnica para acompanhar a prestação de serviços.

4.5.3. Acúmulo de Funções

A segregação de funções é o princípio do controle administrativo que confere maior transparência, eficiência, eficácia, imparcialidade e racionalidade em todas as etapas dos processos de execução das despesas públicas.

As funções de fiscal administrativo e fiscal técnico poderão ser acumuladas pelo mesmo servidor, no mesmo contrato, desde que não haja prejuízo ao acompanhamento da execução contratual. Como exemplo, são os casos de contratos de bens comuns, de objetos de menor porte, de menor valor. Não se recomenda, no entanto, o acúmulo de funções no caso de contratações cujo objeto seja mais complexo e de maior valor.

O acúmulo de funções no mesmo contrato é permitido entre quaisquer dos fiscais e gestores. Entretanto, esta é uma exceção à regra, em que é necessário observar a segregação de funções relativas a atores nas etapas do processo de contratações, não podendo ser acumuladas, especialmente aquelas que envolvam a prática de atos e, posteriormente, a revisão desses mesmos atos. A questão é o eventual comprometimento da imparcialidade e, por conseguinte, a execução do contrato, conforme previsto no art. 67 da Lei nº 8.666/93, art. 117 da Lei Federal nº 14.133/2021. Exemplos: exercer função de fiscal e membro da comissão de licitação; fiscal e gestor do contrato; fiscal e integrante da equipe de planejamento, dentre outros.

Caso ocorra a referida acumulação de funções, o gestor do contrato registrará no Plano de Fiscalização.

O suplente do fiscal do contrato terá as mesmas atribuições do fiscal respectivo, na sua substituição, com o acúmulo ou não das funções, conforme previsto, ou poderá acumular também as funções de mais de um fiscal, registrando a opção pelo acúmulo de funções no Plano de Fiscalização.

Recomenda-se que, em novas contratações com objetos de natureza similar, os fiscais sejam mantidos e indicados já na fase inicial de planejamento da contratação, de modo que as informações acerca da execução contratual vigente sejam utilizadas nas definições das quantidades e dos requisitos do processo em fase de elaboração. Caso não sejam mantidos, é importante que eles repassem informações de modo a subsidiar o aprimoramento para as próximas contratações.

4.5.4. Preposto da Empresa

O preposto da empresa será formalmente designado pela contratada antes do início da prestação dos serviços, devendo constar expressamente no instrumento os poderes e deveres em relação à execução do objeto.

A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo gestor de contratos, desde que devidamente justificada, devendo a empresa designar outro representante para o exercício da atividade.

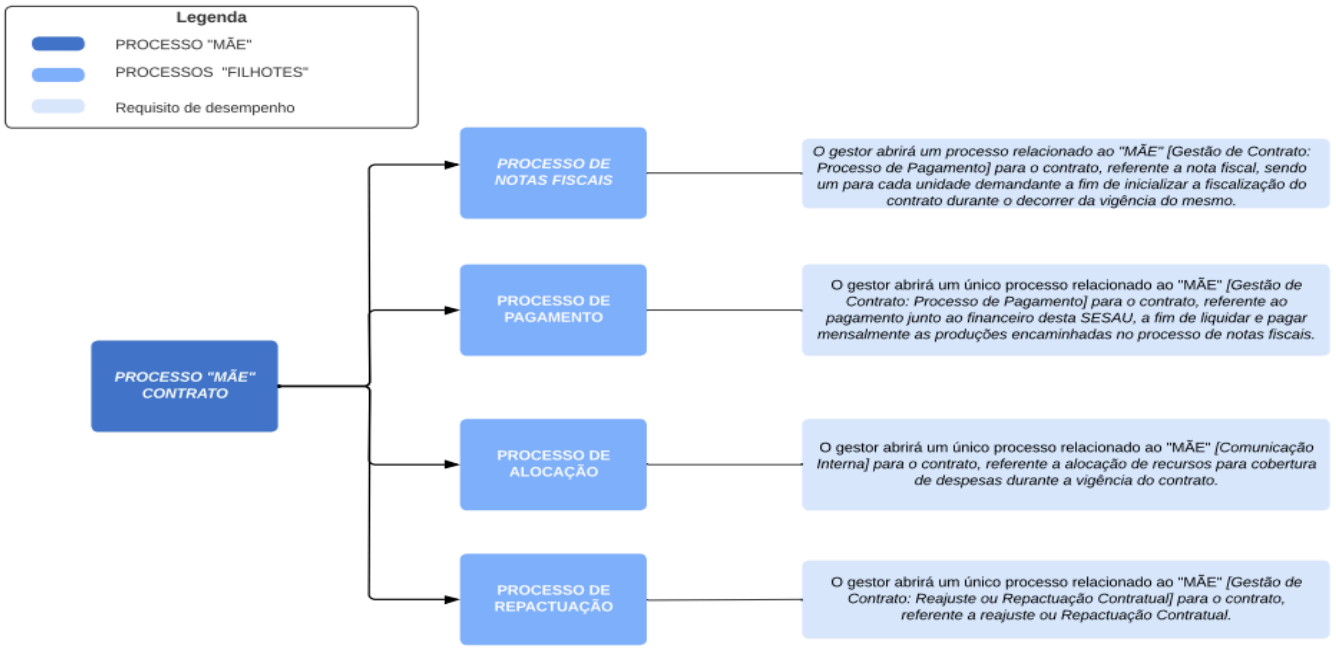
As comunicações entre a SESAU e a contratada devem ser realizadas por escrito sempre que for exigida tal formalidade, podendo ser utilizadas mensagens eletrônicas para esse fim, preferencialmente pelo sistema SEI.

4.5.5. Inicialização da Fiscalização

Após a designação da Comissão de Fiscalização pelo titular da unidade administrativa, ocorrerá a inicialização da fiscalização, na qual o gestor do contrato manterá registros por meio de Processos SEI relacionados ao Processo Originário “MÃE” :

1. [Gestão de Contrato: Processo de Pagamento] para o contrato, referente a nota fiscal, sendo um para cada unidade demandante a fim de inicializar a fiscalização do contrato durante o decorrer da vigência do mesmo.
2. Em seguida o gestor abrirá um único processo relacionado ao "MÃE" [Gestão de Contrato: Processo de Pagamento] para o contrato, referente ao pagamento junto ao financeiro desta SESAU, a fim de liquidar e pagar mensalmente as produções encaminhadas no processo de notas fiscais.
3. O gestor abrirá um único processo relacionado ao "MÃE" [Comunicação Interna] para o contrato, referente a alocação de recursos para cobertura de despesas durante a vigência do contrato.
4. O gestor abrirá um único processo relacionado ao "MÃE" [Gestão de Contrato: Reajuste ou Repactuação Contratual] para o contrato, referente a reajuste ou Repactuação Contratual.

Para isso, será utilizada a função de relacionamento de processos (SEI), que é utilizada para agrupar processos que possuam alguma ligação entre si, porém, autônomos, conforme fluxograma a seguir:



Fluxograma: Organização dos Processos Administrativos, disponível também em PDF, no processo SEI nº 0036.041279/2023-79 (ID: 0041976378).

Dessa forma, os documentos do processo licitatório (nato-digitais ou digitalizados) estarão relacionados e disponíveis para acesso no próprio processo de gestão contratual "processo mãe". Logo, será necessário acessar o processo licitatório SEI que lhe deu origem, e realizar os procedimentos para agrupamento de processos, definidos no SEI.

O subprocesso de fiscalização técnica periódica será conduzido pelo fiscal técnico e pode-se iniciar da seguinte forma:

1. Pelo acompanhamento periódico do fiscal técnico, em que verifica se há alguma ocorrência durante a execução do contrato.
2. Durante a fiscalização técnica periódica, caso seja verificada alguma ocorrência, ela deve:
3. Constar em formulário **"Relatório de fiscalização"**[1] , modelo Anexo, e comunicar à contratante (preposto) e ao gestor do contrato, onde aquela (a contratante) tem um prazo (conforme acordado no planejamento de fiscalização) para realizar a correção da ocorrência informada;

[1] **O Relatório de fiscalização é um importante documento à disposição do Fiscal, onde ficará consignada cada etapa do trabalho de Fiscalização e onde será anotado quando forem realizadas visitas, vistorias, encaminhamento de providências, resultados de diligências, incidentes etc. É uma ferramenta com valor de documento formal, e por isso deve ser preenchido com atenção.**

4. Toda vez que detectar alguma ocorrência o fiscal técnico encaminhará um ofício à empresa prestadora dos serviços.
5. Em resposta ao ofício da ocorrência pelo fiscal, se a ocorrência for solucionada pela contratada dentro do prazo, ela enviará a comunicação para o fiscal com o comprovante de correção, e este registrará a solução da ocorrência, que será comunicada também ao gestor do contrato;
6. Após o vencimento do prazo, caso a comunicação não seja enviada pela contratada, faz-se o registro da ocorrência no relatório de fiscalização e comunica-se a irregularidade por meio de despacho, ao gestor do contrato, solicitando notificação;
7. Caso envie a comunicação dentro do prazo e a ocorrência não seja solucionada, faz-se o registro e comunica-se ao gestor do contrato por meio de Despacho, via SEI, ao gestor do contrato, solicitando notificação;
8. O gestor do contrato, ao receber o despacho da irregularidade, verificará se a ocorrência foi solucionada. Caso positivo, dará ciência ao fiscal do contrato, que recebe ciência de acompanhamento.
9. Caso a ocorrência não tenha sido solucionada, o gestor avaliará o procedimento a ser tomado, seja pela necessidade de concessão de novo prazo para a contratada, seja pela necessidade de aplicação de sanções, e dará ciência ao fiscal do contrato;
10. Caso seja concedido novo prazo, ele é acordado de forma a não se incorrer em prejuízo para a administração pública, sendo registrado e comunicado ao contratado, que, após realizar as correções da ocorrência, comunicará ao gestor do contrato a solução com os devidos comprovantes;
11. Caso haja a necessidade de aplicação de sanções, elas serão encaminhadas por meio de despacho para o NAPCP, apurar e aplicar conforme a previsão no contrato.

4.5.6. Fiscalização Contratual Técnica Periódica

O subprocesso de fiscalização técnica periódica será conduzido pelo fiscal técnico, tendo a sua periodicidade definida no Plano de Fiscalização, e pode-se iniciar de duas formas:

I. Pelo acompanhamento periódico do fiscal técnico, em conformidade à frequência já previamente determinada no plano de fiscalização, em que verifica se há alguma ocorrência durante a execução do contrato.
II. Durante a fiscalização técnica periódica, caso seja verificada alguma ocorrência, ela deve:
III. Constar em formulário “Relatório de fiscalização” , modelo Anexo, e comunicada à contratante (preposto) e ao gestor do contrato, onde aquela (a contratante) tem um prazo (conforme acordado no planejamento de fiscalização) para realizar a correção da ocorrência informada;

IV. Quando não for encontrado qualquer tipo de ocorrência, faz-se o registro no relatório de fiscalização. Caso a ocorrência seja encontrada pelo fiscal requisitante, esse comunicará ao fiscal técnico, que avaliará se há necessidade de atuar junto à contratada. Caso positivo, comunicará a ocorrência à contratada e realizará o registro da ocorrência. Caso contrário, apenas realizará o registro da avaliação da ocorrência;

V. Toda vez que detectar alguma ocorrência na execução do contrato, o fiscal do contrato irá verificar se esta medida estava prevista nos riscos indicados no Plano de Gerenciamento de Riscos. Em caso afirmativo, ele fará uma reavaliação das medidas de tratamento adotadas, identificando o motivo de ter ocorrido, e realimentar o Plano de Gerenciamento de Riscos, inserindo as novas medidas a serem adotadas;

VI. Caso a ocorrência não tenha sido prevista no Plano, esse será realimentado, mencionando a ocorrência como um novo risco, avaliando e registrando o seu impacto e probabilidade, e as medidas de tratamento adotadas para fins de se evitá-lo ou mitigá-lo. E sempre que ocorrer alguma alteração na análise de riscos, o fiscal comunicará ao gestor do contrato, e registrar a ciência sobre essa atualização ao fiscal do contrato;

VII. Em resposta à comunicação da ocorrência pelo fiscal, se a ocorrência for solucionada pela contratada dentro do prazo, ela enviará a comunicação para o fiscal com o comprovante de correção, e este registrará a solução da ocorrência, que será comunicada também ao gestor do contrato;

VIII. Após o vencimento do prazo, caso a comunicação não seja enviada pela contratada, faz-se o registro da ocorrência e comunica-se a irregularidade por meio de despacho, ao gestor do contrato, solicitando notificação;

IX. Caso envie a comunicação dentro do prazo e a ocorrência não seja solucionada, faz-se o registro e comunica-se ao gestor do contrato por meio de Despacho, via SEI, ao gestor do contrato, solicitando notificação;

X. O gestor do contrato, ao receber o despacho da irregularidade, verificará se a ocorrência foi solucionada. Caso positivo, dará ciência ao fiscal do contrato, que recebe ciência de acompanhamento e a registrou no relatório de fiscalização;

XI. Caso a ocorrência não tenha sido solucionada, o gestor avaliará o procedimento a ser tomado, seja pela necessidade de concessão de novo prazo para a contratada, seja pela necessidade de aplicação de sanções, e dará ciência ao fiscal do contrato;

XII. Caso seja concedido novo prazo, ele é acordado de forma a não se incorrer em prejuízo para a administração pública, sendo registrado e comunicado ao contratado, que, após realizar as correções da ocorrência, comunicará ao gestor do contrato a solução com os devidos comprovantes; − Caso haja a necessidade de aplicação de sanções, elas serão aplicadas conforme a previsão no contrato e registradas em relatório de fiscalização, com a notificação da contratada.

A figura abaixo ilustra o processo de fiscalização técnica mensal, disponível também em PDF, no processo SEI nº 0036.041279/2023-79, (ID: 0041976401).

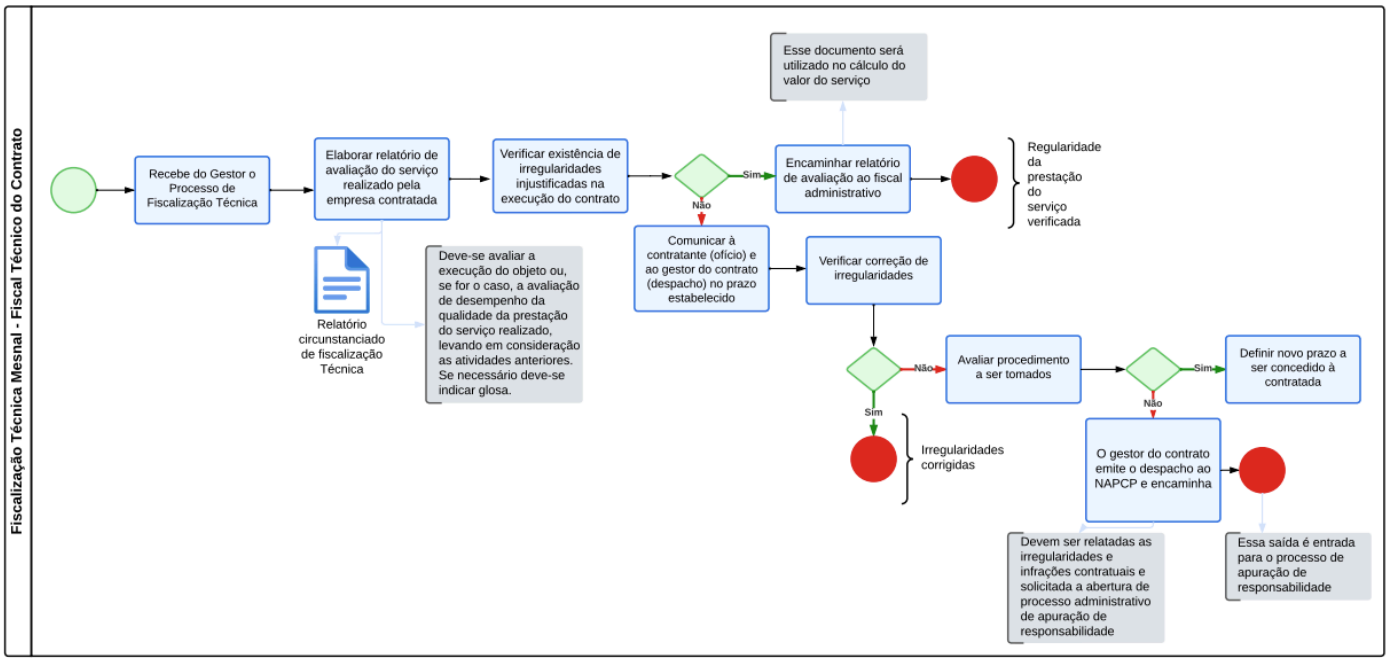


Figura 06 - Fiscalização Técnica Mensal

4.5.7. Fiscalização Contratual Administrativa Mensal

O fiscal administrativo ficará responsável de realizar as tratativas previstas no manual para garantir cumprimento contratual, de regularidades fiscais, de FGTS, sociais e trabalhistas; da situação dos sócios e da empresa, das penalidades e da necessidade de análise de risco.

4.5.8. Verificação Quanto ao Cumprimento Contratual

Consiste na checagem do cumprimento das cláusulas previstas no contrato, principalmente quanto às obrigações da contratada, nas atribuições acessórias relacionadas ao objeto principal contratado. Como exemplo, cumprimento de prazos, entrega de relatórios, oferecer meios de aferição do serviço quando for necessário, verificação de regularidade da documentação, além de:

I. Caso a contratação seja por Registro de Preços, deverá o fiscal administrativo fiscalizar inclusive a Ata de Registro de Preço.
II. Ao detectar irregularidades, fará o registro em Relatório Administrativo de acompanhamento mensal, comunicando a ocorrência ao gestor do contrato e

à contratada, para responder dentro do prazo previsto no Plano de Fiscalização.

III. Em resposta da contratada à comunicação da ocorrência pelo fiscal, se a ocorrência for solucionada dentro do prazo, ela enviará a comunicação para o fiscal com o comprovante de correção, e o fiscal registrará a solução da ocorrência, comunicando também ao gestor do contrato.

IV. Após o vencimento do prazo, caso a comunicação não seja enviada pela contratada, faz-se o registro no relatório e comunica-se a irregularidade por meio de despacho ao gestor do contrato, solicitando notificação.

V. Caso envie a comunicação dentro do prazo e a ocorrência não seja solucionada, faz-se o registro no relatório e comunica-se ao gestor do contrato por meio de despacho (conforme modelo) ao gestor do contrato, solicitando notificação.

VI. O gestor do contrato, ao receber o despacho da irregularidade, verificará se a ocorrência foi solucionada. Caso positivo, registra-se no relatório, e comunica ao fiscal do contrato, que confirmará o cumprimento deste passo, para autorização do pagamento.

VII. Caso a ocorrência não tenha sido solucionada o gestor avaliará o procedimento a ser tomado, sendo a necessidade de conceder um novo prazo para a contratada, ou a necessidade de aplicação de sanções, e dará ciência ao fiscal do contrato.

VIII. Caso seja concedido um novo prazo, ele é acordado de forma a não se incorrer em prejuízo para a administração pública, sendo registrado no relatório, e comunicado ao contratado, que, após realizar as correções da ocorrência, e comunicar ao fiscal do contrato a solução com os devidos comprovantes, e este confirmará o cumprimento deste passo para a autorização do pagamento.

IX. Caso haja a necessidade de aplicação de sanções, elas serão aplicadas conforme a previsão no contrato e registradas no relatório, e notificadas à contratada.

X. Caso não seja detectada irregularidade pelo fiscal administrativo do contrato, realiza-se o registro no relatório, conforme a periodicidade prevista no Plano de Fiscalização, e comunica ao Gestor do contrato, que confirmará o cumprimento deste passo para a autorização do pagamento.

XI. Toda vez que detectar alguma ocorrência na execução do contrato, o fiscal do contrato também irá verificar se esta medida estava prevista nos riscos indicados no Plano de Gerenciamento de Riscos. Em caso afirmativo, ele fará uma reavaliação das medidas de tratamento adotadas, identificando o motivo de ter ocorrido, e realimentará o Plano de Gerenciamento de Riscos, inserindo as novas medidas a serem adotadas.

XII. Caso a ocorrência não tenha sido prevista no Plano, este será realimentado, mencionando a ocorrência como um novo risco, avaliando e registrando o seu impacto e probabilidade, e as medidas de tratamento adotadas para fins de se evitá-lo ou mitigá-lo.

XIII. E sempre que ocorrer alguma alteração na análise de riscos, o fiscal comunicará ao gestor do contrato, e registrará a ciência sobre esta atualização ao fiscal do contrato.

4.5.9. Verificação de Regularidades Fiscais, Sociais e Trabalhistas

Essa verificação consiste em avaliar o cumprimento das obrigações fiscais da contratada perante as esferas federal, estadual e municipal, a regularidade perante o Fundo de Garantia de Tempo de Serviço – FGTS, e a regularidade relativa aos encargos sociais e trabalhistas

A regularidade será comprovada por meio da apresentação dos seguintes documentos:

01. Certidão de Débitos Relativos a Créditos Tributários Federais e à Dívida Ativa da União, quanto à regularidade fiscal no âmbito federal;
02. Certidões Negativas de Débitos emitidas pela Secretaria de Fazenda do Estado de Rondônia e a Secretaria de Fazenda do estado onde ela se encontra situada;
03. Certidão negativa de débitos municipais referente ao município sede da empresa, e ao município onde ela presta o serviço;
04. Certidão negativa do INSS quanto à verificação da existência de débitos previdenciários, referentes aos encargos sociais, e outros documentos que forem pertinentes;
05. Certificado de Regularidade do FGTS – CRF, quanto à regularidade perante o FGTS;
06. Certidão Negativa de Débitos Trabalhistas, referente à regularidade perante o Ministério do Trabalho.

Neste sentido o TCU, nos Acórdãos nº 897/2011-Plenário e 7049/2012 – 2ª Câmara, recomenda a verificação da regularidade fiscal do fornecedor em cada pagamento nos contratos de execução parcelada ou continuada. Eis os textos dos Acórdãos:

> Acórdão nº 879/2011 – Plenário
> **[ACÓRDÃO]**
> 9.2. alertar à Secretaria Municipal de Saúde de Caxias do Sul/RS que:
> 9.2.2. a cada pagamento referente a contrato de execução continuada ou parcelada, deve ser exigida do contratado a comprovação da regularidade fiscal para com a Seguridade Social, o FGTS, as Fazendas Federal, Estadual e Municipal, em observância ao § 3º do art. 195 da Constituição Federal e aos arts. 29, incisos III e IV, e 55, inciso XIII, da Lei nº 8.666/1993; (Grifamos.)
> Acórdão nº 7049/2010 – 2ª Câmara
> **[ACÓRDÃO]**

> 9.2. determinar à Eletrobrás que:
> [...]
> 9.2.8. exija das empresas no ato da assinatura dos contratos, e a cada pagamento, no caso de contratos de execução continuada ou parcelada, a comprovação da regularidade fiscal para com a Seguridade Social (INSS e SRF), com o FGTS (CEF) e com a Fazenda Federal (SRF e PGFN), em observância à Constituição Federal (art. 195, § 3º), Lei nº 8.666/1993 (arts. 29, incisos III e IV, e 55, inciso XIII), Lei nº 8.036/1990 (art. 27, 'a') c/c a de nº 9.012/1995 (art. 2º), Lei nº 8.212/1991 (art. 47) c/c o Decreto nº 3048/1999 (art. 195 e parágrafo único, art. 257, inciso I, alínea 'a' e § 10, alíneas 'a' e 'b'), ao Decreto-Lei nº 147/1967 (art. 62) e ao Acórdão nº 1.922/2003-Primeira Câmara; (Grifamos.)

4.5.10. Pesquisa de Situação dos Sócios e da Empresa

Além das verificações relativas à execução e ao cumprimento do contrato, e das verificações fiscais, existem elementos que podem ocasionar situações de risco que podem comprometer a execução do contrato e a imagem da SESAU-RO.

Essas situações podem ser detectadas por meio de verificações a serem adotadas pelo fiscal do contrato, sempre que julgar necessário e durante toda a vigência do contrato, para avaliar a situação dos sócios, pelas seguintes pesquisas:

I. mudanças expressivas do capital social do fornecedor;
II. mudança no objeto social do fornecedor, em data próxima ao certame;
III. identificação de doações políticas que possam indicar a existência de conflito de interesses dos fornecedores, sócios e representantes;
IV. sócios falecidos ou outra inconsistência que sinalize indícios de fraude, como CPF suspenso, por exemplo;
V. identificação de indícios de alterações em documentos (rasuras, adulterações, falsificações);
VI. realização de pesquisas na internet no processo de contratação e respectivas prorrogações contratuais, para verificação da sua existência ou permanência física no endereço cadastrado;
VII. outras que entenderem necessárias.
VIII. De mesmo modo, avaliar a situação da empresa por meio das seguintes pesquisas:
IX. existência de denúncias e/ou representações relativas à contratação, se:
X. noticiam indicativos de fraude, conluio, direcionamento ou superfaturamento;
XI. noticiam condutas impróprias de agentes da Administração ou a participação societária, ainda que indireta, de servidor/dirigente do órgão/entidade contratante;

XII. noticiam que o fornecedor contratado pelo órgão/entidade subcontrata outra empresa (que participou ou não da cotação de preços);

XIII. se foram divulgadas na mídia notícias de práticas antiéticas, de fraude ou de corrupção referentes ao fornecedor contratado;

XIV. se foram reportadas notícias de ocorrência de situações de conflitos de interesses envolvendo servidores, dirigentes e o fornecedor contratado;

XV. se as denúncias e/ou representações noticiam que agentes da administração possam ter obtido algum tipo de vantagem financeira com a contratação;

XVI. se as denúncias e/ou representações noticiam que a empresa/fornecedor não têm empregados registrados ou não possui patrimônio condizente com a contratação;

XVII. se as denúncias e/ou representações noticiam a participação de agente público, mesmo que informalmente, como representante ou intermediário dos interesses de fornecedor licitante no órgão/entidade contratante;

XVIII. outras que entenderem necessárias.

XIX. No Anexo constam de forma exemplificativa fontes de busca/consulta em que podem ser realizadas essas pesquisas. Ressalta-se que a não detecção da situação avaliada, por meio dessas pesquisas, não garante que o fato não tenha ocorrido. Essas fontes podem ser alteradas com o decurso do tempo.

XX. A periodicidade da realização dessas pesquisas, a seleção de quais pesquisas serão realizadas constarão no planejamento de fiscalização da contratação, podendo-se, a qualquer momento durante a execução do contrato, serem inseridas novas pesquisas.

XXI. Ao detectar alguma dessas situações ou divergências, o fiscal faz:

XXII. o registro da constatação ou divergência e a evidenciação em documento próprio - Anexo;

XXIII. uma avaliação do risco ao contrato e o registro da recomendação de tratamento do risco no Modelo de Análise de Riscos; e

XXIV. prepara um despacho a ser encaminhado para o Gestor do Contrato, com a constatação ou divergência, e a avaliação do risco junto com a sugestão de tratamento (no caso dos riscos mitigáveis e evitáveis).

Caso o risco da constatação não seja aceitável, deverá ser mitigado ou evitado, sendo necessário, que o fiscal administrativo elabore um despacho a ser encaminhado para o gestor do contrato, com a avaliação do risco, que deverá conter a constatação ou divergência e a avaliação do risco, já com a sugestão de tratamento, e registrou também a recomendação do tratamento do risco no Modelo de Análise de Riscos.

Cabe ressaltar que mesmo que não for detectada a constatação ou divergência pelo fiscal administrativo do contrato, de qualquer forma, o registro no relatório será realizado. Ao gestor do Contrato, ao receber o despacho,o mesmo irá avaliar a constatação ou divergência e o seu risco, e:

a) Caso avaliar o risco da constatação como aceitável, ele registra a aceitação do risco no Modelo de Análise de Riscos, e comunicará a aceitação do risco para o fiscal administrativo.
b) Caso o risco seja mitigável, o gestor do contrato avalia a recomendação de tratamento registrada pelo fiscal no Modelo de Análise de Risco.
c) Caso seja aprovado o tratamento, registra a aprovação no Modelo de Análise de Risco, e aplicará o tratamento ao risco e comunicará ao fiscal.
d) Caso o tratamento não seja aprovado, é realizada nova avaliação do risco, no qual será estabelecido um novo tratamento, que será aplicado, e registrado no Modelo de Análise Riscos, e comunica-se ao fiscal.
e) Caso o risco for evitável, o gestor do contrato notifica a contratada.

4.5.11. Das Penalidades

No caso de ocorrências de fatos decorrentes do contrato que ensejem penalidades cabíveis à contratada, conforme informações prestadas pelo fiscal de contrato, o gestor deve analisá-los e realizar entendimentos devidamente fundamentados que possam subsidiar a instauração de processo administrativo para aplicação de penalidades à contratada, sem prejuízo das demais ações cabíveis no âmbito das competências dos fiscais e gestores de contrato.

Conforme art. 7º da Lei Federal nº 10.520/02, em relação aos contratos com a administração pública, existe a necessidade do gestor autuar processos administrativos contra as empresas que praticarem atos ilegais tipificados neste artigo, como: (i) convocado dentro do prazo de validade da sua proposta, não celebrar o contrato, (ii) deixar de entregar, ou apresentar documentação falsa exigida para o certame, iii) ensejar o retardamento da execução de seu objeto, (iv) não mantiver a proposta, (v) falhar ou fraudar a execução do contrato, (vi) comportar-se de modo inidôneo ou (vii) cometer fraude fiscal.

A não autuação sem justificativa dos referidos processos poderá ensejar a aplicação de sanções a seus gestores, conforme previsão do art. 82 da Lei Federal nº 8.666/93, bem como representação por parte do Tribunal de Contas do Estado.

Da mesma forma, constitui motivo para rescisão do contrato o desatendimento das determinações regulares da autoridade designada para acompanhar e fiscalizar a sua execução, assim como as de seus superiores, bem como razões de interesse público, de alta relevância e amplo conhecimento, justificadas e determinadas pela máxima autoridade da esfera administrativa a que está subordinado o contratante, e exaradas no processo administrativo a que se refere o contrato (Lei Federal nº 8.666/93, art. 78, VII e XII).

Deve-se observar a aplicação das sanções legais previstas na Lei n.º 8.666/93, arts. 81 a 88 e 109, conforme o caso concreto.

4.5.12. Verificação da Necessidade de Análise de Riscos

Quanto à gestão de riscos, refere-se ao processo contínuo que consiste no desenvolvimento de um conjunto de ações destinadas a identificar, analisar, avaliar, priorizar, tratar e monitorar riscos positivos ou negativos capazes de afetar os objetivos, programas, projetos ou processos de trabalho do Tribunal nos níveis estratégico, tático e operacional.

Cabendo ao gestor manter atualizado o mapa de riscos elaborado na fase de planejamento da contratação, procedendo à sua reavaliação anualmente, nas prorrogações de vigência ou após a ocorrência de eventos relevantes, visando à boa e regular execução do contrato.

A implementação da gestão de riscos e controles internos dos processos licitatórios e os respectivos contratos está prevista na recente Lei das Licitações (Lei nº 14.133/2021), no parágrafo único do art. 11, e art. 169, que tratam de diretrizes para a implementação de práticas contínuas e permanentes de gestão de riscos e controle preventivo, de responsabilidade da alta administração e integrantes das três linhas de defesa do órgão.

Eis o texto da Lei:

> "Art. 11 - Parágrafo único. A alta administração do órgão ou entidade é responsável pela governança das contratações e deve implementar processos e estruturas, inclusive de gestão de riscos e controles internos, para avaliar, direcionar e monitorar os processos licitatórios e os respectivos contratos, com o intuito de alcançar os objetivos estabelecidos no caput deste artigo, promover um ambiente íntegro e confiável, assegurar o alinhamento das contratações ao planejamento estratégico e às leis orçamentárias e promover eficiência, efetividade e eficácia em suas contratações."

Da mesma forma que é feita pela fiscalização periódica, toda vez que se detectar a ocorrência na execução do contrato, o fiscal administrativo do contrato:

I. Verificará se essa medida estava prevista no Plano de Gerenciamento de Riscos. Em caso afirmativo, ele fará uma reavaliação das medidas de tratamento propostas, identificando o motivo de ter ocorrido, e realimentará o plano de risco inserindo as novas medidas a serem adotadas.
II. Caso a ocorrência não tenha sido prevista no Plano, este será realimentado, mencionando a ocorrência como um novo risco, avaliando e registrando o seu impacto e probabilidade, e as medidas de tratamento adotadas para fins de mitigá-lo ou evitá-lo.
III. Sempre que ocorrer alguma alteração na análise de riscos, o fiscal administrativo comunicará ao gestor do contrato, e retornará ao fiscal administrativo do contrato a ciência sobre esta atualização.

Alguns exemplos de considerações de riscos e controles que uma organização do setor público pode ter na fase de gerenciamento e fiscalização do processo de contratação estão descritos em anexo.

4.5.13. Preparação e Instrução do Processo para fins de Pagamento ao Fornecedor

A despesa será liquidada e paga mediante exame prévio de sua legalidade, com base nos documentos comprobatórios exigidos em legislação específica.

O processo de liquidação e pagamento das despesas provenientes de compras, de prestação de serviços, inclusive de serviços de Tecnologia da Informação e Comunicação (TIC), ou de execução de obras será formalizado pela unidade orçamentária/executora contratante, em expediente devidamente autuado no SEI, com a junção dos seguintes documentos necessários, conforme o caso:

- Cópia do ato que designou a comissão de Fiscalização do contrato;
- Cópia do contrato ou instrumento hábil equivalente e seus termos aditivos (vincular o processo de contratação SEI correspondente);
- Cópia da nota de empenho, devidamente assinada por meio de certificação digital;
- Primeira via da nota fiscal ou nota fiscal / fatura, nota fiscal de serviços eletrônica ou documento equivalente;
- Cópia da requisição de fornecimento de materiais, de prestação de serviços ou execução de obras;
- Medições detalhadas que atestem a execução de obras ou serviços executados no período a que se refere o pagamento;
- Cópia do Certificado de Regularidade Cadastral do fornecedor (caso esteja irregular, entrar em contato com a empresa e solicitar a regularização);
- Demonstrativo de retenção dos impostos devidos e outros descontos referentes ao pagamento da despesa;
- Certificado de regularidade do FGTS;
- Certidão negativa ou positiva com efeitos de negativa, de débitos relativos às contribuições previdenciárias e às de terceiros – INSS;
- Certidão negativa de débitos trabalhistas;
- Outras certidões de regularidade fiscal julgadas necessárias previstas no contrato;
- Outros documentos definidos em contrato.

Para pagamento de serviços contínuos com dedicação de mão de obra, incluir nos autos os seguintes documentos:

- Relatórios com os resultados dos exames admissionais, periódicos, demissionais, por mudança de função e por retorno ao trabalho, assinado pelo

médico do trabalho coordenador, conforme NR7 que compõe a Portaria n.º 3.214 do Ministério do Trabalho, de 08 de junho de 1978, e suas alterações;
- Convenção Coletiva a qual há empresa é vinculada.
- Cópia da carteira de trabalho e a conferência se o salário registrado está de acordo com a convenção coletiva. (as cópias deverão ficar na unidade).
- Relação atualizada dos empregados vinculados à execução do contrato;
- Escala dos funcionários referente ao período de execução do serviço (deverá ser entregue ao fiscal administrativo 24 horas antes do início do mês e informá-lo quanto a qualquer alteração de funcionário).
- Folha de frequência ou registros correspondentes dos empregados vinculados à execução do contrato (Todos os funcionários deverão ter).
- Folha de pagamento dos empregados vinculados à execução do contrato (correspondentes ao mês da última nota fiscal vencida), caso seja o primeiro pagamento não é necessário a apresentação do mesmo.
- Contracheques e Comprovantes de pagamento salário (correspondentes ao mês da última nota fiscal vencida), caso seja o primeiro pagamento não é necessário a apresentação do mesmo.
- Comprovante de Pagamento de Vale Transporte (correspondentes ao mês da última nota fiscal vencida), caso seja o primeiro pagamento não é necessário a apresentação do mesmo.
- Comprovante de Pagamento de Vale alimentação (correspondentes ao mês da última nota fiscal vencida), caso seja o primeiro pagamento não é necessário a apresentação do mesmo.
- Comprovantes de pagamento de seguro contra acidentes de trabalho
- Cópia do Protocolo de envio de arquivo emitido pela conectividade Social (GFIP/SEFIP);
- Cópia da relação dos trabalhadores constantes do arquivo SEFIP do mês da última fatura vencida;
- Cópia da guia quitada do INSS correspondente ao mês anterior ao pedido de pagamento;
- Cópia da guia quitada do FGTS correspondente ao mês anterior ao pedido de pagamento.

Gestor do contrato

Ao receber toda a documentação supra relacionada, o Gestor do contrato providenciará:

- Ciência, em campo próprio do Termo de recebimento definitivo, dos relatos informados, verificações realizadas e atestes dos fiscais responsáveis pelo recebimento do material, bens ou serviços, com declaração de que foram recebidos ou efetuados em condições satisfatórias para a Administração Estadual.
- Estando de acordo, o Termo Recebimento Definitivo do bem e/ou serviço contratado (caso contrário, devolverá a documentação para os fiscais

designados para tomar as providências necessárias, até que sejam sanados os apontamentos).

- Ateste para liberação da Nota Fiscal / Fatura para o Setor Financeiro para os procedimentos regulares de liquidação e ordem de pagamento ao fornecedor.
- Despacho dos autos para o Ordenador de despesas, conforme fluxograma de pagamento abaixo.

A figura abaixo ilustra o processo de fiscalização Administrativa mensal, disponível também em PDF, no processo SEI nº 0036.041279/2023-79, (ID: 041976413).

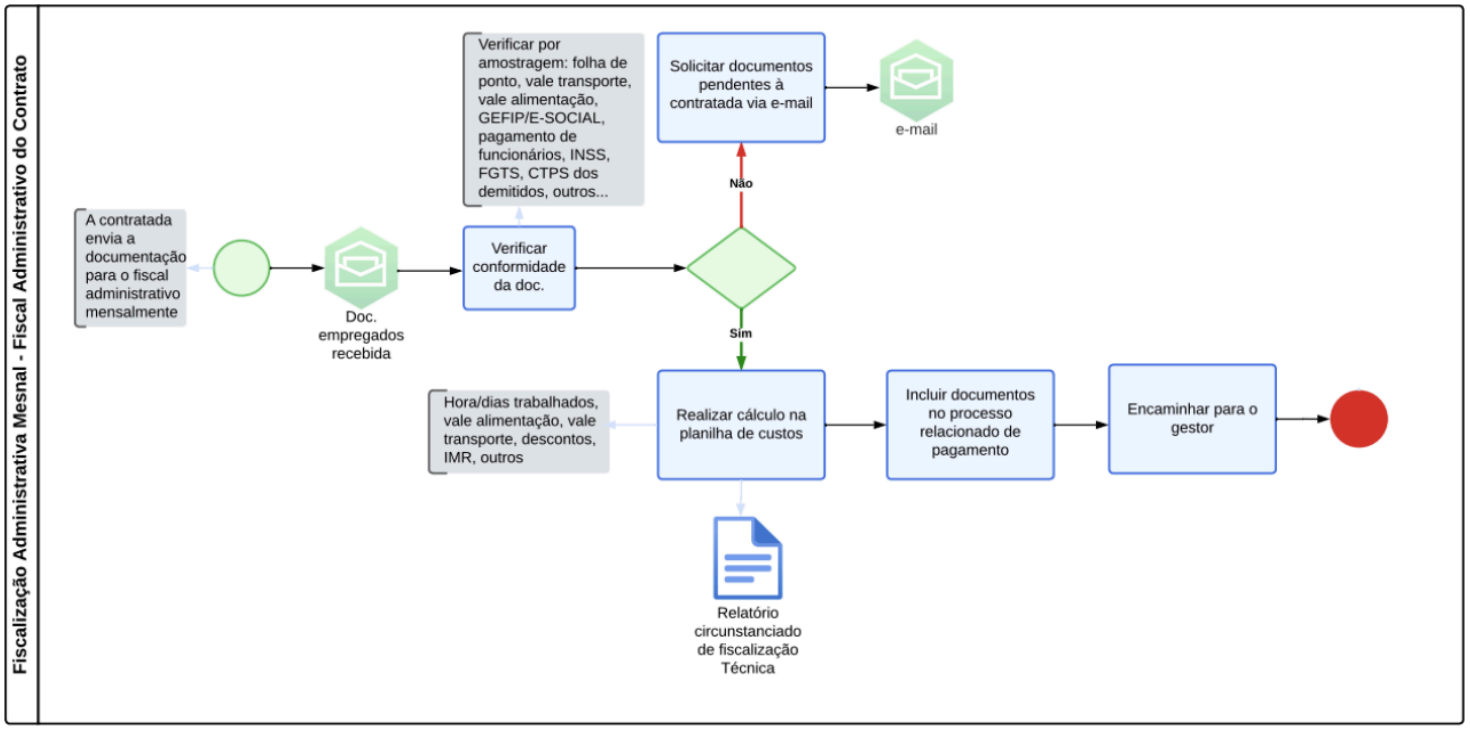


Figura 07 - Fiscalização Administrativa mensal

Setor Financeiro da Unidade Executora

Por fim, o Ordenador de despesas verificará se a documentação recebida atende às condições para o prosseguimento do processo de pagamento da despesa, nos termos da Lei Federal n.º 4.320/64.

Caso não atender às condições contratadas, o Ordenador das despesas devolverá a documentação para o Gestor do contrato, para tomar as providências necessárias, e quando sanados os apontamentos, retornará para o ordenador de despesas.

5. GESTÃO E FISCALIZAÇÃO DE CONTRATOS ESPECÍFICOS DE SAÚDE

As empresas que prestam serviços de saúde deverão apresentar à Administração Pública relatórios mensais para fins de comprovação do adimplemento do objeto do contrato qualitativa e quantitativamente, para avaliação da Coordenadoria de Regulação e Controle dos Serviços de Saúde (SESAU-CRECSS), que procederá com as análises necessárias para fins de comprovação dos serviços prestados.

5.1. Do Monitoramento e Avaliação dos Serviços

A contratante/credenciante, por meio da Coordenadoria de Regulação e Controle dos Serviços de Saúde – CRECSS e equipe da comissão de fiscalização das Regionais de Saúde acompanharão a avaliação da qualidade do atendimento, controle e monitoramento dos serviços realizados, de acordo com a legislação vigente.

As empresas contratadas/credenciadas se obrigam a permitir que a equipe de controle, avaliação e auditoria e comissão de fiscalização de contrato da Secretaria de Saúde e/ou auditoria externa por ela indicada tenham acesso a todos os documentos que digam respeito ao objeto do instrumento contratual.

A avaliação será considerada pela contratante para avaliar a necessidade de solicitar à contratada/credenciada que melhore a qualidade dos serviços prestados, para decidir sobre a conveniência de renovar ou rescindir o contrato ou, ainda, para fornecer, quando solicitado declarações sobre o desempenho e conformidade dos serviços prestados.

5.2. Do Reajustamento ao Contrato de Saúde

Os preços contratados serão alterados de acordo com os reajustes efetuados pelo Ministério da Saúde no Sistema de Gerenciamento da Tabela de Procedimentos, Medicamentos e OPM do SUS (SIGTAP), e/ou ainda de acordo com as tabelas complementares de financiamento definidas por meio de pactuações na Comissão Intergestores Bipartite (CIB), as quais serão incorporadas no âmbito da Secretaria de Estado da Saúde de Rondônia por meio de Portaria específica.

5.3. Pagamento - Contrato de Saúde

O pagamento ocorrerá mensalmente a partir do segundo mês de execução, exclusivamente sobre os serviços efetivamente executados, consoante aos parâmetros de valoração estabelecidos na contratação, devendo ser apresentadas para a SESAU/RO, as Notas Fiscais/Faturas emitidas em 02 (duas) vias, juntamente com a produção referente ao período requerido, contendo documentos probantes (relação de pacientes atendidos, com endereço, documentos pessoais, telefone e outros que a CONTRATANTE achar pertinente) e devidamente atestadas pela Administração, devendo constar no corpo da mesma: a descrição do objeto, o número do Contrato e número da Conta Bancária da empresa contratada/credenciada, para depósito do pagamento, o qual deverá ser efetuado, em ordem cronológica, no prazo de até **30 (trinta)** dias corridos.

E será efetuado mediante a apresentação de Nota Fiscal ou da Fatura pela contratada, devidamente atestada pela Administração.

A figura a seguir ilustra quanto ao fluxo de pagamento para os serviços de saúde com a finalidade de cumprir o prazo de até 30 (trinta) dias corridos, disponível também em PDF, no processo SEI nº 0036.041279/2023-79 (ID: 041976429).

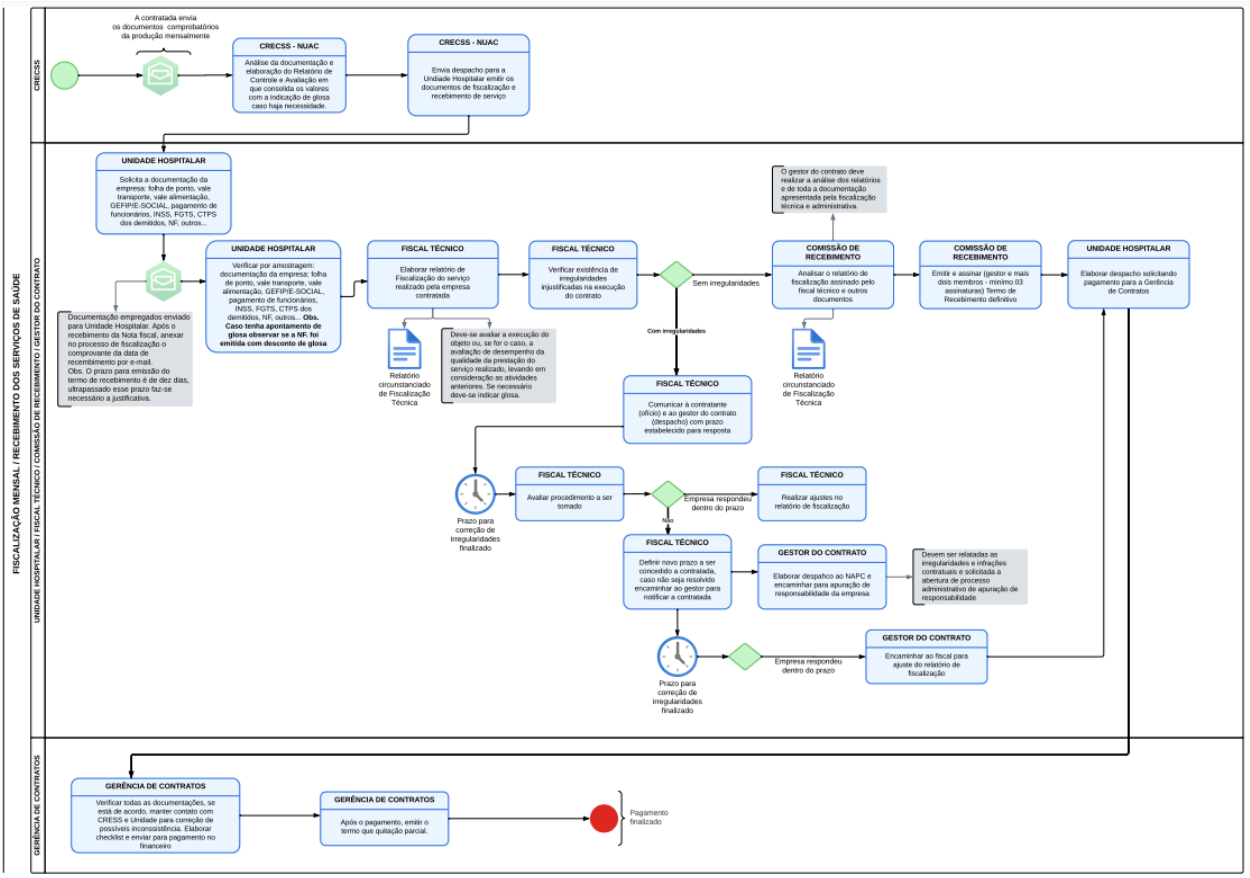


Figura 08 - Fluxo de pagamento dos serviços de saúde

6. DA COMPETÊNCIA DOS SETORES E PRAZOS

SETOR	COMPETÊNCIA
Gerência de Contratos	Gestor de Contrato
Unidades hospitalares e Administrativas	Fiscal Técnico
GAD das unidades hospitalares e Administrativas	Fiscal Administrativo
DOCUMENTOS	**PRAZOS**
Relatório de Fiscalização Técnica	No início do mês, abre o documento “relatório de fiscalização” e inicia o registro das ocorrências durante aquela competência. Ex. No dia 03/01, inicia a fiscalização com registros das ocorrências e no decorrer do mês faz a alimentação de

	todas as ocorrências e quando necessário notifica a empresa e comunica o gestor. Ao final do mês o fiscal assina o documento e encaminha o processo para o fiscal administrativo.
Relatório Administrativo	Após o fechamento do mês, com o prazo de 10 (dez) dias, o Fiscal Administrativo emite o relatório com toda a verificação da documentação trabalhista e pagamentos da empresa.
Termo de Recebimento Definitivo	Com prazo de até 10 dias após o recebimento da nota fiscal, caso seja ultrapassado o prazo é necessário inserir a justificativa da morosidade na emissão do documento.

7. ANEXOS

Buscando atender as ações e tratativas, atinentes a gestão de contratos, disponibilizamos no quadro 4, a relação dos documentos (Modelo), que por sua vez, configuram-se como sugestão,o qual não restringe, readaptar, restruturar, pela unidade recebedora dos serviços julgar necessários, desde que estejam em consonância com os ditames, previstos no o Art. 140 da Lei nº 14.133, de 1º de Abril de 2021, que trata do recebimento em termo detalhado dos serviços.

Quadro 4- Exemplos de documentos, disponibilizados no processo SEI nº 0036.041279/2023-79, com a disponibilização de documentos a serem utilizados como modelo.	
Documentos - Processo SEI nº 0036.041279/2023-79.	**Documento Modelo**
Minuta de Portaria designação da Comissão de Fiscalização	**(0041384119)**
Fluxograma Organização dos processos "filhotes"	**(0041976378)**
Fluxograma Fiscalização Mensal Administrativa	**(0041976413)**

Fluxograma Pagamento Saúde	**(0046352436)**
Análise 1 Considerações de risco na fiscalização	**(0041546889)**
Adendo Ex. de fontes de consulta de situação da empresa	**(0041546986)**
Termo de Recebimento Provisório Geral todos os objetos	**(0041541099)**
Termo de Recebimento Definitivo Geral todos os objetos	**(0041384717)**
Planilha Mão de obra	**(0041549508)**
Relatório Administrativo DEMO TODOS OS OBJETOS	**(0041549547)**
Relatório de Fiscalização LAVANDERIA	**(0041489140)**
Relatório de Fiscalização VIGILÂNCIA	**(0041554333)**
Termo de Recebimento Definitivo 2 Aluguel	**(0041682401)**
Relatório de Fiscalização Aluguel	**(0041688415)**
Termo de Recebimento Definitivo 4 Monitoramento de Água	**(0041699949)**
Relatório de Fiscalização Monitoramento de Água	**(0041815812)**
Relatório de Fiscalização Serviço Autônomo de Água	**(0041726325)**
Relatório de Fiscalização Ar e Gases Medicinais	**(0041702595)**
Relatório de Fiscalização Locação de Compressor	**(0041800790)**
Relatório de Fiscalização Cirurgia Neurologia e Pediátrica	**(0041704540)**

Termo de Recebimento Definitivo 8 Cirurgia Neurologia e Pediátrica	**(0041806171)**
Relatório de Fiscalização Coleta de Lixo	**(0041727712)**
Termo de Recebimento Definitivo 5 Tratamento de Esgoto	**(0041740995)**
Relatório de Fiscalização SERVIÇO DE UROLOGIA Litotripsia Extracorpórea	**(0041749351)**
Relatório de Fiscalização Limpeza Administrativa/Hospitalar	**(0041782247)**
Relatório de Fiscalização Técnica de Engenharia Clínica	**(0041799235)**
Termo de Recebimento Definitivo 7 Serviços de acolhimento voluntário	**(0041803736)**
Relatório de Fiscalização Tratamento de Esgoto	**(0041804691)**
Relatório de Fiscalização Técnica de UTI - NEO/PED/ADULTO	**(0041806237)**
Termo de Recebimento Provisório Serviços de impressão	**(0041808404)**
Termo de Recebimento Definitivo 9 Serviços de impressão	**(0041807756)**
Relatório de Fiscalização Serviços de impressão	**(0041809151)**
Relatório de Fiscalização Manutenção de Climatização - Ar Condicionado	**(0041808997)**
Relatório de Fiscalização técnica de TRS	**(0041810573)**
Relatório de Fiscalização Container	**(0041811072)**

Termo de Recebimento Definitivo 11 Container	**(0041813885)**
Termo de Recebimento Definitivo 10 Locação e Manutenção de Grupo Gerador	**(0041811815)**
Termo de Recebimento Definitivo 10 Locação e Manutenção de Grupo Gerador	**(0041811815)**
Termo de Recebimento Definitivo 12 Mandados Judiciais	**(0041815581)**
Relatório de Fiscalização Mandados Judiciais	**(0041820025)**
Termo de Recebimento Definitivo 16 Leitos Clínicos	**(0041824934)**
Relatório de Fiscalização SERVIÇOS DE HEMODIÁLISE	**(0041816069)**
Relatório de Fiscalização Limpeza de Fossas	**(0041823396)**
Termo de Recebimento Definitivo 17 Análises clínicas	**(0041825441)**
Relatório de Fiscalização Serviços Funerários	**(0041828216)**
Termo de Recebimento Definitivo 19 - Plantões Médicos	**(0041829046)**
Relatório de Fiscalização serviços postais	**(0041831901)**
Termo de Recebimento Definitivo 20 AMBULÂNCIA	**(0041834560)**
Relatório de Fiscalização AMBULÂNCIA	**(0042195879)**
Relatório de Fiscalização CIRURGIA PEDIÁTRICA	**(0041860012)**
Termo de Recebimento Provisório Alimentação	**(0041670156)**
Relatório de Fiscalização Alimentação	**(0041667856)**

Adendo Relatório de Fiscalização Alimentação	**(0041882443)**
Relatório Administrativo Alimentação	**(0041667803)**
Termo de Recebimento Definitivo 1 Alimentação	**(0041670194)**
Relatório de Fiscalização Agenciamento de Passagem Terrestre	**(0042270791)**
Termo de Recebimento Provisório Agenciamento de Passagem Terrestre	**(0042334405)**
Termo de Recebimento Definitivo 25 Agenciamento de Passagem Terrestre	**(0042334430)**
Relatório de Fiscalização serviço de Dosimetria	**(0042334005)**
Termo de Recebimento Definitivo 24 serviço de Dosimetria	**(0042334112)**
Relatório de Fiscalização RECEPÇÃO	**(0042334668)**
Termo de Recebimento Provisório RECEPÇÃO	**(0042334685)**
Termo de Recebimento Definitivo 26 RECEPÇÃO	**(0042334696)**
Relatório de Fiscalização Agenciamento de Passagem aérea	**(0042458627)**

8. REFERÊNCIAS

BRASIL. Lei n° 14.133, de 1º de abril de 2021. Lei de Licitações e Contratos Administrativos. Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14133.htm. Acesso em: 01 mar. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2018]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm. Acesso em: 01 mar. 2024.

BRASIL. Decreto n° 7.892, de 23 de janeiro de 2013. Regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993. Brasília, DF: Presidência da República, [2013]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/decreto/d7892.htm. Acesso em: 01 mar. 2024.

BRASIL. Decreto n° 10.024, de 20 de setembro de 2019. Regulamenta a licitação, na modalidade pregão, na forma eletrônica, para a aquisição de bens e a contratação de serviços comuns, incluídos os serviços comuns de engenharia, e dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal. Brasília, DF: Presidência da República, [2019]. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019- 2022/2019/Decreto/D10024.htm. Acesso em: 01 mar. 2024.

BRASIL. Decreto n° 11.246, de 27 de outubro de 2022. Regulamenta o disposto no § 3° do art. 8º da Lei n° 14.133, de 1° de abril de 2021. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Decreto/D11246.htm. Acesso em: 01 mar. 2024.

_____. Lei nº 4.320, de 17 de março de 1964. Estatui Normas Gerais de Direito Financeiro para elaboração e controle dos orçamentos e balanços da União, dos Estados, dos Municípios e do Distrito Federal. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l4320.Acesso em: 01 mar. 2024.

_____. Lei nº 8.666, de 1 de junho de 1993. Regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências. Acesso em: 01 mar. 2024.

MINAS GERAIS. Manual de Fiscalização de Gestão e Fiscalização de Contratos Administrativos. Secretaria de Estado de Fazenda de Minas Gerais . Belo Horizonte, 2023. Disponível em:https://https://www.fazenda.mg.gov.br/transparencia/compras-e-contratos/Manual_de_Gestao_e_Fiscalizacao_SEF_2022.pdf.Acesso em: 01 mar. 2024.

BRASÍLIA. Manual de Gestão e Fiscalização de Contratos. Ministério da Cultura. Brasília, 2013. Disponível em: contratos.cultura.gov.br/Manual/Manual_gestao_fiscalizacao_de_contratos_Minc.PDF.Acesso em: 01 mar. 2024.

GOVERNO DO ESTADO DE RONDÔNIA
Secretaria de Estado da Saúde - SESAU

MAPA DE RISCO

Risco	Descrição	Possíveis Causas	Fase	Nível	Ações Preventivas	Controle de Contingência	Responsável
Impugnação do edital de licitação	Impugnação do edital por participantes, atrasando o processo licitatório.	Edital mal redigido, cláusulas ambíguas.	Licitação	Alto	Revisar o edital detalhadamente antes da publicação, consulta pública prévia.	Responder prontamente às impugnações e corrigir o edital se necessário.	SUPEL
Falta de propostas qualificadas	Poucas ou nenhuma proposta que atendam aos requisitos da licitação.	Divulgação insuficiente, requisitos muito restritivos.	Licitação	Alto	Divulgação ampla da licitação, reuniões de esclarecimento com possíveis interessados.	Realizar nova licitação com ajustes nos requisitos.	Unidade requisitante / GECOMP
Problemas na análise de propostas	Erros ou falhas na análise das propostas recebidas, levando a recursos e atrasos.	Falta de capacitação da comissão, critérios de avaliação mal definidos.	Licitação	Médio	Treinamento da comissão de licitação, estabelecimento de critérios claros de avaliação.	Revisão das propostas por uma equipe secundária, se necessário.	SUPEL
Recursos administrativos	Interposição de recursos administrativos pelos participantes, atrasando o processo.	Falta de transparência, erros na análise.	Licitação	Médio	Garantir transparência e clareza no processo licitatório.	Responder rapidamente aos recursos e corrigir possíveis falhas.	SUPEL
Irregularidades na documentação dos proponentes	Documentação incompleta ou irregular dos participantes da licitação.	Falta de verificação detalhada.	Licitação	Médio	Verificação rigorosa da documentação durante a fase de habilitação.	Dar prazo para regularização e verificar novamente.	SUPEL
Fraude ou conluio entre participantes	Tentativas de manipulação do processo licitatório por conluio entre os participantes.	Falta de monitoramento e auditoria.	Licitação	Alto	Monitoramento contínuo e auditoria do processo licitatório.	Denúncia às autoridades competentes, cancelamento da licitação.	SUPEL
Problemas de comunicação entre as partes	Falhas na comunicação entre SESAU e a empresa contratada.	Falta de canais de comunicação definidos, reuniões insuficientes.	Execução	Médio	Estabelecer canais de comunicação claros, reuniões regulares de acompanhamento.	Implementação de sistema de gestão de comunicação.	Fiscal de contrato / Gerência de contratos

Atraso	Atraso na entrega das soluções	Problemas logísticos; Fornecedor enfrenta dificuldades operacionais	Execução	Médio	Cronograma claro e monitoramento constante do progresso; Penalidades contratuais por atrasos	Negociação com a contratada para resolução rápida; Escalonamento para gerência de contratos	Fiscal de contrato / Gerência de contratos
Dificuldade em atender aos requisitos	Dificuldade em atender aos requisitos regulatórios de segurança	Mudanças nas regulamentações; Falta de atualização das soluções	Execução	Médio	Acompanhamento contínuo das regulamentações aplicáveis; Reuniões periódicas com a contratada para alinhamento	Implementação de soluções complementares; Revisão do contrato para inclusão de novas exigências	Unidade requisitante, Fiscal de contrato

Porto Velho, 16 de agosto de 2024.

TALITA BRILHANTE SANTANA AZEVEDO
Técnico Administrativo Operacional da Saúde - GECOMP/SESAU

MARCOS ALESSANDRO FERNANDES SALES
Gerente de Compras em substituição- GECOMP/SESAU
Portaria nº 4477 de 28 de junho de 2024

Documento assinado eletronicamente por **Marcos Alessandro Fernandes Sales**, **Subgerente**, em 16/08/2024, às 14:22, 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 **TALITA BRILHANTE SANTANA AZEVEDO**, **Técnico**, em 19/08/2024, às 09:16, 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 **0051897532** e o código CRC **743FCF31**.

Referência: Caso responda este(a) Mapa de Risco, indicar expressamente o Processo nº 0036.028242/2024-36 SEI nº 0051897532

GOVERNO DO ESTADO DE RONDÔNIA
Secretaria de Estado da Saúde - SESAU
NÚCLEO DE PROCEDIMENTOS ACESSÓRIOS - SESAU-NPA

RELATÓRIO

RELATÓRIO DE PESQUISA DE PREÇOS

Instrução Normativa nº 01/2024/SUPEL-CPEAP

(Processo Administrativo nº 0036.028242/2024-36)

1. DESCRIÇÃO DO OBJETO A SER CONTRATADO (art. 3º, inc. I)

Objeto: O Relatório da Pesquisa de Preços foi elaborada em atenção ao Art. 51 do Decreto Estadual nº 28.874/2024 e Art. 23 da Lei Federal nº 14.133/2024 . Des agente tecnicamente capaz de definir quantitativa e qualitativamente as necessidades do objeto, visando Registro de Preços para contratação de empresa para fornecimento, sob mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da período de 3 (três) anos. , conforme descrito no Documento de Oficialização de Demanda - DOD (0054733868) de justificativa id. 0049992803., conforme Art. 106 da Lei Federal nº 14

Esta Justificativa, como ressaltado pelo Professor Ulysses Jacoby, transcende a mera aceitação do preço imposto pelo contratado, demandando uma análise mercado, aferida por meio de métodos que assegurem a economicidade e a adequação aos parâmetros legais. Nesse contexto, a presente justificativa busca fornecer esclarecim dúvidas quanto à idoneidade e coerência do processo de contratação em questão, alinhando-se aos princípios basilares que regem as contratações públicas.

2. METODOLOGIA APLICADA

Assim, no presente processo será considerado a metodologia de ordem sub-sequencial constante no art. 23 da Lei Federal nº 14.133/2021, vejamos:

Art. 1º O valor previamente estimada da contratação deverá ser compatível com os valores praticados pelo mercado, considerados os preços constantes de banco observadas a potencial economia de escala e as peculiaridades do local de execução do objeto.

Parágrafo único. No processo licitatório para aquisição de bens e contratação de serviços em geral, conforme regulamento, o valor estimado será definido com b seguintes parâmetros, adotados de forma combinada ou não:

I - composição de custos unitários menores ou iguais à mediana do item correspondente no painel para consulta de preços ou no banco de preços em saúde di (PNCP);

II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusi índice de atualização de preços correspondente;

III - utilização de dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios elet contenham a data e hora de acesso;

IV - pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses forn com mais de 6 (seis) meses de antecedência da data de divulgação do edital;

V - pesquisa na base nacional de notas fiscais eletrônicas, na forma de regulamento.

Em análise ao Decreto Estadual nº 28.874/2024 que regulamenta licitações no âmbito do Governo do estado de Rondônia, percebe-se que a fonte preferencial a de preços, vejamos:

Art. 2º pesquisa de preços deverá ser realizada da forma mais ampla possível e de acordo com o regramento do art. 23, da Lei Federal n° 14.133, de 2021.

Parágrafo único. como fonte preferencial para elaboração de estimativa de valor de veículos oficiais de divulgação de valores referenciais, tais como bancos ou pa

Para definição do valor de referência, poderá ser aplicada a metodologia estatística prevista no art. 6º da **IN nº 01/2024/SUPEL-CPEAP**:

Mediana: quando o Coeficiente de Variação (CV) foi superior a 25,99%.

Média: quando o CV foi inferior a 25,99%.

Menor Preço: nos casos de mercado restrito, com poucos fornecedores ou único fabricante, conforme o **Acórdão nº 1850/2020 do TCU**.

Antes da escolha do método, os preços foram ordenados e submetidos à medida saneadora, com aplicação do **desvio padrão de 25%**, visando eliminar valores ex

(**outliers**).

I - Painel de Preços (SEI nº 68241097)

No processo em análise, a busca por parâmetros de definição de preço incluiu a verificação da existência de contratações comparáveis no painel de preços con encontrado resultado para o objeto em questão conforme consta no relatório (SEI nº 68241097) por problemas no site.

II - Banco de Preços (SEI nº 68241045)

Em análise ao banco de preços (68241045) foram localizados valores de balizamento para o Registro de Preços para contratação de empresa para fornecimento, e-mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades d período de 3 (três) anos, conforme descrito no Documento de Oficialização de Demanda - DOD (0054733868) de justificativa id. 0049992803., conforme Art. 106 da Lei Federal nº 14.

Em análise mais detalhada dos valores, verifica-se que o objeto dos contratos se assemelha ao pretendido na contratação, sendo possível assim a utili Preços.

III - Banco de Preços em saúde.

O dispositivo de Banco de Preços em Saúde disponível não se aplica a presente contratação, visto que a Contratação de empresa para fornecimento, sob dema Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da Secretar 3 (três) anos e o portal citado é com finalidade de registro de medicamentos e dispositivos médicos:

O Banco de Preços em Saúde - BPS é um sistema de registro de informações de compras públicas e privadas de medicamentos e dispositivos médicos que existe de informações de compras públicas e privadas de medicamentos e dispositivos médicos, a fim de subsidiar a compra pública mais eficiente no setor saúde, pelos entes federado

IV - Portal Nacional de Contratações Públicas (68241084).

No intuito de atender ao preceito normativo que preconiza a busca por contratações similares realizadas pela Administração Pública, em execução ou concluídas preços, inclusive mediante sistema de registro de preços, buscou-se diligentemente informações que pudessem subsidiar a análise e definição de preços para o presente processo.

Em busca pormenorizada de contratações similares, foram localizadas Contratação de empresa para fornecimento, sob demanda, de solução de segurança para avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da Secretaria de Estado da Saúde - SESAU/RO

V - Utilização de dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônic

Em conformidade com o disposto no Decreto Estadual nº 28.874/2024, que regulamenta as contratações públicas no âmbito do Governo do Estado de Rondônia, as fontes estabelecidas no referido normativo, buscando garantir a fidedignidade dos valores estimados e a seleção da proposta mais vantajosa à Administração.

No entanto, a utilização de dados provenientes de mídia especializada, tabelas de referência formalmente aprovadas pelo Poder Executivo Federal ou de sítios mostrou adequada para a presente estimativa, pelos seguintes motivos:

1. **Incompatibilidade técnica e especificações distintas** – As informações disponíveis nas referidas fontes não contemplam as especificações técnicas exatas d modelo, configuração ou características que poderiam comprometer a exatidão da estimativa.

2. **Desatualização ou ausência de dados regionais** – As tabelas e mídias consultadas não apresentam valores atualizados ou não refletem a realidade de mercado Rondônia, podendo gerar distorções na formação do preço estimado.

3. **Falta de representatividade comercial** – As mídias e sítios eletrônicos consultados não possuem abrangência suficiente para retratar as condições comerciais localidade, o que inviabiliza a adoção de seus valores como base comparativa.

4. **Predominância de fontes mais aderentes** – Optou-se por adotar, de forma fundamentada, outras fontes de pesquisa de preços mais adequadas e fidedignas, t atas de registro de preços vigentes ou contratações recentes realizadas por órgãos públicos, que demonstraram maior conformidade com o objeto e com o mercado local.

Dessa forma, a não utilização das referidas fontes se justifica pela necessidade de assegurar a precisão e a confiabilidade da estimativa de preços, em observância eficiência previstos no Decreto Estadual nº 28.874/2024 e na Lei Federal nº 14.133/2021.

VI - Pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornec com mais de 6 (seis) meses de antecedência da data de divulgação do edital.

A utilização de pesquisa direta com fornecedores locais deve ser observada com cautela pela Administração Pública durante a elaboração da estimativa, de fo realidade do mercado. A Instrução Normativa/SEGES-ME nº 65 de 07 de julho de 2021 estabeleceu que a Lei 14.133/2021 dispõe que os cinco parâmetros citados podem ser **deverão ser priorizados os dois primeiros parâmetros, ou seja, o módulo integrado para pesquisa de preços no sistema Compras.gov.br; e as contratações similares** devem ser utilizadas de forma complementar ou subsidiária, com as devidas justificativas, **devendo ser evitada a cotação somente junto a potenciais fornecedores,** vejamos:

Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição de bens e contratação de serviços em g parâmetros, empregados de forma combinada ou não:

I - composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou banco de preços correspondente;

II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusi índice de atualização de preços correspondente;

III - dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos esp no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso;

IV - pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; ou

V - pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data de Logística, elaborado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.

§ 1º Deverão ser priorizados os parâmetros estabelecidos nos incisos I e II, devendo, em caso de impossibilidade, apresentar justificativa nos autos. (grif

O Decreto Estadual nº 28.874/2024, através do art. 51 regulamentou as formas de pesquisa de preços previstas no art. 23 da Lei Federal nº 14.133/2021, e definiu veículos oficiais, tais como bancos ou painéis de preços, bem como ainda exigindo a justificativa quando a pesquisa realizada somente por meio de pesquisa de mercado:

Art. 51.A pesquisa de preços deverá ser realizada da forma mais ampla possível e de acordo com o regramento do art. 23, da Lei Federal n° 14.133, de 2021.

§ 1°Adotar-se-á como fonte preferencial para elaboração de estimativa de valor de veículos oficiais de divulgação de valores referenciais, tais como bancos ou pa

§ 2°A realização de estimativa de valor exclusivamente por meio de pesquisa de mercado somente será admitida em caso de expressa justificativa do setor respon das propostas com a correspondente justificativa de escolha dos agentes econômicos pesquisados.

O Tribunal de Contas da União através do Acórdão nº 1.875/2021-Plenário já definiu que os valores deverão ser baseados em cestas de preços, sendo preferencial somente utilizado pesquisa junto a fornecedores em caso de ausência extrema de preços públicos, vejamos:

9.5.1. as pesquisas de preços para estimativa de valor de objetos a serem licitados devem ser baseadas em uma “cesta de preços”, devendo dar preferência para pr

9.5.2. a pesquisa de preços feita exclusivamente junto a fornecedores deve ser utilizada em último caso, **na extrema ausência de preços públicos ou cestas de p**

Diante disso, percebe-se que não existiu necessidade no processo a realização de pesquisa com fornecedores locais, considerando a existência de preç preços e estimativa necessária.

3. SÉRIE DE PREÇOS COLETADOS (art. 3º, inc. IV)

ITEM	ESPECIFICAÇÃO	UNIDADE	QUANTIDADE	EMPRESA ITPROTECT	PNCP 1	PNCP 2	BANCO DE PREÇOS 1	BANCO DE PREÇOS 2	BANCO DE PREÇOS 3	MENOR VALOR	VALOR MEDIANO	VALOR MÉDIA	I
01	Solução de proteção de Endpoints com abordagem proativa para resposta eficaz a incidentes	Por Endpoint	2150	R$ 483,21	R$ 539,25	R$ 832,55	R$ 800,00	R$ 693,10	N/C	R$ 483,21	R$ 693,10	**R$ 669,62**	I
02	Solução de proteção de Servidores com abordagem proativa para resposta eficaz a incidentes	Por Servidor	139	R$ 4.390,00	R$ 4.200,00	R$ 5.037,50	R$ 4.200,00	R$ 5.000,00	R$ 5.700,00	R$ 4.200,00	R$ 4.695,00	**R$ 4.754,58**	I
03	Solução de segurança avançada para mitigação de ameaças na rede	Por Throughput de dados	2	R$ 3.600.000,00	R$ 3.996.162,02	R$ 4.295.547,05	R$ 3.295.000,00	R$ 3.901.534,00	R$ 3.640.000,00	R$ 3.295.000,00	R$ 3.770.767,00	**R$ 3.778.040,51**	3
04	Solução de prevenção de intrusão de próxima geração (NGIPS)	Por Throughput de dados	4	R$ 2.025.000,00	R$ 2.648.300,11	R$ 2.849.774,40	R$ 2.648.300,11	R$ 1.750.000,00	R$ 2.846.016,00	R$ 1.750.000,00	R$ 2.648.300,11	**R$ 2.461.231,77**	4
05	Serviço de suporte pro ativo, corretivo e para resposta a incidentes	Por Solução	4	R$ 401.500,00	R$ 582.000,00	R$ 430.000,00	R$ 581.790,63	R$ 430.000,00	R$ 450.000,00	R$ 401.500,00	R$ 440.000,00	**R$ 479.215,11**	8
06	Serviço de implantação	Por Solução	4	R$ 45.000,00	R$ 39.088,92	R$ 35.000,00	R$ 36.000,00	R$ 32.575,00	R$ 35.000,00	R$ 32.575,00	R$ 35.500,00	**R$ 37.110,65**	
07	Serviço de capacitação e repasse de conhecimento	40 Horas	2	R$ 35.000,00	R$ 42.500,00	R$ 30.000,00	R$ 42.500,00	R$ 30.000,00	R$ 40.200,00	R$ 30.000,00	R$ 37.600,00	**R$ 36.700,00**	

VALOR ESTIMADO ANUAL DA CONTRATAÇÃO R$ 21.660.280,76 (vinte e um milhões seiscentos e sessenta mil duzentos e oitenta reais e setenta e s

4. DA ANÁLISE DOS VALORES OBTIDOS E DEFINIÇÃO DE VALOR DE REFERÊNCIA

Diante do exposto, considerando que o Decreto Estadual nº 28.874/24 define em seu Art. 53:

Art. 3º resultado da pesquisa de preços será a **média, mediana ou o menor dos preços obtidos**, observados os seguintes parâmetros:

I - para a obtenção do resultado da pesquisa de preços, deverá ser realizada análise crítica dos preços pesquisados, a fim de verificar eventuais propostas excessivamente elevados e, ainda, verificar a similaridade com o objeto, especificações, qualidade, prazos e garantias definidos pela Administração;

II - o responsável deverá fazer um balizamento entre o resultado obtido e os preços praticados no âmbito dos órgãos e entidades da Administração Pública, atrav Registro de Preços e outros meios para verificar se o resultado apresenta o preço praticado no mercado.

Sugere-se no presente processo, a utilização do critério média de preço para a definição do Registro de Preços para contratação de empresa para fornecimento, sol mail, Endpoint e proteção contra ataques avançados, incluindo instalação, configuração, repasse de conhecimento, suporte técnico e garantia, para atender às necessidades da período de 3 (três) anos. , conforme descrito no Documento de Oficialização de Demanda - DOD (0054733868) de justificativa id. 0049992803., conforme Art. 106 da Lei Federal nº 14

Os documentos que deram suporte para justificar o tratamento dado aos preços coletados, bem como a metodologia que foi aplicada encontram-se anexos aos a Nacional de Contratações Públicas (68241084), Banco de Preços (68241045), Painel de Preços Negativo (68241097) e **Orçamento da Empresa ITPROTECT (68238823)**, o órgãos e entidades da Administração Pública.

5. CONCLUSÃO

Em conclusão, ratificamos que a pesquisa de preços realizada para embasar o presente certame seguiu criteriosamente os preceitos estabelecidos na legislaçã Decreto Estadual nº 28.874/2024 foi cuidadosamente cumprido e obtido preço através de ampla cesta de preços utilizada para estimativa do valor do plantão e definiçã administração na busca por referências adequadas para a definição dos valores estimados.

Visto isso e considerando o caso concreto, diante da conformidade com os dispositivos legais e da adequada justificação dos parâmetros utilizados, o presente pı conduzir uma pesquisa de preços idônea e alinhada aos princípios da Administração Pública, assegurando, dessa forma, a lisura e a legalidade do procedimento de contratação, tendo o processo o valor estimado de **R$ 21.660.280,76 (vinte e um milhões seiscentos e sessenta mil duzentos e oitenta reais e setenta e seis centavos).**

MARCOS EDUARDO IGNÁCIO REGO
NÚCLEO DE PROCEDIMENTOS ACESSÓRIOS - SESAU-NPA

JUNIOR SANTANA DE ARAUJO
CHEFE DE NÚCLEO - SESAU/NPA

SESAU RO GOV

Documento assinado eletronicamente por **Junior Santana de Araujo**, **Chefe de Núcleo**, em 15/01/2026, às 11:27, 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 **Marcos Eduardo Ignacio Rego**, **Assessor(a)**, em 15/01/2026, às 11:48, 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 **68244109** e o código CRC **AF01FF54**.

Referência: Caso responda este(a) Relatório, indicar expressamente o Processo nº 0036.028242/2024-36 SEI nº 68244109