TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO

DOD - Documento de Oficialização da Demanda

Despesa prevista no PCA

1. Unidade Demandante

Seção de Gestão de Redes e Comunicação - SERCO

1.1 Titular da Unidade Demandante

Nome do Servidor	Matrícula	Telefone	E-mail
Ana Luiza Maia Soares de Azevedo	289	9221	ana.azevedo@tre-pe.jus.br

2. Detalhamento da Demanda

2.1 Exercício do PCA

PCA2025

2.2 Descrição Sucinta da Demanda

Aquisição de switches gerenciáveis com licença de suporte 24x7 e garantia de hardware e aquisição de transceiver.

2.3 Itens, Quantidades e Valores Previstos do PCA

Aquisições						
Nº Item	Descrição do Item	Grupo de Natureza da Despesa (GND)	Elemento de Despesa	CATMAT	Quantidade	Unidade de Medida

01	**Switch com 48 portas 1000Base-T,** 4 slots SFP para conexão de fibras ópticas operando em 10GbE. Alimentação 110/220V. Com licença de suporte 24x7 e garantia de hardware.	4	52	618775	16	un
02	**Switch Poe com 48 portas 1000Base-T,** 4 slots SFP para conexão de fibras ópticas operando em 10GbE. Alimentação 110/220V. Com licença de suporte 24x7 e garantia de hardware.	4	52	618779	7	un
03	Transceiver - Transceiver, tipo: conversor de mídia, aplicação: redes de dados, características adicionais: SFP LC LX Tipo: cabeamento ótico com conector LC, aplicação: conexão 10G BASE-SR, caracterísiticas adicionais: CONEXÃO SFP+, FULL DUPLEX	4	52	295671	50	un

Valor Total da Demanda Previsto no PCA	R$ 313.200,00

2.4 Alinhamento Estratégico

Objetivo do Planejamento Estratégico Institucional (PEI) do TRE-PE:	Nº 12 (Aprimorar a estratégia de tecnologia da informação e comunicação e proteção de dados)
Objetivo do Plano Setorial da Unidade Gestora:	Nº 01 (Aumentar a satisfação dos usuários do sistema judiciário) Nº 08 (Promover serviços de infraestrutura e soluções corporativas)
Sequencial no Plano de Contratações Anual, se houver:	Sequencial 36 do PCA2025

3. Motivação da Demanda

A presente contratação objetiva a substituição dos switches obsoletos existentes no Data Center backup e no prédio da Rui Barbosa.

Equipamentos obsoletos, ou seja, sem garantia e, consequentemente sem atualização de "firmware", tornam-se vulneráveis e

podem causar risco no que se refere à segurança de TIC.

Além disso, alguns componentes de tais equipamentos têm apresentado falhas no seu funcionamento, o que prejudica o acesso aos serviços de rede por parte dos usuários.

4. Resultados Pretendidos

A presente aquisição possibilitará:

- Correto funcionamento de conectividade da rede local;
- Suporte técnico 24 x 7 e garantia de hardware e firmaware;
- Garantia da segurança no acesso à rede.

5. Indicação de Integrante Demandante

Nome do Servidor	Matrícula	Telefone	E-mail
Ana Luiza Maia Soares de Azevedo	289	9221	ana.azevedo@tre-pe.jus.br

6. Anexos

Não há Anexos.

7. Aprovação e Assinaturas

Obs.: Devem assinar este documento o integrante demandante, o titular (chefia imediata) e o gestor tático da unidade demandante.

Documento assinado eletronicamente por **ANA LUIZA MAIA SOARES DE AZEVEDO**, **Chefe de Seção**, em 08/11/2024, às 09:21, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **JOSÉ FERREIRA DE LIMA JÚNIOR**, **Coordenador(a)**, em 08/11/2024, às 12:08, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-pe.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2771073** e o código CRC **0726297B**.

TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO

Estudos Técnicos Preliminares

Contratação de TIC

1. Análise de Viabilidade da Contratação

1.1. Descrição Sucinta do Objeto

Aquisição de switches gerenciáveis de 48 portas, com serviços de suporte 24x5 e garantia de hardware, e aquisição de transceiver.

1.2. Unidade Demandante

Nome da Unidade Demandante	Sigla da Unidade Demandante
Seção de Gestão de Redes e Comunicação	SERCO

1.3. Referência ao DOD e ao Termo de Ciência da Equipe de Planejamento

Documento de Oficialização da Demanda	2771073
Termo de Ciência da Equipe de Planejamento	2866804

1.4. Necessidades e Requisitos do Objeto

A presente contratação objetiva a substituição dos switches obsoletos existentes no Data Center backup e no prédio da Rui Barbosa.

Equipamentos obsoletos, ou seja, sem garantia e, consequentemente sem atualização de "firmware", tornam-se vulneráveis e podem causar risco no que se refere à segurança de TIC.

Além disso, alguns componentes de tais equipamentos têm apresentado falhas no seu funcionamento, o que prejudica o acesso aos serviços de rede por parte dos usuários.

A necessidade dos transceivers é de extrema importância para a conexão dos novos swtiches. Os equipamentos atuais, que serão substituídos, são conectados por duas maneiras: a) O 6509 é composto de 7 placas cada, conectados internamente via barramento; b) O 3750 e os SG350 são conectados via cabo DAC. Os novos swtiches a serem adquiridos não são conectados por essas tecnologias.

Requisitos de negócio:

Item 01 - Switch de acesso com 48 portas

- Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
- Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);
- Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;
- Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W em 24 portas;
- Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
- Deve possuir 1 (uma) interface USB.

Item 02 - Transceiver SFP+ 10GBase-SR

- Transceiver SFP+ para conexão de fibras ópticas multimodo;
- Deve ser compatível com o padrão 10GBase-SR para fibras ópticas de até 300m;
- Deve ter velocidade de 10GbE;
- Deve ser do mesmo fabricante e compatível com os firewalls, switches concentrador e de acesso que estão sendo demandados nesta contratação.

Os itens 01 e 02 constantes do DOD foram consolidados em apenas um item, o item 01 deste ETP, considerando o requisito de negócio indicado acima: "Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W em 24 portas", onde 24 portas do switch são Poe e 24 não Poe, o que atende a demanda do TRE-PE.

Requisitos de Garantia e Suporte Técnico:

- Acesso ao suporte técnico no regime 24 x 5;
- Garantia de hardware e firmware pelo período de 60 (sessenta) meses.

Requisitos legais:

- Lei nº 14.133, de 1º de abril de 2021, que instituiu normas para licitações e contratos da Administração Pública;
- Resolução CNJ nº 468, de 15 de julho de 2022, que dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação, pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça;
- Instrução Normativa SEGES/ME n.° 65, de 7 de julho de 2021, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral de acordo com a Lei nº 14.133/2021;
- Resolução TRE-PE nº 433, de 29 de novembro de 2022, que dispõe sobre o macroprocesso de contratações do Tribunal Regional Eleitoral de Pernambuco;
- Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a Lei Geral de Proteção de Dados Pessoais (LGPD);
- Decreto nº 11.462, de 31 de março de 2023, que dispõe sobre o registro de preços para a contratação de bens e serviços.

Requisitos de segurança:

- A empresa contratada deve assinar termo de confidencialidade através de seu representante legal em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, abrangendo todos os seus colaboradores e terceiros.
- Caso seja necessária a presença de técnico da empresa nas dependências do TRE-PE para execução de serviços, estes devem ser previamente autorizados e portar crachá de identificação com nome, cargo e nome da empresa;
- Caso o fornecedor tome conhecimento ou possua suspeita da ocorrência de um evento ou incidente envolvendo informações ou ativos de informação do TRE-PE, deverá comunicar imediatamente à área de Segurança da Informação e manter a área gestora do contrato informada.
- Quando logs forem tramitados entre o CONTRATANTE, a CONTRATADA e o fabricante, logo após seu uso, os mesmos deverão ser eliminados e não poderão ser utilizados para outros fins;
- Em casos de manutenção solicitada pelo CONTRATANTE, as informações tramitadas deverão transitar de forma segura, utilizando, sempre que possível, mecanismos de criptografia;
- A contratada não deverá utilizar indevidamente os dados da contratante fora do escopo do projeto.

1.5. Benefícios Esperados

A presente aquisição possibilitará:

- Correto funcionamento de conectividade da rede local;
- Diminuição de falhas no acesso à rede pelos usuários;
- Aumento da segurança no acesso à rede.

1.6. Quantidade a ser Contratada e Justificativa

A presente aquisição objetiva a substituição dos switches obsoletos existentes no Data Center backup e no prédio da Rui Barbosa. Os novos switches a serem adquiridos precisam ser conectados por equipamentos específicos, por isso torna-se necessária, também, a aquisição de transceivers. As quantidades correspondem ao que é necessário para a instalação dos novos switches que substituirão os obsoletos.

Assim será necessária a aquisição de:

Item	Descrição do Item	Quantidade
1	**Switch com 48 portas 1000Base-T,** 4 slots SFP para conexão de fibras ópticas operando em 10GbE. Alimentação 110/220V. Com garantia e serviços de suporte e manutenção 24 x 5 (vinte e quatro horas de segunda a sexta-feira), pelo período de 60 (sessenta) meses.	28
2	**Transceiver SFP+ 10GBase-SR**	20

1.7. Correlação ou Interdependência com outra Contratação do Órgão

No momento, não há correlação com outra contratação do TRE-PE.

1.8. Alinhamento Estratégico

Objetivo(s) Estratégico(s) do Planejamento Estratégico Institucional (PEI) do TRE-PE:	Nº 12 (Aprimorar a estratégia de tecnologia da informação e comunicação e proteção de dados)
Objetivo(s) Estratégico(s) do Plano Diretor de TIC (PDTIC) do TRE-PE:	Nº 01 (Aumentar a satisfação dos usuários do sistema judiciário) Nº 08 (Promover serviços de infraestrutura e soluções corporativas)
Sequencial no Plano de Contratações Anual:	Sequencial 36 do PCA 2025

1.9. Soluções Existentes no Mercado

1.9.1. Soluções Encontradas

O acesso à rede de acesso do TRE-PE pode ser provido através de cabeamento estruturado, em que há necessidade de switches gerenciáveis, ou através da rede sem fio (Wi-Fi).

Id	Descrição das Soluções ou Cenários Possíveis
1	Rede de acesso através de switches gerenciáveis
2	Rede de acesso através de rede sem fio

1.9.2. Quadro Comparativo de Soluções

Requisito	Solução	Sim	Não	Observação
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	Não se aplica, pois não se trata de solução de software.
	Solução 2		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	Não se aplica, pois não se trata de solução de software.
	Solução 2		X	
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1		X	Não se aplica, pois não se trata de solução de software.
	Solução 2		X	
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1		X	Não se aplica, pois não envolve certificação digital.
	Solução 2		X	
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1		X	Não se aplica, pois não se refere a solução arquivística.
	Solução 2		X	

1.10. Descrição e Justificativa da Solução Escolhida

Atualmente, na infraestrutura do TRE-PE, a rede de acesso para os computadores, telefones IP, pontos de acesso e câmeras de monitoramento, é realizada majoritariamente através de cabeamento estruturado fornecido por switches de acesso.

O TRE-PE possui apenas 24 pontos de acesso para a rede sem fio (Wi-Fi), distribuídos no prédio Sede e Anexo da Rui Barbosa, representando um percentual muito baixo comparado ao acesso cabeado.

Para o item 1, portanto, este estudo visa a manutenção da rede de acesso local, com a aquisição do mesmo quantitativo de switches existentes no Data Center backup e no prédio da Rui Barbosa, em substituição aos que estão obsoletos.

O item 2, referente aos transceivers, faz-se necessário para a conexão entre os switches, permitindo o gerenciamento dos equipamentos de forma centralizada.

1.11. Adequações Necessárias

Recursos Humanos, incluindo necessidades de capacitação	Não há necessidade de capacitação dos servidores envolvidos com a presente contratação, pois o objeto é de uso comum e de conhecimento dessa equipe. Além disso, não haverá necessidade de fornecer capacitação quanto aos procedimentos relativos à gestão e fiscalização contratuais.
Infraestrutura Tecnológica	Não se aplica.
Infraestrutura Elétrica	Não se aplica.
Espaço Físico	Não se aplica.
Mobiliário	Não se aplica.
Outros	Não se aplica.

1.12. Classificação dos Itens da Solução

Nº Item	Descrição do Item	Grupo de Natureza da Despesa (GND)	Elemento de Despesa	CATMAT
1	**Switch com 48 portas 1000Base-T,** 4 slots SFP para conexão de fibras ópticas operando em 10GbE. Alimentação 110/220V. Com garantia e serviços de suporte e manutenção 24 x 5 (vinte e quatro horas de segunda a sexta-feira), pelo período de 60 (sessenta) meses.	4	52	618780
2	**Transceiver SFP+ 10GBase-SR**	3	30	624360

1.13. Pesquisa de Preços de Mercado

1.13.1. Servidor Responsável pela Pesquisa de Preços

Nome do Servidor	Lotação do Servidor
Ana Luiza Maia Soares de Azevedo	SERCO

1.13.2. Extrato das Pesquisas Realizadas

Empresa	Fonte*	É ME/EPP?	UF	Trabalha com Adm. Pública?	Data do documento**	Referência no Proc. SEI
Copwire Informática Ltda.	Contratação similar	Não	SC	Sim	16/07/2024	ARP 17/2024 do TRT 5ª Região (2868868)
P. Cheles Comércio e Serviços Ltda.	Contratação similar	Não	SP	Sim	17/12/2024	ARP 359/2024 do UFBA (2868871)
YSSY Soluções S.A	Contratação similar	Não	SP	Sim	30/12/2024	Contrato 48/2024 do STM (2868874)
Teltec Networks Ltda.	Contratação similar	Não	SC	Sim	24/05/2024	Contrato 51/2024 do TJ-MA (2868877)
LETTEL Distribuidora de Telefonia Ltda.	Contratação similar	Não	SC	Sim	30/12/2024	Contrato 95/2024 do TSE (2868879)
2R Datatel Telefinformática Ltda.	Contratação similar	Não	RJ	Sim	01/10/2024	ARP 90014/2024 do Arquivo Nacional (2868880)

CLM Software Comércio e Importação e Exportação Ltda.	Contratação similar	Não	SP	Sim	24/10/2024	Contrato 67/2024 do TCE-PI (2868883)
LETTEL Distribuidora de Telefonia Ltda.	Contratação similar	Não	SC	Sim	04/04/2024	Contrato 20/2024 do TCU (2868885)

1.13.3. Análise das Pesquisas Realizadas

Inicialmente, foi verificado se o objeto da contratação constava no Catálogo de Soluções de TIC com Condições Padronizadas da SGD ou no Catálogo Eletrônico de Padronização do Governo Federal, porém não foi encontrada nessas plataformas nenhuma solução para atendimento ao objeto.

Foi realizada consulta às empresas Arpsist, SEGER e 1Telecom (docs. 2872364, 2872365 e 2872368), mas nenhuma apresentou proposta até a presente data. Estas empresas foram consultadas por já terem celebrado contratos com este TRE-PE e com outros TRE's.

Foi realizada consulta no Sistema Comprasnet Contratos e no Painel de Preços, e seus preços foram considerados para composição do preço médio estimado.

Os contratos relacionados no tópico anterior constam anexados ao presente processo.

1.13.4. Cálculo do Preço Estimado

1.13.4.1. Detalhamento do Cálculo do Preço

SWITCH 48 PORTAS GERENCIÁVEL						
PREÇOS		**Desvio Padrão**	**Coeficiente de Variação (desvio padrão/média)**	**Média**	**Mediana**	**Método a ser Utilizado**
TRT5 (item 3)	25.300,00	5.799,87	19%	**30.242,00**	28.000,00	Média, em razão do valor do coeficiente de variação ser inferior ou igual a 25%
UFBA	25.094,00					
STM (item 4)	35.276,00					
TJ-MA (item 2)	28.000,00					
TSE (item 5)	37.540,00					
TRANSCEIVER						
PREÇOS		**Desvio Padrão**	**Coeficiente de Variação (desvio padrão/média)**	**Média**	**Mediana**	**Método a ser Utilizado**
Arquivo Nacional (item 4)	4.200,00	1.133,62	48%	2.341,40	**2.050,00**	Mediana, em razão do valor do coeficiente de variação ser superior a 25%
TCE-PI (item 3)	2.050,00					
TCU (item 10)	1.157,00					
TRT5 (item 9)	1.900,00					
TJ-MA (item 09)	2.400,00					

1.13.4.2. Valor Estimado Obtido

Da análise dos preços médios calculados com base nas pesquisas de mercado realizadas (tópico acima), verifica-se que os preços constantes da proposta vencedora do Pregão Eletrônico nº 90001/2025 do TRE-AP (doc. 2869230), do qual o TRE-PE é participante da IRP, mostram-se vantajosos para a presente contratação.

O processo licitatório do Pregão Eletrônico nº 90001/2025 do TRE-AP foi homologado no dia 21/02/2025, conforme Termo de Homologação (2872332).

Considerando, então, os valores indicados no Pregão nº 90001/2025 do TRE-AP, tem-se que o valor total estimado da contratação corresponde ao detalhado abaixo:

Nº e Descrição do Item	Valor Unitário Estimado	Quantidade	Valor Total Estimado
Switch com 48 portas 1000Base-T, 4 slots SFP para conexão de fibras ópticas operando em 10GbE. Alimentação 110/220V. Com garantia e serviços de suporte e manutenção 24 x 5 (vinte e quatro horas de segunda a sexta-feira), pelo período de 60 (sessenta) meses. (Item 6)	R$ 19.468,13	28	R$ 545.107,64

Transceiver SFP+ 10GBase-SR (Item 10)	R$ 888,16	20	R$ 17.763,20
Valor Total Estimado da Contratação			R$ 562.870,84

O valor previsto no PCA 2025 é de R$ 313.200,00. Assim, será solicitado o acréscimo de valor quando for finalizada à Ata de Registro de Preços daquele órgão.

1.13.4.3. Metodologia Utilizada para Definição do Preço Estimado e Justificativa

Com o objetivo de verificar o preço médio do mercado para os dois itens desta contratação, foram consideradas as orientações dispostas na IN ME nº 73/2020 para a pesquisa dos preços dos itens, e a metodologia orientada pelo Manual de Pesquisa de Preços do STJ para análise quanto à exequibilidade dos valores obtidos e cálculo dos valores estimados.

Considerando que todos os preços coletados na pesquisa foram originados de contratações similares, todos foram mantidos para cálculo do valor médio de mercado para o objeto.

Os procedimentos relacionados a essa análise constam no tópico 1.13.4.1 deste ETP.

O resultado foi usado para comparar com os valores estimados no Pregão Eletrônico nº 90001/2025 do TRE-AP (doc. 2869230), do qual o TRE-PE é participante da IRP.

1.14. Aplicabilidade do Objeto para ME e EPP

Não se aplica, visto se tratar de participação do Pregão Eletrônico nº 90001/2025 do TRE-AP.

1.15. Posicionamento Conclusivo sobre a Viabilidade da Contratação

A equipe de planejamento opina pela viabilidade da contratação.

A contratação é essencial, em razão da necessidade de substituição dos switches obsoletos existentes no Data Center backup e no prédio da Rui Barbosa, gerando risco à segurança de TIC.

Ante a vantajosidade econômica demonstrada no tópico 1.13.4.2, esta Equipe de Planejamento opina pela contratação dos itens através da participação do Pregão Eletrônico nº 90001/2025 do TRE-AP.

2. Sustentação do Contrato

2.1. Recursos Materiais e Humanos

Não haverá necessidade de treinamento para a equipe de gestão da contratação.

2.2. Impacto Ambiental

Não haverá impacto ambiental. Os equipamentos substituídos serão enviados à Comissão de Bens Inservíveis para desfazimento.

2.3. Sustentabilidade

2.3.1. Critérios Sociais

Não se aplica a indicação neste ETP, por se tratar de participação do Pregão Eletrônico nº 90001/2025 do TRE-AP. Tais critérios, caso exigidos, foram definidos e solicitados quando do procedimento licitatório daquele órgão.

2.3.2. Critérios Ambientais

Não se aplica a indicação neste ETP, por se tratar de participação do Pregão Eletrônico nº 90001/2025 do TRE-AP. Tais critérios, caso exigidos, foram definidos e solicitados quando do procedimento licitatório daquele órgão.

2.3.3. Critérios Culturais

Não se aplica a indicação neste ETP, por se tratar de participação do Pregão Eletrônico nº 90001/2025 do TRE-AP. Tais critérios, caso exigidos, foram definidos e solicitados quando do procedimento licitatório daquele órgão.

2.3.4. Critérios de Acessibilidade

Não se aplica a indicação neste ETP, por se tratar de participação do Pregão Eletrônico nº 90001/2025 do TRE-AP. Tais critérios, caso exigidos, foram definidos e solicitados quando do procedimento licitatório daquele órgão.

2.3.5. Critérios de Saúde

Não se aplica a indicação neste ETP, por se tratar de participação do Pregão Eletrônico nº 90001/2025 do TRE-AP. Tais critérios, caso exigidos, foram definidos e solicitados quando do procedimento licitatório daquele órgão.

2.4. Descontinuidade do Fornecimento

Não sendo possível a realização da contratação, a rede de acesso local da Sede e do prédio Anexo da Rui Barbosa fica vulnerável a uma paralisação da comunicação por problema/defeito em um dos equipamentos que serão substituídos. Como ação para minimizar o impacto, poderão ser utilizados 2 switches reserva (48 portas cada um), porém insuficientes para atender a capacidade de apenas um switch CISCO 6509, que possui 240 portas.

2.5. Transição Contratual

Os equipamentos serão substituídos fora do horário do expediente do TRE-PE, de forma a não ocorrer a minimizar o transtorno causado pela paralisação na comunicação dos computadores, telefones IP, pontos de acesso e câmeras de viedomonitoramento durante a troca dos equipamentos.

3. Estratégia para a Contratação

3.1. Natureza do Objeto

O objeto da presente contratação possui características comuns e usuais encontradas no mercado, cujos padrões de desempenho e de qualidade podem ser definidos.

3.2. Modalidade da Contratação

Adesão à Ata de Registro de Preços (ARP) de outro órgão federal	
Contratação Direta – Dispensa de Licitação	
Contratação Direta – Inexigibilidade	
Pregão Eletrônico	
Pregão Eletrônico pelo Sistema de Registro de Preços (órgão participante)	
Pregão Presencial	
Termo de Cooperação, Convênio ou documentos afins	
Prorrogação Contratual	
Outras *(descrever a modalidade)*	Aquisição por meio de ARP do TRE-AP - a ser gerada após a conclusão do Pregão Eletrônico nº 90001/2025 do referido Tribunal, onde o TRE-PE é órgão participante.

3.3. Justificativa para a Modalidade de Contratação Escolhida

A equipe de planejamento da contratação opina pela contratação dos itens do Pregão Eletrônico nº 90001/2025 do TRE-AP (Edital doc. 2869219), onde o TRE-PE é órgão participante, em razão do preço ser vantajoso quando comparado ao preço de mercado, conforme evidenciado nos itens 1.13.4.1 e 1.13.4.2 deste Estudo Preliminar.

3.4. Período de Execução e Vigência do Contrato

Conforme previsto no Termo de Referência anexo ao Edital do TRE-AP - doc. nº 2869219 - a vigência da contratação será por 60 (sessenta) meses contados a partir da assinatura do contrato, prorrogáveis, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021, e sua eficácia está condicionada à divulgação no Portal Nacional de Contratações Públicas (PNCP), na forma do art. 94 da Lei nº 14.133, de 2021.

3.5. Parcelamento e Adjudicação do Objeto

Não se aplica, por se tratar de participação do Pregão Eletrônico nº 90001/2025 do TRE-AP.

3.6. Formalização da Contratação

A formalização da contratação será por contrato administrativo firmado entre as partes.

3.7. Equipe de Apoio à Contratação

Nome	E-mail	Lotação	Telefone
Ana Luiza Maia Soares de Azevedo	ana.azevedo@tre-pe.jus.br	SERCO	9221
Josias Santiago Barbosa Filho	josias.santiago@tre-pe.jus.br	SERCO	9319
Robson André Costa Lopes	robson.lopes@tre-pe.jus.br	SECOM	9338

3.8. Equipe de Gestão da Contratação

Função	Nome	E-mail	Lotação	Telefone
Gestor da Contratação	Ana Luiza Maia Soares de Azevedo	ana.azevedo@tre-pe.jus.br	SERCO	9221
Gestor substituto	Diego Wesley de Carvalho Spíndola	diego.spindola@tre-pe.jus.br	SERCO	9322
Fiscal Técnico	Josias Santiago Barbosa Filho	josias.santiago@tre-pe.jus.br	SERCO	9319
Fiscal Administrativo	Robson André Costa Lopes	robson.lopes@tre-pe.jus.br	SECOM	9338
Fiscal Demandante	Josias Santiago Barbosa Filho	josias.santiago@tre-pe.jus.br	SERCO	9319

Os papéis de fiscal técnico e demandante serão acumulados pelo mesmo servidor, em razão de ser lotado na Seção demandante, que também é a unidade que possui o domínio técnico para acompanhar o objeto a ser contratado.

4. Análise de Riscos

4.1. Riscos Relacionados ao Processo da Contratação

Descrição do Risco	Descrição do Dano	Probabilidade	Impacto	Criticidade	Ação de Controle ou Contingência	Prazo	Responsável
Não contratação para aquisição dos switches e transceivers	• Risco de paralisação em caso de defeito no equipamento atualmente em funcionamento • Impossibilidade de atualização do firmware dos equipamentos atualmente em funcionamento	1	3	3	Contratação direta emergencial	Até 30/04/2025	SERCO

Atraso no trâmite para a formalização do contrato	• Risco de paralisação em caso de defeito no equipamento atualmente em funcionamento • Impossibilidade de atualização do firmware dos equipamentos atualmente em funcionamento	1	3	3	Celeridade no trâmite pelas unidades envolvidas	Até 30/04/2025	DG/ASJUR/CEC/SERCO/COSINF/STIC
Atraso na entrega do serviço contratado	• Risco de paralisação em caso de defeito no equipamento atualmente em funcionamento • Impossibilidade de atualização do firmware dos equipamentos atualmente em funcionamento	1	2	2	Aplicação de penalidades/glosas previstas no contrato	Até 30/06/2025	Gestor contratual

4.2. Riscos Relacionados à Segurança da Informação

Descrição do Risco	Descrição do Dano	Probabilidade	Impacto	Criticidade	Ação de Controle ou Contingência	Prazo	Responsável
Incidente de segurança da informação	Vazamento de dados confidenciais que possibilitem a exploração de vulnerabilidades nos ativos da instituição em razão de incidente de segurança da informação no fornecedor de serviços.	1	3	3	Comunicar imediatamente à área de Segurança da Informação e manter a área gestora do contrato informada.	Imediato ao ter a informação da ocorrência de incidente	CONTRATADO
Indisponibilidade dos serviços	Indisponibilidade de acesso à rede de dados local, em razão de defeito nos equipamentos atualmente em funcionamento	2	3	6	Ampliação da comunicação dos equipamentos em funcionamento através da rede sem fio.	Imediato	SERCO/COSINF

5. Informações Complementares

Conforme previsão contida no § 2.º do art. 18 da Lei n.º 14.133/2021, acerca da necessidade de justificativas quanto a não utilização dos elementos não obrigatórios, informamos que todos os itens previstos no § 1.º do art. 18 da Lei n.º 14.133/2021, obrigatórios ou não, estão contemplados neste ETP.

6. Anexos

Edital do Pregão Eletrônico nº 90001/2025 do TRE-AP (2869219).

7. Assinaturas

Obs.: Todos os integrantes da equipe de planejamento da contratação devem assinar este documento.

Documento assinado eletronicamente por **ROBSON ANDRÉ COSTA LOPES**, **Técnico(a) Judiciário(a)**, em 25/02/2025, às 08:09, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ANA LUIZA MAIA SOARES DE AZEVEDO**, **Chefe de Seção**, em 25/02/2025, às 08:31, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **JOSIAS SANTIAGO BARBOSA FILHO**, **Técnico(a) Judiciário(a)**, em 25/02/2025, às 09:04, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.tre-pe.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **2866820** e o código CRC **312CFBE5**.

14 DAS DISPOSIÇÕES GERAIS

14.1 É vedada a 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 (artigo 82, inciso VIII da Lei 14.133/2021).

14.2 Será divulgada ata da sessão pública no sistema eletrônico.

14.3 Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário, pelo Pregoeiro.

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

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

14.6 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.

14.7 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.

14.8 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.

14.9 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.

14.10 Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.

14.11 A contratada não poderá ocupar posto de trabalho, inclusive na função de preposto, com empregado que sejam cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade até o terceiro grau, inclusive, de ocupantes de cargos de chefia, direção e de assessoramento ou membros do TRE/AP, nos termos do que dispõe o art. 3º da Resolução nº 7/2005, do Conselho Nacional de Justiça.

14.12 É vedada a manutenção, aditamento ou prorrogação do contrato decorrente deste Pregão, caso o empregado da contratada que ocupe função de chefia ou supervisão, incida na vedação prevista nos artigos 1º e 2º da Resolução CNJ nº 156/2012.

14.13 A contratada deverá garantir que todos os profissionais alocados para a prestação dos serviços não tenham filiação partidária, por analogia à disposição contida no Art. 366 da Lei nº 4.737/1965 (Código eleitoral), devendo apresentar, antes do início da execução dos serviços, declaração de inexistência de registro dos empregados a serem alocados no contrato em relação oficial de filiados de órgão partidário e manter essa condição até o final de seu vínculo contratual.

14.14 O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico **https://www.gov.br/compras/pt-br.**

14.15 Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

Anexo I do Edital - Termo de Referência
- Anexo I do TR – TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE
- Anexo II do TR – ESPECIFICAÇÕES E QUANTITATIVOS ESTIMADOS
- Anexo III do TR – DOCUMENTO DE FORMALIZAÇÃO DA DEMANDA – DFD
- Anexo IV do TR – INFORMAÇÃO DO VALOR ESTIMADO – ICVE
- Anexo V do TR – ANÁLISE DE RISCOS

Anexo II do Edital – Minuta de Ata de Registro de Preços - ARP
- Anexo I da ARP – Cadastro Reserva

Anexo III do Edital – Minuta de Contrato
- Anexo I do Contrato – Termo de Responsabilidade e Confidencialidade
- Anexo II do Contrato – Termo de Referência

Macapá/AP, 09 de janeiro de 2025.

Francisco Valentim Maia
Diretor Geral – TRE/AP

ANEXO I DO EDITAL
TERMO DE REFERÊNCIA – LEI Nº 14.133/21

1. DAS CONDIÇÕES GERAIS DA CONTRATAÇÃO (art. 6º, XXIII, "a" e "i" da Lei n. 14.133/2021).

1.1. Registro de Preços para aquisição de Ativos de Rede e Segurança da Informação, incluindo Switches, Access Points, Firewalls, Soluções de Gerenciamento, Controle de Acesso e acessórios necessários, com garantia de pelo menos 60 (sessenta) meses, instalação, configuração da solução e treinamento, visando atender às demandas do TRE-AP.

.

LOTE	ITEM	ESPECIFICAÇÃO	QTD TRE-AL	QTD TRE-AM	QTD TRE-AP	QTD TRE-MA	QTD TRE-PB	QTD TRE-PE	QTD TRE-SE	QTD JF-1ªRegião	QTD TOTAL	ESTIMATIVA DE VALOR UNITÁRIO	VALOR TOTAL

1	1	Solução de Gerenciamento Centralizado de Configuração	2	1	2	0	0	0	0	0	5	R$ 24.591,06	R$ 122.955,30
	2	Solução de Logs e Relatoria	2	1	2	0	0	0	1	1	7	R$ 107.473,00	R$ 752.311,00
	3	Solução de Controle de Acesso à Rede (100 endpoints)	14	30	10	0	35	0	20	1	110	R$ 63.744,68	R$ 7.011.914,80
	4	Switch Core	0	4	4	0	0	0	0	0	8	R$ 120.344,93	R$ 962.759,44
	5	Switch de Distribuição	0	8	10	0	14	4	2	0	38	R$ 109.404,48	R$ 4.157.370,24
	6	Switch de Acesso - Tipo 1 (48 Portas)	0	35	40	0	50	28	28	10	191	R$ 21.631,26	R$ 4.131.570,66
	7	Switch de Acesso - Tipo 2 (24 Portas)	0	10	25	0	70	0	30	10	145	R$ 14.134,60	R$ 2.049.517,00
	8	Access Point	0	100	100	0	0	0	0	50	250	R$ 4.647,01	R$ 1.161.752,50
	9	Firewall de Nova Geração (NGFW)	14	70	15	120	100	4	0	4	327	R$ 19.521,83	R$ 6.383.638,41
	10	Transceiver SFP+ 10GBase-SR	0	70	50	0	50	208	56	40	474	R$ 986,84	R$ 467.762,16
	11	Transceiver SFP+ 10GBase-LR	0	10	10	0	0	0	0	0	20	R$ 1.700,92	R$ 34.018,40
	12	Transceiver SFP 1000Base-LX	0	0	10	0	0	0	0	0	10	R$ 1.159,63	R$ 11.596,30
	13	Transceiver SFP 1000Base-SX	0	0	30	0	0	0	0	40	70	R$ 590,15	R$ 41.310,50
	14	Solução de ZTNA (Pacote de 25 dispositivos)	14	60	10	0	20	1	25	0	130	R$ 22.217,65	R$ 2.888.294,50
	15	Banco de Horas Técnicas	250	0	200	0	200	0	0	100	750	R$ 746,77	R$ 560.077,50
	16	Solução de Orquestração, Automação e Resposta de Segurança (SOAR)	1	1	1	0	0	0	0	0	3	R$ 2.888.558,66	R$ 8.665.675,98
	17	Treinamento Oficial - Switches	0	6	5	0	8	0	3	4	26	R$ 28.912,54	R$ 751.726,04
	18	Treinamento Oficial - Access Points	0	6	5	0	0	0	0	4	15	R$ 18.942,72	R$ 284.140,80
	19	Treinamento Oficial - Controle de Acesso à Rede	5	6	5	0	9	0	5	0	30	R$ 28.912,54	R$ 867.376,20
	20	Treinamento Oficial - Infraestrutura e Segurança	5	6	2	0	0	0	1	4	18	R$ 25.974,90	R$ 467.548,20
	21	Treinamento Oficial - Gerenciamento e Relatoria	5	6	2	0	0	0	0	4	17	R$ 14.061,60	R$ 239.047,20
	22	Treinamento Oficial - Solução de Orquestração, Automação e Resposta de Segurança (SOAR)	5	6	5	0	0	0	0	0	16	R$ 18.942,72	R$ 303.083,52
	23	Implantação com Hands On - UST	225	350	225	0	350	0	58	68	1276	R$ 1.116,33	R$ 1.424.437,08

1.2. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 2021. Ademais, é caracterizado como comum, uma vez que se trata de equipamentos para infraestrutura de redes que estão presentes em grandes empresas e em grande quantidade.

1.3. VIGÊNCIA

1.3.1. O prazo de vigência da Ata de Registro de Preços será de 1 (um) ano, contado do primeiro dia útil subsequente à data de divulgação no Portal Nacional de Compras Públicas e poderá ser prorrogado, mediante comprovação de vantajosidade, por igual período, nos termos do art. 22 do Decreto 11.462/2023;

1.3.2. A vigência do contrato formado a partir da aquisição de cada item registrado, deverá ser de 60 (sessenta) meses, contado da data de assinatura do instrumento contratual.

1.4. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

1.4.1. O custo estimado total da contratação é de **R$ 43.739.883,73** (quarenta e três milhões, setecentos e trinta e nove mil oitocentos e oitenta e três reais e setenta e três centavos), conforme custos unitários apostos na tabela acima.

2. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO (art. 6º, inciso XXIII, alínea 'b', da Lei nº 14.133/2021).

2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em Tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

Conforma explanado nos Estudos Técnicos Preliminares (0766126), a demanda por Tecnologia da Informação e Comunicação no setor judiciário está aumentando, destacando a necessidade de uma infraestrutura de rede sólida e segura para suportar operações críticas e dados. No TRE-AP, essa exigência é evidenciada pelo uso intensivo de sistemas variados como PJe, SEI, internet e videoconferências, tornando uma rede de dados eficiente fundamental para as operações do tribunal.
A importância da segurança dos dados trafegados também se intensifica com essa demanda crescente, especialmente considerando o papel crucial do tribunal em assegurar eleições legítimas e apoiar a democracia.
Diante disso, e com os switches e pontos de acesso atualmente próximos ao fim de sua vida útil de garantia, torna-se essencial avaliar e implementar novas soluções de telecomunicações e segurança que atendam às necessidades do TRE-AP. Essa atualização é vital para reforçar a gestão e a segurança da rede, garantindo assim a continuidade e a eficiência das operações do tribunal.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO (art. 6º, inciso XXIII, alínea 'c', e art. 40, §1º, inciso I, da Lei nº 14.133/2021).

3.1. A descrição da solução como um todo, encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares (0766126), apêndice deste Termo de Referência.

A solução proposta envolve a aquisição de ativos de rede, mais especificamente Switches e Access Points, da fabricante Fortinet. Esta escolha visa a padronização com equipamentos

já em uso no TRE-AP e participantes, para melhor gerenciamento, redução de custos operacionais, facilitação na configuração e centralização do controle. Esta abordagem é detalhada nos estudos técnicos preliminares.
É fundamental que os ativos adquiridos contem com uma garantia e suporte técnico de no mínimo 60 meses, refletindo o ciclo de vida esperado para esses equipamentos.
Os switches serão diferenciados em quatro categorias, conforme a capacidade e robustez necessária para cada local de instalação:
1. Switch Core
2. Switch de Distribuição
3. Switch de Acesso 1 - 48 portas
4. Switch de Acesso 2 - 24 portas
Para os Access Points, apenas um modelo será necessário, conforme definido no Anexo I -Especificações Técnicas, deste Termo de Referência.
Este projeto visa não somente otimizar a cobertura e gestão da rede sem fio do TRE-AP, mas também atualizar a topologia de rede, mas implementar mecanismos de segurança, bem como aumentar a robustez, disponibilidade, confiabilidade e eficiência da rede deste Tribunal.
Adicionalmente, pretende-se adquirir Firewalls de pequeno porte, que se integrem à solução de rede proposta e atendam às necessidades do Tribunal, conforme especificações técnicas detalhadas no Anexo I - Especificações Técnicas, deste Termo de Referência.
Além dos dispositivos físicos, busca-se soluções que devem agregar a segurança da informação e gerenciamento dos equipamentos adquiridos, motivo pelo qual deve ser registrado preço para os seguintes serviços:
Solução de Gerenciamento Centralizado de Configuração, Logs e Relatoria: Soluções de análise de segurança e gerenciamento de logs. Ele coleta, consolida e analisa logs e eventos de segurança de vários dispositivos, permitindo uma visão abrangente da postura de segurança de uma organização e solução de gerenciamento centralizado para a infraestrutura de segurança, que permite a administração, configuração e atualização eficiente de dispositivos e políticas de segurança em larga escala
Solução de Controle de Acesso à Rede: Solução projetada para proporcionar visibilidade completa de todos os dispositivos conectados às redes cabeadas e sem fio de uma organização. Ele ajuda a garantir que apenas dispositivos autorizados e conformes possam acessar a rede e seus recursos, aumentando assim a segurança da rede.
Solução de ZTNA: Solução que fornece acesso seguro e controlado a aplicativos e serviços, baseando-se na identidade dos usuários, na análise do contexto de suas solicitações de acesso, e na contínua avaliação da confiança. O objetivo é garantir que apenas usuários autenticados e dispositivos autorizados possam acessar recursos específicos, minimizando assim a superfície de ataque e melhorando a segurança geral da rede.
Solução de Orquestração, Automação e Resposta de Segurança: Solução que visa ajudar as equipes de operações de segurança (SOCs) a gerenciar e responder a alertas de segurança de forma mais eficiente e eficaz, reduzindo o tempo de resposta a incidentes e melhorando os processos de segurança
O pacote contempla ainda a contratação de treinamento oficial referente a cada solução, bem como banco de horas técnicas para suporte especializado adicional, e serviços de implantação da solução com treinamento prático.
A aquisição de cada equipamento, quais sejam, switches, firewalls ou access points, enseja a garantia do fabricante, bem como suporte técnico da fornecedora, durante toda a vigência do Contrato, a fim de garantir o pleno funcionamento, bem como a resposta adequada a eventos de indisponibilidade, seja por necessidade de configurações ou aprimoramentos (suporte técnico), bem como por falha do equipamento em si (garantia).
Resumindo, o objetivo é estabelecer um Registro de Preços para aquisição de Ativos de Rede e Segurança da Informação, incluindo Switches, Access Points, Firewalls e acessórios necessários, bem como Soluções de Segurança da Informação, garantia de pelo menos 60 (sessenta) meses, instalação, configuração da solução e treinamento oficial, visando atender as demandas do TRE-AP e demais participantes.

4. REQUISITOS DA CONTRATAÇÃO (art. 6º, XXIII, alínea 'd', da Lei nº 14.133/21).

4.1. A contratação deverá observar os seguintes requisitos:

4.1.1. Sustentabilidade:

4.1.1.1. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

a) os equipamentos de tecnologia de informação e comunicação, bem como os seus periféricos e acessórios não contenham substâncias perigosas como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenil-olibromados (PBDEs) em concentração acima da recomendada pela diretiva da Comunidade Econômica Européia Restriction of Certain Hazardous Substances – RoHS17;

4.1.2. Indicação de marcas ou modelos (Art. 41, inciso I, da Lei nº 14.133/2021):

4.1.2.1. Na presente contratação será admitida a indicação da(s) seguinte(s) marca(s), característica(s) ou modelo(s), de acordo com as justificativas contidas nos Estudos Técnicos Preliminares:

4.1.2.1.1. Fabricante Fortinet

4.1.2.2. Tal exigência está de acordo com o art. 41, inciso I, alíneas a e b da Lei 14.133/21, visto que trata-se de solução com itens interrelacionados, que visam centralizar a administração de rede do TRE-AP e participantes, reduzindo o esforço operacional, aumentando a eficiência dos controles, bem como é necessária a manutenção da compatibilidade entre os itens adquiridos e as plataformas e padrões já adotados pela Administração.

4.1.3. Negócio:

4.1.3.1. Manter e aprimorar a Rede Local do TRE-AP e participantes;
4.1.3.2. Prover gerenciamento centralizado de switches e Access Points;
4.1.3.3. Prover a documentação da arquitetura de rede local, incluindo diagramas de rede (físico e lógico), incluindo informações de configuração e modelo de firewalls, switches e access points;
4.1.3.4. Instalação e repasse de conhecimento da solução;
4.1.3.5. Compatibilidade com soluções/equipamentos/licenças de telecomunicações e segurança da informação já contratadas por este TRE-AP.

4.1.4. Legais:

4.1.4.1. Lei 14.133/2021;
4.1.4.2. Resolução CNJ n.º 468/2022;
4.1.4.3. Decreto 11.462/2023;
4.1.4.4. IN SEGES/ME 65/2021.

4.1.5. Garantia e Manutenção:

4.1.5.1. Serviços de suporte e manutenção aos ativos em garantia deverão estar disponíveis 24 (vinte e quatro horas) por dia 5 (cinco) dias por semana (segunda à sexta);
4.1.5.2. Serviços de suporte e manutenção ocorrerão sem nenhum ônus, mesmo quando for necessária a atualização, o translado e a estada de técnicos ou qualquer outro tipo de serviço necessário para garantir a operação dos ativos;
4.1.5.3. Disponibilidade dos números de telefone, endereços de correio eletrônico ou área em sítio da Web voltados para a abertura dos chamados técnicos;
4.1.5.4. A manutenção nos equipamentos, em eventuais defeitos durante o período de garantia, ficará a cargo da CONTRATADA, cabendo-lhe efetuar a substituição dos ativos, ajustes nos sistemas, conserto ou troca de peças defeituosas, por novas, sem nenhum tipo de ônus para a CONTRATANTE;
4.1.5.5. Os ativos devem possuir garantia da fabricante e suporte técnico da CONTRATADA, pelo período mínimo de 60 (sessenta) meses;
4.1.5.6. A empresa licitante deverá dispor de meios de comunicação públicos ou privados para facilitar a efetivação de chamados.

4.1.6. Temporais:

4.1.6.1. A contratação deverá ocorrer até o término do exercício de 2024;
4.1.6.2. A vigência contratual deverá ser de 60 (sessenta) meses.

4.1.7. Segurança da Informação:

4.1.7.1. A Contratada deve se comprometer com a guarda do sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

4.1.8. Metodologia de trabalho e implantação da solução:

4.1.8.1. A entrega dos equipamentos, bem como a execução dos serviços deverão ser realizados nos locais indicados no item 5.3.

4.1.9. Capacitação e experiência profissional da equipe:

4.1.9.1. A Contratada deverá apresentar comprovação de que os técnicos responsáveis pela instalação dos hardwares e/ou softwares essenciais para a prestação do serviço estão devidamente habilitados tecnicamente para prover o serviço.

4.2. Não será admitida a subcontratação do objeto contratual.

4.3. Não haverá exigência da garantia da contratação dos arts. 96 e seguintes da Lei nº 14.133/21, pelas razões abaixo justificadas:

4.3.1. O pagamento se dará com a entrega dos equipamentos, bem como dos serviços registrados, de forma que eventual risco de descumprimento de contrato se dará em relação à garantia e suporte técnico.
4.3.2. Dessa forma, não há necessidade de exigência de garantia, visto que se trata de risco baixo e aceito pela Equipe de Planejamento da Contratação, sendo medida desproporcional reter valores a título de garantia para eventos que, pelos requisitos da contratação, dificilmente se concretizariam.

5. MODELO DE EXECUÇÃO CONTRATUAL (arts. 6º, XXIII, alínea "e" e 40, §1º, inciso II, da Lei nº 14.133/2021).

5.1. O prazo de entrega dos bens é de 30 (trinta) dias, contados da data de emissão da Ordem de Serviço referente a cada item contratado.
5.3. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 5 (cinco) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.
5.3. Os bens deverão ser entregues nos seguintes endereços:

ORGÃO	ENDEREÇO:	SETOR RESPONSÁVEL:
Tribunal Regional Eleitoral de Alagoas / TRE-AL	Rua Coronel Pedro Lima, 230, Jaraguá, CEP: 57.022-220, Maceió - AL	Seção de Almoxarifado
Tribunal Regional Eleitoral do Amazonas / TRE-AM	Avenida André Araújo, 200, Aleixo, CEP: 69.060-000, Manaus - AM	Coordenadoria de Infraestrutura / COINF
Tribunal Regional Eleitoral do Amapá / TRE-AP	Avenida Mendonça Junior, 1502, Centro, CEP: 68.900-914, Macapá - AP	Coordenadoria de Material e Patrimônio / CMP
Tribunal Regional Eleitoral do Maranhão / TRE-MA	Avenida Senador Vitorino Freire, Areinha, CEP: 65.010-917, São Luís - MA	Seção de Gestão de Redes / SERED
Tribunal Regional Eleitoral da Paraíba / TRE-PB	Avenida Princesa Isabel, 201, Tambiá, CEP: 58.020-528, João Pessoa - PB	Seção de Gestão Patrimônio / SEGEP
Tribunal Regional Eleitoral de Pernambuco / TRE-PE	Avenida Rui Barbosa, 320, Graças, CEP: 52011-40, Recife - PE	Seção de Almoxarifado
Tribunal Regional Eleitoral de Sergipe / TRE-SE	CENAF, Lote 7, Variante 2, CEP: 49.081-000, Aracaju - SE	Servidor: José Carvalho Peixoto
Justiça Federal de Primeiro Grau – Seção Judiciária do Amapá / SJAP-SECAD	Rodovia Norte/Sul s/n, Infraero II, CEP: 68.908-911, Macapá - AP	NUTEC/SJAP

5.5. Os bens serão recebidos provisoriamente, de forma sumária, no prazo de 5 (cinco) dias, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.
5.6. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 (quinze) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.
5.7. Os bens serão recebidos definitivamente no prazo de 30 (trinta) dias, contados do recebimento provisório, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.
5.7.1. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.
5.8. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.
5.9. Antes de cada pagamento à CONTRATADA, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação.
5.10. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.
5.11. Não havendo regularização ou sendo a defesa considerada improcedente, a CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.
5.12. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, sem prejuízo da aplicação de penalidade.
5.13. Em caso de reajuste, a ser concedido conforme os requisitos previstos em lei, o índice aplicável será o Índice Nacional de Preços ao Consumidor Amplo (IPCA/IBGE).

6. ESPECIFICAÇÃO DA GARANTIA CONTRATUAL EXIGIDA E DAS CONDIÇÕES DE MANUTENÇÃO E ASSISTÊNCIA TÉCNICA (art. 40, §1º, inciso III, da Lei nº 14.133/2021).

6.1. GARANTIA DO FABRICANTE

6.1.1. O prazo de garantia contratual dos bens, compreendidos estes pelos itens 5, 6, 7, 8, 9 e 10, do presente Termo de Referência, complementar à garantia legal, é de, **no mínimo, 60 (sessenta) meses**, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.
6.1.2. A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.
6.1.3. A garantia abrange a realização da manutenção corretiva dos bens pelo próprio Contratado, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.
6.1.4. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.
6.1.5. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.
6.1.6. Uma vez notificado, o Contratado realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 10 (dez) dias úteis, contados a partir da data de retirada do equipamento das dependências da Administração pelo Contratado ou pela assistência técnica autorizada.
6.1.7. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada do Contratado, aceita pelo Contratante.
6.1.8. Antes de retirar o equipamento das dependências da Administração, o Contratado deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.
6.1.9. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pelo Contratado, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do Contratado o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.
6.1.10. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do Contratado.
6.1.11. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.
6.1.12. Todos os itens de software que vierem instalados de fábrica no equipamento ofertado deverão estar cobertos pela garantia e serviço de suporte do fabricante;

6.2. SUPORTE TÉCNICO

6.2.1. O Contratado deve possuir suporte técnico remoto para a solução de problemas comuns de suporte;
6.2.2. O Contratado deve realizar atendimento on-site em até 05 (cinco) dias úteis, com tempo de atendimento contado a partir da abertura do chamado;
6.2.2.1. Caso viável e solicitado pelo Contratado, o atendimento poderá ser realizado de forma remota.
6.2.3. Para cada chamado técnico, o Contratado deverá disponibilizar número de protocolo único para que o Contratante possa acompanhar a resolução de cada problema, bem como monitorar se os tempos de atendimento técnico estão em conformidade;
6.2.4. Deverá ser disponibilizado acesso Web para consulta da utilização do serviço contratado, por meio de ferramentas de mercado;

6.2.5. Os serviços de suporte técnico incluem serviços de atualização do(s) equipamento(s) componente(s) da solução ofertada, sendo responsáveis pelo fornecimento de patches, correções e novas versões de software de equipamentos, quando aplicável.

7. MODELO DE GESTÃO DO CONTRATO (art. 6º, XXIII, alínea "f", da Lei nº 14.133/21).

7.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial (Lei nº 14.133/2021, art. 115, *caput*).

7.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila (Lei nº 14.133/2021, art. 115, §5º).

7.3. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133/2021, art. 117, *caput*).

7.3.1. O fiscal do contrato anotará em registro próprio todas as ocorrências relacionadas à execução do contrato, determinando o que for necessário para a regularização das faltas ou dos defeitos observados (Lei nº 14.133/2021, art. 117, §1º).

7.3.2. O fiscal do contrato informará a seus superiores, em tempo hábil para a adoção das medidas convenientes, a situação que demandar decisão ou providência que ultrapasse sua competência (Lei nº 14.133/2021, art. 117, §2º).

7.4. O Contratado será obrigado a reparar, corrigir, remover, reconstruir ou substituir, a suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes de sua execução ou de materiais nela empregados (Lei nº 14.133/2021, art. 119).

7.5. O Contratado será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo contratante (Lei nº 14.133/2021, art. 120).

7.6. Somente o Contratado será responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato (Lei nº 14.133/2021, art. 121, *caput*).

7.6.1 A inadimplência do Contratado em relação aos encargos trabalhistas, fiscais e comerciais não transferirá à Administração a responsabilidade pelo seu pagamento e não poderá onerar o objeto do contrato (Lei nº 14.133/2021, art. 121, §1º).

7.7. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se, excepcionalmente, o uso de mensagem eletrônica para esse fim (IN 5/2017, art. 44, §2º).

7.8. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato (IN 5/2017, art. 44, 31º).

7.9. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade convocará o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros (IN 5/2017, art. 44, 31º).

7.10. Antes do pagamento da nota fiscal ou da fatura, deverá ser consultada a situação da empresa junto ao SICAF.

7.11. Serão exigidos a Certidão Negativa de Débito (CND) relativa a Créditos Tributários Federais e à Dívida Ativa da União, o Certificado de Regularidade do FGTS (CRF) e a Certidão Negativa de Débitos Trabalhistas (CNDT), caso esses documentos não estejam regularizados no SICAF.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR (art. 6º, inciso XXIII, alínea 'h', da Lei nº 14.133/2021).

8.1. DA NATUREZA DO OBJETO

8.1.1. Considerando que as soluções que compõem a presente contratação possuem padrões de desempenho e qualidade que podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado, trata-se de contratação de bens e serviços comuns, nos termos da Lei 14.133/21.

8.2. DO PARCELAMENTO DO OBJETO

8.2.1. Conforme abordado nos Estudos Técnicos Preliminares, caso haja adjudicação por item, na presente contratação, haverá prejuízo para o conjunto e em perda de economia em escala, além de aumentar de forma desproporcional a complexidade da implantação;

8.2.2. Dessa forma, será realizada a adjudicação por preço global, visto que se trata de lote único.

8.3. DA SELEÇÃO DO FORNECEDOR

8.3.1. Serão selecionadas as propostas dos fornecedores que apresentarem o MENOR PREÇO POR LOTE, desde que atendam todos os requisitos deste Termo de Referência e anexos e não ultrapassem o valor máximo estimado para cada item.

8.4. DA MODALIDADE E TIPO DE LICITAÇÃO

8.4.1. Conforme abordado nos Estudos Técnicos Preliminares, considerando a aquisição de bens e contratação de serviços que visam atender mais de um órgão ou entidade, bem como a necessidade de possibilidade de entregas parceladas e economia de escala, a presente contratação será realizada utilizando-se do sistema de Registro de Preços;

8.4.2. Verifica-se que o objeto pretendido é oferecido por diversos fornecedores no mercado de TIC e apresenta características padronizadas e usuais. Assim, pode-se concluir que o objeto é comum e, portanto, é recomendada, pela Lei 14.133/21, a utilização da modalidade **PREGÃO**. Sendo, preferencialmente, em sua forma eletrônica e do tipo **MENOR PREÇO**.

8.5. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

8.5.1. Os órgãos e as entidades que não participarem do procedimento de intenção de registro de preços poderão aderir à Ata de Registro de Preços na condição de não participantes, observados os seguintes requisitos:

8.5.1.1. Apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;

8.5.1.2. Demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado na forma do artigo 23 da Lei nº 14.133/2021;

8.5.1.3. Prévias consulta e aceitação do órgão ou entidade gerenciadora e do fornecedor.

8.5.1.3.1. Eventual concessão de autorização por parte do Órgão gerenciador será realizada após a aceitação da adesão pelo fornecedor, conforme item 8.5.4.

8.5.2. O limite das aquisições ou das contratações, a que se refere o subitem 8.5.1, não poderá exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do instrumento convocatório registrados para o Órgão gerenciador e para os órgãos ou as entidades participantes.

8.5.3. O limite global de adesões à ata de registro de preços, a que se refere o item 8.5.1, não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o Órgão gerenciador e os órgãos ou as entidades participantes, independentemente do número de órgãos ou entidades não participantes que aderirem.

8.5.3.1. O limite referenciado no item 8.5.3 não se aplica nas hipóteses descritas no artigo 32, §§ 1º e 2º, do Decreto nº 11.462 /2023.

8.5.4. Os órgãos e entidades que não participaram do registro de preço deverão encaminhar ofício ao órgão gerenciador, juntamente com a concordância e declaração do fornecedor, nos termos do subitem 8.5.1.3.

8.5.5. Caberá ao fornecedor beneficiário desta Ata de Registro de Preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento, desde que este fornecimento não prejudique as obrigações anteriormente assumidas com o órgão gerenciador e os órgãos participantes.

8.5.1. A concordância do fornecedor beneficiário desta Ata de Registro de Preços deverá conter declaração de que não haverá prejuízos às obrigações presentes e futuras decorrentes desta Ata firmada com o TRE-AP.

8.5.6. Ao órgão não participante que aderir a esta Ata competem os atos relativos à cobrança do cumprimento pelo fornecedor das obrigações contratualmente assumidas e a aplicação, observada a ampla defesa e o contraditório, de eventuais penalidades decorrentes do descumprimento de cláusulas contratuais, em relação às suas próprias contratações, informando as ocorrências ao órgão gerenciador.

8.5.7. O órgão não participante deverá efetivar a contratação solicitada em até 90 (noventa) dias, observado o prazo de vigência desta Ata de Registro de Preços.

8.5.8. Caberá ao órgão gerenciador autorizar, excepcional e justificadamente, a prorrogação do prazo para efetivação da contratação, respeitado o prazo de vigência desta Ata, desde que solicitada pelo órgão não participante.

8.5.9 - É vedada a participação de 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, ressalvada a hipótese de ata com registro de quantitativo inferior ao máximo previsto no Edital do Pregão Eletrônico mencionado no preâmbulo.

8.5.10 - O órgão ou a entidade que integra esta Ata de Registro de Preços poderá aderir a item desta ata, na qualidade de não participante, para aqueles itens para os quais não tenha quantitativo registrado, observados os requisitos previstos no Edital do Pregão Eletrônico mencionado no preâmbulo.

8.6. DOS CRITÉRIOS TÉCNICOS DE HABILITAÇÃO

8.6.1. A Licitante deverá apresentar no mínimo 02 (dois) atestados de capacidade técnica compatíveis com o objeto desta licitação, expedido por pessoa jurídica de direito público ou privado, para a qual a Licitante forneceu ou está fornecendo, de modo efetivo, soluções e/ou bens do mesmo Fabricante e de mesma natureza e/ou similares e/ou compatíveis coma proposta apresentada;

8.6.2. O(s) atestado(s) de capacidade técnica deverá(ão) conter, no mínimo, as seguintes informações:

8.6.2.1. Identificação da pessoa jurídica e do responsável pela emissão do atestado;

8.6.2.2. Identificação do licitante, constando o seu CNPJ e endereço completo;

8.6.2.3. Descrição clara dos produtos/serviços, devendo ser assinado por seus sócios, diretores, administradores, procuradores, gerentes ou servidor/empregado responsável, com expressa indicação de seu nome completo, cargo/função e meios de contato;

8.6.2.3. As declarações de pessoas jurídicas de direito privado devem estar, preferencialmente, com firma reconhecida;

8.6.3. A Licitante vencedora deverá comprovar que atende às especificações técnicas exigidas neste Termo de Referência, através de documentação do fabricante, em língua portuguesa ou inglesa, em formato de arquivos PDF e/ou em endereços de internet do fabricante do produto;

8.6.4. A Licitante deve comprovar que é fornecedora autorizada e credenciada, pela fabricante, para comercialização das soluções que compõem o objeto da presente contratação;

8.6.5. A Licitante vencedora deverá apresentar planilha única com as informações de onde consta cada especificação técnica atendida;

8.6.6. O não atendimento de qualquer um dos subitens anteriores desclassificará a Licitante, devendo o pregoeiro chamar a próxima licitante mais bem classificada para o respectivo Lote.

9. OBRIGAÇÕES DO CONTRATANTE

9.1. Constituem obrigações do TRE-AP (órgão gerenciador):

9.1.1. gerenciar a ata de registro de preços, providenciando a indicação, sempre que solicitado, da empresa registrada, para atendimento às necessidades da Administração, obedecendo aos quantitativos definidos no Termo de Referência;

9.1.2. efetuar os pagamentos nas condições e preços ora pactuados, desde que não haja óbice legal nem fato impeditivo provocado pela beneficiária da Ata;

9.1.3. prover todas as condições necessárias para o desenvolvimento das atividades contratadas;

9.1.4. notificar a beneficiária da Ata, via e-mail, salvo a abertura de chamados técnicos, sobre a ocorrência de eventuais falhas no curso da execução dos serviços por meio de seus Fiscais ou Gestores;

9.1.4.1. Esta obrigação compete também aos demais participantes deste Registro de Preços em relação às suas contratações.

9.1.5. responsabilizar-se pela comunicação, em tempo hábil, dos serviços a serem executados;

9.1.6. efetuar toda a comunicação originada pelo TRE-AP através de mensagem de correio eletrônico, salvo a abertura de chamados técnicos, endereçada ao representante da beneficiária da Ata;

9.1.7. acompanhar e fiscalizar a execução do Registro de Preços por meio dos servidores indicados pelo TRE-AP, nos termos da Lei n.º 14.133/2021;

9.1.8. publicar o extrato desta Ata de Registro de Preços no Diário Oficial da União.

9.2. A Administração não se obriga a adquirir a quantidade total ou parcial do objeto adjudicado constante nesta Ata de Registro de Preços;

9.3. Assinada a Ata de Registro de Preços e publicado o seu extrato no D.O.U, é facultado à Administração assinar o termo de contrato em favor da empresa adjudicatária.

10. OBRIGAÇÕES DA BENEFICIÁRIA DA ATA

10.1. Será de responsabilidade da beneficiária da Ata a entrega do objeto a ela adjudicado, de acordo com a especificação do Edital, na forma do Termo de Referência e seus anexos, obedecendo a todas as condições estabelecidas no Edital que originou a presente Ata, bem como as oferecidas em sua proposta;

10.2. Constituem obrigações da beneficiária da ata:

10.2.1. arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas, responsabilizando-se pelos danos causados diretamente à administração ou a terceiros, decorrentes de sua culpa ou dolo, sem qualquer ônus ao TRE-AP;

10.2.2. prestar todos os esclarecimentos que forem solicitados pelo TRE-AP, credenciando um representante para prestar os devidos esclarecimentos e atender às reclamações que porventura surgirem durante a execução do objeto;

10.2.3. quando, por problemas técnicos, os prazos pactuados não puderem ser cumpridos, a beneficiária da Ata deverá comunicar por escrito ao TRE-AP até 2 (dois) dias úteis anteriores ao término do prazo, cabendo ao gestor da Ata aceitar ou rejeitar as justificativas;

10.2.4. a beneficiária da Ata é obrigada a reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou de materiais empregados;

10.2.5. não transferir a outrem, no todo ou em parte, o objeto da presente contratação, sem prévia e expressa anuência do TRE-AP;

10.2.6. informar qualquer alteração necessária à consolidação dos ajustes decorrentes da execução do objeto, tais como: mudança de endereços, razão social, telefone, fax, dissolução da sociedade, falência e outros;

10.2.7. comunicar imediatamente ao gestor da Ata, qualquer anormalidade verificada, inclusive de ordem funcional, para que sejam adotadas as providências de regularização necessárias, em qualquer tempo até o final da garantia;

10.2.8. responder, para cada um dos itens contratados, por todas e quaisquer obrigações relativas a direitos de marcas e patentes, ficando esclarecido que o TRE-AP não aceitará qualquer imputação nesse sentido; além de atender a todos os encargos, inclusive os de natureza tributária, incidentes sobre o funcionamento do objeto (ISS, PIS e COFINS), cabendo-lhe, também, a responsabilidade total e exclusiva, pela reparação de quaisquer danos diretos causados a pessoas e a bens ou serviços do TRE-AP ou de terceiros), ou em virtude de manuseio ou utilização dos produtos por ela fornecidos;

10.2.9. garantir, na atualização dos softwares relativos ao contrato de suporte, enquanto vigente a contratação, o fornecimento de upgrades para versões mais recentes, bem como releases e patches das licenças de uso dos softwares, não implicando custos adicionais para a contratação;

10.2.10. garantir acesso aos canais de suporte técnico no regime de 24x7 - 24 horas, 7 dias na semana - através de número de telefone de discagem gratuita (0800) e/ou internet, para abertura de chamados técnicos, objetivando a resolução de problemas e dúvidas quanto ao funcionamento dos softwares, bem como permitir a utilização de estrutura de pesquisa em base de conhecimento de solução de problemas e documentos técnicos, todos de propriedade da beneficiária da Ata;

10.2.11. manter confidencialidade e, em nenhum momento, divulgar a terceiros, sem a ciência e o consentimento do TRE-AP, documentos, imagens/fotos, dados ou outra informação que tiver sido direta ou indiretamente proporcionada pelo TRE-AP, antes, durante ou depois de encerrada a vigência do contrato, nos termos da política de suporte técnico da beneficiária da Ata;

10.2.12. manter, durante toda a execução do objeto licitado, em compatibilidade com as obrigações assumidas por ela, todas as condições de habilitação e qualificação exigidas na licitação;

10.2.13. comunicar ao TRE-AP qualquer modificação em seu endereço, sob pena de se considerar perfeita a notificação realizada no endereço apresentado durante o Pregão;

10.2.14. manter as condições de sustentabilidade exigidas para o certame durante toda a execução da Ata de Registro de Preço;

10.2.15. ser responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução contratual. A inadimplência da beneficiária da Ata, com referência aos encargos estabelecidos neste subitem não transfere a responsabilidade por seu pagamento à administração do TRE-AP, nem poderá onerar o objeto da licitação, razão pela qual a beneficiária da Ata renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com o TRE-AP;

10.2.16. obedecer às normas de segurança da informação existentes na Justiça Eleitoral e também as normas/regras específicas dos participantes responsáveis pela aquisição.

10.3. Todos os impostos, taxas, fretes, seguros e encargos sociais e trabalhistas, que incidam ou venham a incidir sobre a presente Ata de Registro de Preços ou decorrentes de sua execução, serão de exclusiva responsabilidade da beneficiária da Ata.

10. NÍVEIS DE SERVIÇO

10.1. Deverão ser observados os Níveis de Serviço, conforme a tabela abaixo:

SEVERIDADE	DESCRIÇÃO	TIPO DE ATENDIMENTO	TEMPO DE INÍCIO DE ATENDIMENTO	TEMPO DE SOLUÇÃO OU CONTORNO	OBSERVAÇÃO
1 - Crítica	Chamados referentes à situação de emergência ou problemas críticos, caracterizados pela existência de sistema paralisado, indisponível para o uso	Remoto / On-site	No máximo 1 (uma) hora corrida após a abertura do chamado	No máximo 6 (seis) horas corridas após o início do atendimento	O atendimento não poderá ser interrompido até o completo restabelecimento da solução, mesmo que se estenda por períodos noturnos e dias não úteis
2 - Alta	Chamados associados a situações de alto impacto, incluindo os casos de degradação severa de desempenho	Remoto / On-site	No máximo 1 (uma) hora corrida após a abertura do chamado	No máximo 10 (dez) horas corridas após o início do atendimento	O atendimento não poderá ser interrompido até o completo restabelecimento da solução, mesmo que se estenda por períodos noturnos e dias não úteis
3 - Média	Chamados referentes a situações de baixo	Remoto	No máximo 2 (duas)	No máximo 24 (vinte	Caso o problema não possa ser resolvido

	impacto ou para aqueles problemas que se apresentem de forma intermitente, incluindo os casos em que haja a necessidade de substituição de componente(s) que possua(m) redundância		hora corrida após a abertura do chamado	quatro) horas corridas após o início do atendimento	remotamente dentro do prazo estabelecido, a CONTRATADA deverá colocar à disposição e às suas expensas, um especialista devidamente habilitado e credenciado que trabalhará o tempo que for necessário para a solução do problema.
	Chamados com objetivo de solicitar acompanhamento técnico presencial para o desligamento e posterior ligação do(s) equipamento(s) em virtude de atividade programada	On site	No máximo 1 (uma) semana corrida após a abertura do chamado	Conforme agendamento	O atendimento deverá ser realizado conforme o agendamento, mesmo que contemple períodos noturnos e dias não úteis
4 - Baixa	Chamados de suporte técnico em garantia, com objetivo de sanar dúvidas quanto ao uso ou à implementação do produto	Remoto	No máximo 8 (oito) horas úteis após a abertura do chamado	No máximo 24 (vinte quatro) horas corridas após o início do atendimento	Caso a dúvida não possa ser respondida pela CONTRATADA ou dependa do Fornecedor ou de um terceiro para composição da resposta, deve ser informado ao requisitante dentro do prazo estabelecido para atendimento do chamado.

10.2. Caso seja necessário, a CONTRATADA poderá aplicar solução de contorno, providenciando em caráter temporário componente/equipamento equivalente para substituição do item danificado, estando a CONTRATADA responsável por toda logística, instalação e configuração dos equipamentos, assim como pela retirada dos antigos, sem qualquer ônus adicional ao CONTRATANTE;
10.2. O fechamento do chamado poderá se dar, quer pela aplicação de correção ao produto ou pela aplicação de solução de contorno que possibilite a operação do sistema.
10.3. Caso haja necessidade de dilação de prazo, a CONTRATADA deverá fazer solicitação fundamentada à CONTRATANTE;

11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.
11.1.1. A contratação será atendida pela ação orçamentária julgamento de causas e gestão administrativa na Justiça Eleitoral - Proposta Orçamentária 0001 e julgamento de causas e SEGO - Segurança da Informação.

339040 - Serviço de Tecnologia da Informação
449040 - Aquisição de software
449052 - Outros equipamentos e materiais permanentes.

12. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

12.1. Constituída através da Portaria Presidência nº 140/2024 TRE-AP/PRES/DG/SGP/COPES
Integrante demandante: Jimmy Almendra Macedo – Matrícula: 30927192
Integrante técnico: Renan Coutinho Diniz – Matrícula: 30928172
Integrante administrativo: Juarez do Carmo Benício Dias da Silva – Matrícula: 30927296

ANEXO I DO TERMO DE REFERÊNCIA
ESPECIFICAÇÕES E QUANTITATIVOS ESTIMADOS

LOTE	ITEM	DESCRIÇÃO DO OBJETO
1	1	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO
	2	SOLUÇÃO DE LOGS E RELATORIA
	3	SOLUÇÃO DE CONTROLE DE ACESSO À REDE
	4	SWITCH CORE
	5	SWITCH DE DISTRIBUIÇÃO
	6	SWITCH DE ACESSO TIPO 1 – 48 PORTAS GIGABIT
	7	SWITCH DE ACESSO TIPO 2 – 24 PORTAS GIGABIT
	8	ACCESS POINT
	9	FIREWALL DE NOVA GERAÇÃO (NGFW)
	10	TRANSCEIVER SFP+ 10GBase-SR
	11	TRANSCEIVER SFP+ 10GBase-LR
	12	TRANSCEIVER SFP 1000Base-LX
	13	TRANSCEIVER SFP 1000Base-SX
	14	SOLUÇÃO DE ZTNA (PACOTE DE 25 DISPOSITIVOS)
	15	BANCO DE HORAS TÉCNICA
	16	SOLUÇÃO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA DE SEGURANÇA (SOAR)
	17	TREINAMENTO OFICIAL - SWITCHES
	18	TREINAMENTO OFICIAL - ACCESS POINTS
	19	TREINAMENTO OFICIAL - CONTROLE DE ACESSO À REDE
	20	TREINAMENTO OFICIAL - INFRAESTRUTURA E SEGURANÇA
	21	TREINAMENTO OFICIAL - GERENCIAMENTO E RELATORIA
	22	TREINAMENTO OFICIAL - SOLUÇÃO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA DE SEGURANÇA (SOAR)
	23	IMPLANTAÇÃO COM HANDS ON - UST

ITEM 1 - SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO

1.1. Deve estar dimensionado e licenciado para gerenciar até 10 (dez) Firewalls de Próxima Geração (NGFW) considerando os modelos FortiGate 601E, FortiGate 201F e FortiGate 61F, em uso no TRE , atendendo aos requisitos deste item;

1.2. Possibilitar a criação e administração de políticas de Firewall, Controle de Aplicação, Sistema de Prevenção a Intrusão (IPS - Intrusion Prevention System), Antivírus, Filtro de Conteúdo e URL e Balanceamento inteligente de Links (SD-WAN);
1.3. Como parte da visibilidade dos dispositivos gerenciados centralmente, a solução deve ter visibilidade das verificações de saúde do link, desempenho da aplicação, utilização da largura de banda e conformidade com o nível de serviço definido;
1.4. Deve ter a capacidade de permitir o provisionamento de comunidades VPN e monitorar as conexões VPN de todos os dispositivos gerenciados a partir de uma única console, além de exibir sua localização geográfica em um mapa;
1.5. Permitir criar templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;
1.6. Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.
1.7. A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;
1.8. Deverá garantir a integridade do item de configuração, através de bloqueio de alterações, em caso de acesso simultâneo de dois ou mais administradores no mesmo ativo;
1.9. Permitir acesso concorrente de administradores e que seja definida uma cadeia de aprovação das alterações realizadas;
1.10. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
1.11. Permitir usar palavras chaves ou cores para facilitar identificação de regras;
1.12. Permitir localizar em quais regras um objeto (ex. computador, serviço, etc.) está sendo utilizado;
1.13. Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;
1.14. Permitir criação de regras que fiquem ativas em horário definido;
1.15. Permitir criação de regras com data de expiração;
1.16. Realizar o backup das configurações para permitir o retorno de uma configuração salva;
1.17. Possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem ou conflitem com outras, ou garantir que esta exigência seja plenamente atendida por meio diverso.
1.18. Gerar alertas automáticos via Email, SNMP e Syslog;
1.19. Deve ser permitido ao administrador transferir os backups para um servidor FTP, SCP ou SFTP.
1.20. Permitir backup das configurações e rollback de configuração para a última configuração salva;
1.21. Deve possibilitar a visualização e comparação de configurações atuais e configurações anteriores;
1.22. Possuir um sistema de backup/restauração de todas as configurações da solução de gerência incluso assim como permitir ao administrador agendar backups da configuração em um determinado dia e hora;
1.23. Deve suportar a distribuição e instalação remota de novas versões de software dos equipamentos, de forma remota e centralizada;
1.24. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;
1.25. Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, TACACS+ e PKI.
1.26. A solução deve incluir uma ferramenta para gerenciar centralmente as licenças de todos os appliances controlados pela estação de gerenciamento, permitindo ao administrador atualizar licenças nos appliances através dessa ferramenta.
1.27. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances.
1.28. Deve suportar o gerenciamento de pontos de acesso de forma centralizada.
1.29. Deve suportar o gerenciamento centralizado de switches.
1.30. A solução deve possuir garantia, suporte e atualizações ao software durante a vigência do contrato.
1.31. A solução de gerenciamento centralizado poderá ser ofertada em formato de appliance físico ou appliance virtual, e caso ofertado em formato virtual, será responsabilidade da contratante a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;
1.32. Caso a solução seja entregue em appliance virtual, deverá ser compatível com Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2012 / 2016/ 2019 e KVM no Redhat 7.1 ou superiores;
1.33. Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;
1.34. Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;
1.35. Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;
1.36. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;

ITEM 2 - SOLUÇÃO DE LOGS E RELATORIA

2.1. Deve suportar o acesso via SSH, WEB (HTTPS) para gerenciamento da solução;
2.2. A solução deve suportar receber, no mínimo, 25 (vinte e cinco) GB de logs diários;
2.3. A solução deverá ser capaz de armazenar logs por no mínimo 12 (doze) meses;
2.4. Permitir acesso simultâneo à administração, bem como criar pelo menos 2 (dois) perfis para administração e monitoramento;
2.5. Possuir suporte para SNMP versão 2 e 3;
2.6. Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;
2.7. Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;
2.9. Suporte a definição de perfis de acesso ao console com permissão granular, como: acesso de gravação, acesso de leitura, criação de novos usuários e alterações nas configurações gerais;
2.10. Suporte a autenticação de usuários de acesso à plataforma via LDAP, Radius ou TACACS+;
2.11. Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;
2.12. Deve permitir gerar alertas de eventos a partir de logs recebidos;
2.13. A solução deve ter relatórios predefinidos;
2.14. Permitir importação e exportação de relatórios
2.15. Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
2.16. Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
2.17. Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;
2.18. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
2.19. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;

2.20. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
2.21. Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;
2.22. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;
2.23. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;
2.24. Deve possuir mecanismos de remoção automática para logs antigos;
2.25. Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;
2.26. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
2.27. Permitir o envio por e-mail relatórios automaticamente;
2.28. Deve permitir que o relatório seja enviado por Email para o destinatário específico;
2.29. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
2.30. Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;
2.31. Deve permitir o uso de filtros nos relatórios;
2.32. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
2.33. Permitir especificar o idioma dos relatórios criados;
2.34. Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
2.35. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
2.36. Deve permitir o envio automático dos logs para um servidor FTP externo a solução;
2.37. Deve permitir exportar os logs no formato CSV;
2.38. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
2.39. Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
2.40. Os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;
2.41. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
2.42. Possibilidade de exibir nos relatórios da GUI as informações do sistema, como licenças, memória, disco rígido, uso da CPU, taxa de log por segundo recebido, total de logs diários recebidos, alertas do sistema, entre outros;
2.43. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
2.44. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
2.45. Deve permitir visualizar em tempo real os logs recebidos;
2.46. Deve permitir o encaminhamento de log no formato syslog e CEF (Common Event Format);
2.47. Deve permitir centralmente a exibição de logs recebidos por um ou mais dispositivos, incluindo a capacidade de usar filtros para facilitar a pesquisa nos logs;
2.48. Os logs de auditoria das regras e alterações na configuração do objeto devem ser exibidos em uma lista diferente dos logs relacionados ao tráfego de dados;
2.49. Deve possuir um painel de operações que monitore as principais ameaças à segurança da sua rede;
2.50. Deve possuir um painel de operações que monitora o envolvimento do usuário e o uso suspeito da web em sua rede;
2.51. Deve possuir um painel de operações que monitora o tráfego da rede, aplicativos e sites web;
2.52. Deve possuir um painel de operações que monitoram a atividade da VPN em sua rede;
2.53. Deve possuir um painel de operações que monitoram o desempenho dos recursos locais da solução (CPU, Memória)
2.54. Deve permitir a criação de painéis personalizados para monitorar operações de segurança e rede;
2.55. Deve possuir relatório de uso de aplicações e mídias sociais;
2.56. Deve possuir relatório de prevenção de perda de dados (DLP);
2.57. Deve possuir relatório de VPN, Prevenção de Intrusão (IPS), análise de ameaças cibernéticas;
2.58. Deve possuir relatório diário resumido de eventos e incidentes de segurança;
2.59. Deve possuir um relatório de tráfego DNS e e-mail;
2.60. Deve possuir relatório das 10 principais aplicações utilizadas na rede;
2.61. Deve possuir relatório dos 10 principais sites web utilizados na rede;
2.62. Deve possibilitar a visibilidade da utilização do balanceamento inteligente de links (SD-WAN), mostrando informações de utilização das regras por aplicação, largura de banda e níveis de serviços dos links (latência, Jitter e descarte de pacotes);
2.63. Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados, o monitoramento de computadores que estão potencialmente comprometidas ou usuários com uso de rede suspeito;
2.64. Deve suportar através da análise de tráfego de rede IP, web (URL) e domínios visitados pelos computadores, atribuição de pontuações de risco que definem os vereditos dos níveis de comprometimento como baixo, médio ou alto;
2.65. Deve suportar a análise detalhada dos computadores comprometidos e exibir os detalhes das ameaças detectadas;
2.66. Deve suportar recursos de automação (playbooks) que, por meio de integrações com soluções de firewall, endpoint, Email, ITSM e eventos pré-determinados, possa tomar ações automáticas visando mitigar riscos;
2.67. Deve permitir a correlação de eventos, provendo painéis diversos, bem como possibilitar a criação de novas telas para visualizar os recursos de rede e segurança.
2.68. A solução de gerenciamento de logs e relatoria poderá ser ofertada em formato de appliance físico ou appliance virtual, e caso ofertado em formato virtual, será responsabilidade da contratante a disponibilização dos recursos de hardware e software (hypervisor) necessário para funcionamento da solução;
2.69. Caso a solução seja entregue em appliance virtual, deverá ser compatível com Hypervisors: VMware ESXi 6.5, Microsoft Hyper-V 2012 / 2016/ 2019 e KVM no Redhat 7.1 ou superiores;
2.70. Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;
2.70. Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;
2.72. Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;
2.73. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;

ITEM 3 - SOLUÇÃO DE CONTROLE DE ACESSO À REDE

3.1. Totalmente compatível com os modelos FortiGate 601E, FortiGate 201F e FortiGate 61F em uso no TRE
3.2. Solução de controle de acesso à rede, a ser ofertado em formato de appliance físico ou virtual, este que deverá estar disponível para as plataformas Vmware ESXi, AWS e Microsoft Azure;
3.3. Deve ser uma solução multi-vendor capaz de suportar os switches e concentrador VPN do orgão;
3.4. Deve suportar variadas soluções de Wi-Fi do mercado, tais como: Aruba, Ruckus, Cisco, Fortinet, Aerohive e Enterasys, pelo menos;
3.5. A solução deve suportar capacidade de expansão, sem demandar do cliente a troca do applianceVirtual;
3.6. A solução deve estar licenciada para operação com, pelo menos, 100 (cem) endpoints conectados simultaneamente;
3.7. A solução deve ser entregue em alta disponibilidade;
3.8. A solução deve ser capaz de inspecionar tanto IoT quanto estações/notebooks, sem depender de recursos como 802.1X e Mac-address bypass (MAB);
3.9. Para estações de trabalho, deve suportar verificação de compliance em VPN IPsec e SSL;
3.10. A licença contemplada deverá suportar todas as características exigidas neste termo de referência;
3.11. A solução deve permitir diferentes perfis de administração, com a capacidade de limitar e controlar a quantidade de acesso permitido às funcionalidades disponíveis, dependendo do grupo administrativo da organização ao qual o usuário pertence;
3.12. Deve detectar e classificar automaticamente o tipo dos dispositivos conectados na rede sem a necessidade de softwares instalados nos dispositivos;
3.13. Deve permitir determinar o perfil dos dispositivos descobertos por meio de métodos que não exigem a instalação de agentes, incluindo pelo menos os seguintes:
    3.13.1. Consultas em DHCP Fingerprint;
    3.13.2. Consultas via protocolos HTTP/HTTPS;
    3.13.3. Consultas via protocolo SNMP;
    3.13.4. Consultas via protocolo SSH;
    3.13.5. Consultas via protocolo Telnet;
    3.13.6. Consultas de portas TCP;
    3.13.7. Consultas de portas UDP;
    3.13.8. MAC OUI;
    3.13.9. Consultas via protocolo WMI;
    3.13.10. Protocolo ONVIF;
    3.13.11. Protocolo NetFlow;
    3.13.12. Base assinaturas pré-definidas;
3.14. A solução deve ser capaz de reconhecer as seguintes informações sobre os dispositivos conectados à rede:
    3.14.1. Endereço MAC;
    3.14.2. Endereço IP;
    3.14.3. Sistema operacional;
    3.14.4. Nome do host;
    3.14.5. Horário de conexão;
    3.14.6. Usuário conectado;
    3.14.7. Localização.
3.15. A solução deve ser capaz de reconhecer os seguintes sistemas operacionais em execução nos dispositivos conectados à rede:
    3.15.1. Android;
    3.15.2. Apple iOS para iPhone, iPod e iPad;
    3.15.3. Chrome OS;
    3.15.4. Linux;
    3.15.5. MacOS X;
    3.15.6. Windows 7, 8, 10 e 11;
3.16. Deve lembrar o perfil atribuído a cada dispositivo e verificar sua validade a cada conexão;
3.17. Deve permitir a designação de um sponsor para autorizar a categorização dos dispositivos;
3.18. Deve permitir a recategorização periódica de dispositivos;
3.19. Deve permitir a importação de um arquivo CSV contendo informações sobre os dispositivos a serem registrados;
3.20. A solução deve incluir a detecção de dispositivos desconhecidos conectados à rede e adotar medidas de controle para limitar o acesso;
3.21. A solução deve suportar autenticação através de EAP-PEAP e EAP-TLS;
3.22. A solução deve suportar RADIUS Change of Authorization;
3.23. A solução deve suportar MAC Address Bypass;
3.24. A solução deve consultar bases LDAP e Active Directory para a identificação de usuários e grupos de usuários;
3.25. A solução deve permitir a criação de políticas de controle que combinem informações sobre a identidade do usuário e tipo de dispositivo com objetivo de autorizar dinâmicamente o acesso à rede;
3.26. Deve permitir a definição dos horários em que os dispositivos serão autorizados a conectar na rede;
3.27. Deve garantir a segmentação dinâmica da rede e aplicação de políticas de segurança, tendo como base variadas combinações, como login do AD e atributos (departamento, cidade, email, telefone), características da máquina (asset tag, hostname), localidade e horário;
3.28. A solução deve incluir recursos de gerenciamento de visitantes, permitindo a criação de diferentes perfis de utilização e autorização a serem associados aos usuários, distinguindo por exemplo prestadores de serviços dos visitantes;
3.29. A solução deve permitir o cadastro dos usuários visitantes na base interna da ferramenta para que não seja necessário realizar consultas em bases externas;
3.30. A solução deve possuir ferramenta que permita a geração automática de credenciais para usuários visitantes com login e respectivas senhas;
3.31. A solução deve possuir ferramenta que permita a criação de credenciais para eventos;
3.32. Deve permitir a definição de complexidade da senha dos usuários visitantes;
3.33. Deve ser possível definir um período de validade para as contas de usuários visitantes;
3.34. Deve ser possível definir data e horário para início e encerramento das contas de usuários visitantes;

3.35. A autenticação e autorização dos usuários visitantes deve ocorrer através de portal captivo acessível via browser web;
3.36. Os visitantes em hipótese alguma deverão ter acesso à Internet e rede interna antes que a autenticação seja concluída e o usuário seja autorizado;
3.37. A solução deve vincular o login do visitante à máquina utilizada no acesso;
3.38. Deve suportar a validação de credenciais:
- 3.38.1.. Em base local interna à ferramenta;
- 3.38.2. Em servidores RADIUS;
- 3.38.3. Em servidores LDAP.

3.39. A solução deve autenticar usuários visitantes através das seguintes redes sociais: Facebook, LinkedIn e Twitter;
3.40. A ferramenta deve permitir que os usuários visitantes possam realizar auto-registro através do preenchimento de cadastro disponível em portal web;
3.41. Deve permitir a customização dos campos obrigatórios e opcionais para o cadastro de auto-registro;
3.42. A solução deve suportar o envio da senha de acesso aos visitantes através de SMS e e-mail;
3.43. Deve ser possível definir um período para que os usuários visitantes sejam obrigados a se reautenticar;
3.44. Deve permitir a designação de grupos de usuários com função de sponsor que ficarão responsáveis por autorizar o acesso dos usuários visitantes e prestadores de serviços;
3.45. Os usuários do tipo sponsor poderão cadastrar previamente um usuário visitante. O portal de cadastro e gerenciamento de usuários visitantes não deve permtir gerência administrativa dos demais recursos da solução;
3.46. A solução deve permitir a customização da aparência do captive portal, permitindo editar textos e inserir imagens;
3.47. Os usuários do tipo sponsor podem ser cadastrados na base local da ferramenta ou fazer parte de grupo de usuários em base LDAP/Active Directory;
3.48. A solução deve incluir recursos de conformidade de endpoint. Antes de permitir que os dispositivos acessem a rede, a solução deve garantir que estes cumpram requisitos de segurança, integridade e conformidade;
3.49. Deve permitir o uso de software agente instalado no dispositivo e agentes evanescentes que não precisam ser instalados;
3.50. Tanto para IoTs quanto para estações de trabalho, se configurado, não devem ter qualquer acesso à rede de produção enquanto não forem inspecionados e identificados;
3.51. Se um dispositivo não passar os testes de conformidade, deve ser possível:
3.52. Não forçar a remediação;
3.53. Forçar a remediação imediatamente enviando o dispositivo à rede de quarentena;
3.54. Permitir a remediação retardada, ou seja, dando um período de tolerância para que o usuário corrija o problema. Caso os problemas persistam, o dispositivo deve ser colocado em quarentena;
3.55. A solução deve permitir verificações de conformidade em endpoints que façam uso do sistema operacional:
- 3.55.1. Windows 7;
- 3.55.2. Windows 8;
- 3.55.3. Windows 10;
- 3.55.4. Windows 11;
- 3.55.5. MacOS;
- 3.55.6. Linux.

3.56. Para garantir a conformidade com as políticas de segurança, a solução deve permitir que sejam verificados os seguintes itens antes de autorizar o acesso de um endpoint na rede:
3.56.1. Presença de software de anti-vírus instalado e em execução;
3.56.2. Versão do sistema operacional;
3.56.3. Nome de domínio do Active Directory ao qual a estação Windows pertença;
3.56.4. Serviços em execução para estações Windows;
3.56.5. Informações sobre um determinado certificado digital em estações Windows;
3.56.6. Registros ou chaves de registro para estações Windows;
3.56.7. Processos em execução para estações Windows, Linux e MacOS;
3.56.8. Arquivo armazenado em um determinado diretório para estações Windows, Linux e MacOS;
3.56.9. Pacotes instalados em estações Linux e MacOS.
3.57. A solução deve ser capaz de monitorar quando um serviço requirido for desabilitado ou interrompido em computadores. Além disso deve enviar a estação para quarentena de forma a garantir a conformidade com a política de segurança;
3.58. Deve possuir serviço RADIUS interno, além de permitir o uso de RADIUS externos;
3.59. Deve permitir a distribuição de agentes através de, pelo menos, os seguintes métodos:
3.60. Programas de gerenciamento e distribuição de software;
3.61. GPO do Active Directory;
3.62. Captive Portal;
3.63. Deve permitir a atualização automática ou programada dos agentes instalados nas máquinas;
3.64. O agente instalado nos computadores deve notificar os usuários com mensagens informativas em casos de eventos;
3.65. Quando em quarentena, um portal web deve ser apresentado aos usuários com informações sobre as razões pelas quais estes foram movidos para o isolamento;
3.66. A solução deve compartilhar a identificação dos usuários e/ou dispositivos autenticados para a plataforma de segurança da rede via SSO, de forma que sejam vinculadas aos acessos de Internet, provendo rastreabilidade futura;
3.67. No que tange compliance, quando houver sucesso, falha ou alerta, a solução deve permitir as seguintes ações: alerta, envio de email e SMS, desabilitar o host, envio de mensagem direta para o host envolvido e executar políticas adicionais de compliance;
3.68. A solução deve integrar com plataformas de MDM, suportando pelo menos: FortiClient, In Tune, Mobile Iron e Air Watch;
3.69. Deve suportar integração com soluções de patching;
3.70. Deve suportar integração com soluções de análise de vulnerabilidades;
3.71. A solução deve possuir dashboard que apresente informações e estatísticas relevantes de forma resumida;
3.72. A solução deve permitir a customização do dashboard para apresentar as informações que o administrador considera relevante;

3.73. A solução deve permitir a consulta de informações e alteração de parâmetros de configuração via REST API;
3.74. A solução deve armazenar os eventos internamente e permitir que sejam exportados;
3.75. A solução deve permitir a exportação dos eventos através de syslog;
3.76. Deve suportar alta disponibilidade, suportando todos os registros e autenticações caso um nó da solução esteja indisponível;
3.77. A solução deve ser capaz de isolar hosts na quarentena mesmo quando estes estão conectados em redes de localidades remotas, tais como filiais. Não deve ser necessário estender a VLAN para isso;
3.78. Deve possibilitar o rastreio de dispositivos, notificando a localização dos mesmos quando se conectarem à rede;
3.79. Caso o CONTRATANTE não tenha solução de logs compatível com o NAC ofertado, cabe ao fornecedor inclui-la na proposta, sem ônus, considerando licenciamento e/ou hardware adequado para retenção dos logs;
3.80. Dentre os relatórios disponibilizados pela solução dedicada de logs, deve suportar relatórios listando os endpoints por localidade e fabricante, usuários associados, além de relatórios de inventário, devices registrados e rogues;

ITEM 4 - SWITCH CORE

4.1. O equipamento deve ser do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
4.2. Deve ser compatível e gerenciado com os "Firewall de Próxima Geração (NGFW)" FortiGate 601E, FortiGate 201F e FortiGate 61F em uso no TRE-AP;
4.3. Deve possuir 24 (vinte e quatro) portas SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 10GbE;
4.4. Adicionalmente, deve possuir no mínimo 2 (dois) slots QSFP+ para conexão de fibras ópticas do tipo 40GBase-SR4 operando 40GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do subitem anterior;
4.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
4.6. Deve possuir 1 (uma) interface USB;
4.7. Deve possuir capacidade de comutação de pelo menos 850 Gbps e ser capaz de encaminhar até 1300 Mbps (milhões de pacotes por segundo);
4.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
4.9. Deve possuir tabela MAC com suporte a 60.000 endereços;
4.10. Deve implementar Flow Control baseado no padrão IEEE 802.3X;
4.11. Deve suportar Q-in-Q, recurso também conhecido como Stacked VLAN ou VLAN sobre VLAN em que é possível configurar duas TAGs de VLAN no mesmo frame;
4.12. Deve operar com latência igual ou inferior à 1us (microsegundo);
4.13. Deve implementar Flow Control baseado no padrão IEEE 802.3X;
4.14. Em conjunto com o Flow Control (IEEE 802.3x) o switch deverá, ao invés de enviar pause frames, definir um limite de banda que poderá ser recebida na interface quando o buffer estiver cheio. O switch deverá medir o volume de utilização do buffer para que o recebimento seja restaurado à capacidade máxima automaticamente;
4.15. Deve ser capaz de implementar e orquestrar políticas de segurança de micro segmentação nos switches controlando como os usuários/endpoints se comunicam lateralmente entre si;
4.16. Deve suportar o padrão IEEE 802.1Qbb (Priority-based Flow Control);
4.17. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);
4.18. Deve suportar Multi-Chassis Link Agregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos switches como uma única interface lógica;
4.19. Deve suportar a comutação de Jumbo Frames;
4.20. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
4.21. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
4.21. Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIP, BGP, OSPF em IPv4 e OSPF em IPv6. É obrigatória a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos;
4.22. Deve possuir hardware capaz de suportar roteamento multicast através do protocolo PIM-SSM (Protocol Independent Multicast - Source-Specific Multicast). É obrigatória a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos;
4.23. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É obrigatória a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;
4.24. Deve suportar Bidirectional Forwarding Detection (BFD). É obrigatória a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;
4.25. Deve ser capaz de criar múltiplas tabelas de roteamento através de VRF (Virtual Routing and Forwarding). É obrigatória a entrega de licenças caso o software exija licenciamento adicional para ativação deste recurso;
4.26. Deve implementar serviço de DHCP Server e DHCP Relay;
4.27. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) grupos;
4.28. Deve suportar MLD (Multicast Listener Discovery) Snooping para otimizar a transmissão de tráfego multicast em IPv6;
4.29. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN);
4.30. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN;
4.31. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 30 (trinta) instâncias de Multiple Spanning Tree;
4.32. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;
4.33. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;
4.34. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
4.35. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

4.37. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;
4.38. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;
4.39. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;
4.40. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
4.41. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
4.42. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;
4.43. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ);
4.44. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
4.45. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;
4.46. Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement;
4.47. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
4.48. Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
4.49. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;
4.50. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;
4.51. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
4.52. Deve suportar MAC Authentication Bypass (MAB);
4.53. Deve implementar RADIUS CoA (Change of Authorization);
4.54. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
4.55. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;
4.56. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
4.57. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;
4.58. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
4.59. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
4.60. Deve suportar o protocolo PTP (Precision Time Protocol);
4.61. Deve implementar Netflow, sFlow ou similar;
4.62. Deve suportar o envio de mensagens de log para servidores externos através de syslog;
4.63. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
4.64. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
4.65. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
4.66. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
4.67. Deve permitir ser gerenciado através de IPv6;
4.68. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
4.69. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
4.70. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
4.71. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab
4.72. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
4.73. Deverá suportar ser configurado e monitorado através de REST API;
4.74. Deve possuir ferramenta para captura de pacotes que auxíliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark;
4.75. Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash;
4.76. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
4.77. Deve suportar temperatura de operação de até 40º Celsius;
4.78. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
4.79. Deve ser fornecido com fontes de alimentação redundantes do tipo hot-swap, com capacidade para operar em tensões de 110V e 220V;
4.80. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;
4.81. Deve ser compatível e gerenciado pelo Item 01 deste termo de referência ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

4.81.1. A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo disrupção do serviço mediante a falha de um elemento;
4.81.2. Deverá implementar mecanismos de SDN (Software Defined Networking) que permitam efetuar macro-segmentação (zonas de segurança) e microsegmentação: controle e orquestração de como usuários se comunicam numa mesma VLAN/zona;
4.81.3. Deve operar como ponto central para automação e gerenciamento dos switches;

4.81.4. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;
4.81.5. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;
4.81.6. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;
4.81.7. Deve montar a topologia da rede de maneira automática;
4.81.8. Deve ser capaz de configurar os switches da rede;
4.81.9. Deve através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;
4.81.10. Deve através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
4.81.11. Deve através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
4.81.12. Deve através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
4.81.13. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
4.81.14. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;
4.81.15. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
4.81.16. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
4.81.17. Deve ser capaz de configurar parâmetros SNMP dos switches;
4.81.18. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;
4.81.19. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
4.81.20. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches;
4.81.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
4.81.22. Deve prover indicadores de saúde dos elementos críticos do ambiente;
4.81.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
4.81.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;
4.81.25. Deve possuir API no formato REST

ITEM 5 - SWITCH DE DISTRIBUIÇÃO

5.1. O equipamento deve ser do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
5.2. Deve ser compatível e gerenciado com os “Firewall de Próxima Geração (NGFW)" FortiGate 601E, FortiGate 201F e FortiGate 61F em uso no TRE-AP;
5.3. Deve possuir 24 (vinte e quatro) portas SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 10GbE;
5.4. Adicionalmente, deve possuir no mínimo 2 (dois) slots QSFP+ para conexão de fibras ópticas do tipo 40GBase-SR4 operando 40GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do subitem anterior;
5.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
5.6. Deve possuir 1 (uma) interface USB;
5.7. Deve possuir capacidade de comutação de pelo menos 850 Gbps e ser capaz de encaminhar até 1300 Mbps (milhões de pacotes por segundo);
5.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
5.9. Deve possuir tabela MAC com suporte a 60.000 endereços;
5.10. Deve implementar Flow Control baseado no padrão IEEE 802.3X;
5.11. Deve suportar Q-in-Q, recurso também conhecido como Stacked VLAN ou VLAN sobre VLAN em que é possível configurar duas TAGs de VLAN no mesmo frame;
5.12. Deve operar com latência igual ou inferior à 1us (microsegundo);
5.13. Deve implementar Flow Control baseado no padrão IEEE 802.3X;
5.14. Em conjunto com o Flow Control (IEEE 802.3x) o switch deverá, ao invés de enviar pause frames, definir um limite de banda que poderá ser recebida na interface quando o buffer estiver cheio. O switch deverá medir o volume de utilização do buffer para que o recebimento seja restaurado à capacidade máxima automaticamente;
5.15. Deve ser capaz de implementar e orquestrar políticas de segurança de micro segmentação nos switches controlando como os usuários/endpoints se comunicam lateralmente entre si;
5.16. Deve suportar o padrão IEEE 802.1Qbb (Priority-based Flow Control);
5.17. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);
5.18. Deve suportar Multi-Chassis Link Agregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos switches como uma única interface lógica;
5.19. Deve suportar a comutação de Jumbo Frames;
5.20. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
5.21. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
5.21. Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIP, BGP, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação dos protocolos;
5.22. Deve possuir hardware capaz de suportar roteamento multicast através do protocolo PIM-SSM (Protocol Independent Multicast - Source-Specific Multicast). É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação dos protocolos;

5.23. Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação do protocolo;
5.24. Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação do protocolo;
5.25. Deve ser capaz de criar múltiplas tabelas de roteamento através de VRF (Virtual Routing and Forwarding). É facultada a entrega de licenças caso o software exiga licenciamento adicional para ativação deste recurso;
5.26. Deve implementar serviço de DHCP Server e DHCP Relay;
5.27. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) grupos;
5.28. Deve suportar MLD (Multicast Listener Discovery) Snooping para otimizar a transmissão de tráfego multicast em IPv6;
5.29. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN);
5.30. Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN;
5.31. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 30 (trinta) instâncias de Multiple Spanning Tree;
5.32. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;
5.33. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;
5.34. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
5.35. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;
5.36. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;
5.37. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;
5.38. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;
5.39. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
5.40. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
5.41. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;
5.42. Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ);
5.43. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
5.44. Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados;
5.45. Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement;
5.46. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
5.47. Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
5.48. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;
5.49. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;
5.50. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
5.51. Deve suportar MAC Authentication Bypass (MAB);
5.52. Deve implementar RADIUS CoA (Change of Authorization);
5.53. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
5.54. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;
5.55. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
5.56. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;
5.57. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
5.58. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
5.59. Deve suportar o protocolo PTP (Precision Time Protocol);
5.60. Deve implementar Netflow, sFlow ou similar;
5.61. Deve suportar o envio de mensagens de log para servidores externos através de syslog;
5.62. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
5.63. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
5.64. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
5.65. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
5.66. Deve permitir ser gerenciado através de IPv6;
5.67. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
5.68. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

5.69. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
5.70. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab
5.71. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
5.72. Deverá suportar ser configurado e monitorado através de REST API;
5.73. Deve possuir ferramenta para captura de pacotes que auxiliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark;
5.74. Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash;
5.75. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
5.76. Deve suportar temperatura de operação de até 40º Celsius;
5.77. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
5.78. Deve ser fornecido com fontes de alimentação redundantes do tipo hot-swap, com capacidade para operar em tensões de 110V e 220V;
5.79. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;
5.80. Deve ser compatível e gerenciado pelo Item 01 deste termo de referência ou por solução do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

5.80.1. A solução de gerência centralizada deve suportar operação com elementos redundantes, não havendo disrupção do serviço mediante a falha de um elemento;
5.80.2. Deverá implementar mecanismos de SDN (Software Defined Networking) que permitam efetuar macro-segmentação (zonas de segurança) e microsegmentação: controle e orquestração de como usuários se comunicam numa mesma VLAN/zona;
5.80.3. Deve operar como ponto central para automação e gerenciamento dos switches;
5.80.4. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;
5.80.5. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;
5.80.6. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;
5.80.7. Deve montar a topologia da rede de maneira automática;
5.80.8. Deve ser capaz de configurar os switches da rede;
5.80.9. Deve através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;
5.80.10. Deve através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
5.80.11. Deve através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
5.80.12. Deve através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
5.80.13. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
5.80.14. Deve através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;
5.80.15. Deve através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
5.80.16. A solução de gerência centralizada deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
5.80.17. Deve ser capaz de configurar parâmetros SNMP dos switches;
5.80.18. A solução de gerência centralizada deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;
5.80.19. A solução de gerência centralizada deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
5.80.20. A solução de gerência centralizada deve apresentar graficamente informações sobre erros nas interfaces dos switches;
5.80.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
5.80.22. Deve prover indicadores de saúde dos elementos críticos do ambiente;
5.80.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
5.80.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;
5.80.25. Deve possuir API no formato REST

ITEM 6 - SWITCH DE ACESSO - TIPO 1 (48 PORTAS)

6.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
6.2. Deve ser compatível e gerenciado com os “Firewalls de Próxima Geração (NGFW)" FortiGate 601E, FortiGate 201F e FortiGate 61F em uso no TRE-AP;
6.3. Deve possuir 48 (quarenta e oito) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);
6.4. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;
6.5. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W em 24 portas;
6.6. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
6.7. Deve possuir 1 (uma) interface USB;

6.8. Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo);
6.9. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
6.10. Deve possuir tabela MAC com suporte a 32.000 endereços;
6.11. Deve operar com latência igual ou inferior à 1us (microsegundo);
6.12. Deve implementar Flow Control baseado no padrão IEEE 802.3X;
6.13. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);
6.14. Deve suportar a comutação de Jumbo Frames;
6.15. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;
6.16. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
6.17. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
6.18. Deve implementar serviço de DHCP Relay;
6.19. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;
6.20. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);
6.21. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;
6.22. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;
6.23. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;
6.24. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
6.25. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;
6.26. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;
6.27. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;
6.28. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;
6.29. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
6.30. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
6.31. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;
6.32. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
6.33. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
6.34. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
6.35. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;
6.36. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;
6.37. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
6.38. Deve suportar MAC Authentication Bypass (MAB);
6.39. Deve implementar RADIUS CoA (Change of Authorization);
6.40. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
6.41. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;
6.42. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
6.43. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;
6.44. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
6.45. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
6.46. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;
6.47. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);
6.48. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;
6.49. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
6.50. Deve suportar o envio de mensagens de log para servidores externos através de syslog;
6.51. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
6.52. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
6.53. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
6.54. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
6.55. Deve permitir ser gerenciado através de IPv6;
6.56. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

6.57. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
6.58. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
6.59. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
6.60. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;
6.61. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
6.62. Deverá suportar ser configurado e monitorado através de REST API;
6.63. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
6.64. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
6.65. Deve suportar temperatura de operação de até 45º Celsius;
6.66. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
6.67. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
6.68. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

ITEM 7 - SWITCH DE ACESSO - TIPO 2 (24 PORTAS)
7.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
7.2. Deve ser compatível e gerenciado com os “Firewalls de Próxima Geração (NGFW)" FortiGate 601E, FortiGate 201F e FortiGate 61F em uso no TRE-AP;
7.3. Deve possuir 24 (VINTE E QUATRO) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);
7.4. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;
7.5. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 185W em 12 portas;
7.6. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;
7.7. Deve possuir 1 (uma) interface USB;
7.8. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 190 Mpps (milhões de pacotes por segundo);
7.9. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
7.10. Deve possuir tabela MAC com suporte a 32.000 endereços;
7.11. Deve operar com latência igual ou inferior à 1us (microsegundo);
7.12. Deve implementar Flow Control baseado no padrão IEEE 802.3X;
7.13. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);
7.14. Deve suportar a comutação de Jumbo Frames;
7.15. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;
7.16. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
7.17. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
7.18. Deve implementar serviço de DHCP Relay;
7.19. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;
7.20. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);
7.21. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;
7.22. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;
7.23. Deve implementar mecanismo de proteção da “root bridge” do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo “Denial of Service” no ambiente nível 2;
7.24. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo “fast forwarding” (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;
7.25. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;
7.26. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;
7.27. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;
7.28. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;
7.29. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
7.30. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
7.31. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;
7.32. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
7.33. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

7.34. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
7.35. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;
7.36. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;
7.37. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
7.38. Deve suportar MAC Authentication Bypass (MAB);
7.39. Deve implementar RADIUS CoA (Change of Authorization);
7.40. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
7.41. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;
7.42. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
7.43. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;
7.44. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
7.45. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
7.46. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;
7.47. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);
7.48. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;
7.49. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
7.50. Deve suportar o envio de mensagens de log para servidores externos através de syslog;
7.51. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
7.52. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
7.53. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
7.54. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
7.55. Deve permitir ser gerenciado através de IPv6;
7.56. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
7.57. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
7.58. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
7.59. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
7.60. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;
7.61. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
7.62. Deverá suportar ser configurado e monitorado através de REST API;
7.63. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
7.64. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
7.65. Deve suportar temperatura de operação de até 45º Celsius;
7.66. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
7.67. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
7.68. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;

ITEM 8 - ACCESS POINT

8.1. Ponto de acesso (AP) que permita acesso dos dispositivos à rede através da rede sem fio e que possua todas as suas configurações centralizadas em controlador sem fio;
8.2. Deve ser compatível e gerenciado pelo Firewall de Próxima Geração (NGFW), mais especificamente em relação aos modelos FortiGate 601E, FortiGate 201F e FortiGate 61F;
8.3. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;
8.4. Deve identificar automaticamente o controlador wireless ao qual se conectará;
8.5. Deve permitir ser gerenciado remotamente através de links WAN;
8.6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;
8.7. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;
8.8. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;
8.9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;
8.10. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;
8.11. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;
8.12. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;
8.13. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

8.14. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC;
8.15. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;
8.16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;
8.17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
8.18. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;
8.19. Deve permitir operação em modo Mesh;
8.20. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;
8.21. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;
8.22. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);
8.23. Deve suportar OFDMA;
8.24. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;
8.25. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;
8.26. Deve suportar BSS Coloring;
8.27. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;
8.28. Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20);
8.29. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz;
8.30. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;
8.31. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
8.32. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;
8.33. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;
8.34. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);
8.35. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;
8.36. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
8.37. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;
8.38. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
8.39. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
8.40. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
8.41. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
8.42. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
8.43. Deve implementar o padrão IEEE 802.11e;
8.44. Deve implementar o padrão IEEE 802.11h;
8.45. Deve implementar o padrão IEEE 802.3az;
8.46. Deve suportar ser gerenciado via SNMP;
8.47. Deve suportar consultas via REST API;
8.48. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;
8.49. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;
8.50. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;
8.51. Deve possuir indicadores luminosos (LED) para indicação de status;
8.52. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;
8.53. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
8.54. Deve possuir certificado emitido pela Wi-Fi Alliance;
8.55. Deve estar homologado pela ANATEL na data de execução do pregão.

ITEM 9 - FIREWALL DE NOVA GERAÇÃO (NGFW)

9.1 A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração;
9.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

9.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
9.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
9.5. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;
9.6. Deverá possuir e estar licenciado pelo período de 60 (sessenta) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização;
9.7. FUNCIONALIDADES DE REDE E FIREWALL
9.7.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
9.7.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;
9.7.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
9.7.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;
9.7.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
9.7.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (*Network Address Translation*), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;
9.7.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
9.7.8. Deverá suportar sFlow ou Netflow;
9.7.9. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
9.7.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;
9.7.11. Deve suportar o protocolo padrão da indústria VXLAN;
9.7.12. Deve implementar o protocolo ECMP;
9.7.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
9.7.14. Enviar log para sistemas de monitoração externos;
9.7.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
9.7.16. Deve possui mecanismos de proteção anti-spoofing;
9.7.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);
9.7.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
9.7.19. Suportar OSPF graceful restart;
9.7.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
9.7.21. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
9.7.22. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
9.7.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
9.7.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs eTabelas FIB;
9.7.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
9.7.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;
9.7.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;
9.7.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;
9.7.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
9.7.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
9.7.31. Deverá suportar controle por zonas de segurança;
9.7.32. Deverá suportar controles de políticas por porta e protocolo;
9.7.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
9.7.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
9.7.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
9.7.36. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);
9.7.37. Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
9.7.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
9.7.39. Suporte a objetos e regras IPV6;
9.7.40. Suporte a objetos e regras multicast;
9.7.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.
9.8. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES
9.8.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
9.8.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
9.8.3. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
9.8.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
9.8.5. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2,

mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;

9.8.6. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;

9.8.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;

9.8.8. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

9.8.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação;

9.8.10. Identificar o uso de táticas evasivas via comunicações criptografadas;

9.8.11. Atualizar a base de assinaturas de aplicações automaticamente;

9.8.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

9.8.13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

9.8.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;

9.8.15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;

9.8.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

9.8.17. Deve alertar o usuário quando uma aplicação for bloqueada;

9.8.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;

9.8.19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;

9.8.20. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;

9.8.21. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;

9.8.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

9.8.23. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;

9.8.24. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;

9.8.25. Deve permitir forçar o uso de portas específicas para determinadas aplicações.

9.9. FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS

9.9.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

9.9.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

9.9.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

9.9.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e quarentenar IP do atacante por um intervalo de tempo;

9.9.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

9.9.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

9.9.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

9.9.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

9.9.9. Deve permitir o bloqueio de vulnerabilidades;

9.9.10. Deve permitir o bloqueio de exploits conhecidos;

9.9.11. Deve incluir proteção contra-ataques de negação de serviços;

9.9.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

9.9.13. Detectar e bloquear a origem de portscans;

9.9.14. Bloquear ataques efetuados por worms conhecidos;

9.9.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

9.9.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;

9.9.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

9.9.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

9.9.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

9.9.20. Identificar e bloquear comunicação com botnets;

9.9.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;

9.9.22. Os eventos devem identificar o país de onde partiu a ameaça;

9.9.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

9.9.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

9.9.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

9.9.26. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante

9.9.27. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;

9.9.28. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos.

9.10. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS

9.10.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

9.10.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

9.10.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

9.10.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;

9.10.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

9.10.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;

9.10.7. Possuir pelo menos 70 (setenta) categorias de URLs;

9.10.8. Deve possuir a função de exclusão de URLs do bloqueio;

9.10.9. Permitir a customização de página de bloqueio;

9.10.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;

9.10.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;

9.10.12. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;

9.10.13. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

9.11. FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS

9.11.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;

9.11.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

9.11.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;

9.11.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

9.11.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

9.11.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

9.11.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

9.11.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

9.11.9. Deve suportar o envio e recebimento de credenciais via RADIUS;

9.11.10. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

9.12. FUNCIONALIDADE DE FILTRO DE DADOS

9.12.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);

9.12.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

9.12.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

9.12.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

9.13. FUNCIONALIDADE DE GEOLOCALIZAÇÃO

9.13.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

9.13.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

9.14. FUNCIONALIDADE DE VPN

9.14.1. Suportar VPN Site-to-Site e Cliente-To-Site;

9.14.2. Suportar IPSec VPN;

9.14.3. Suportar SSL VPN;

9.14.4. A VPN IPSEc deve suportar 3DES;

9.14.5. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;

9.14.6. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

9.14.7. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

9.14.8. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

9.14.9. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI

9.14.10. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
9.14.11. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
9.14.12. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
9.14.13. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
9.14.14. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
9.14.15. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
9.14.16. Atribuição de DNS nos clientes remotos de VPN;
9.14.17. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
9.14.18. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
9.14.19. Suportar leitura e verificação de CRL (Certificate Revocation List);
9.14.20. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
9.14.21. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;
9.14.22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;
9.14.23. Deverá manter uma conexão segura com o portal durante a sessão;
9.14.24. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior).

9.15. FUNCIONALIDADE DE QOS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

9.15.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como Youtube e redes sociais, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming;
9.15.2. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:
9.15.3.1. Endereço de origem;
9.15.3.2. Endereço de destino;
9.15.3.3. Usuário e grupo;
9.15.3.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
9.15.3.5. Por porta.
9.15.8. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
9.15.9. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como YouTube, Facebook, entre outros;
9.15.10. O QoS deve possibilitar a definição de fila de prioridade;
9.15.11. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
9.15.12. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
9.15.13. Suportar modificação de valores DSCP para o Diffserv;
9.15.14. Suportar priorização de tráfego usando informação de ToS (Type of Service);
9.15.15. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
9.15.16. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;
9.15.17. Deve possibilitar a definição de bandas distintas para download e upload.

9.16. FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS

9.16.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
9.16.2. A solução deve ser capaz de agregar vários links em uma interface virtual;
9.16.3. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);
9.16.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;
9.16.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;
9.16.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);
9.16.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).
9.16.8. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:
9.16.9. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.
9.16.10. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;

9.16.11. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;
9.16.12. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;
9.16.13. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;
9.16.14. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);
9.16.15. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);
9.16.16. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;
9.16.17. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;
9.16.18. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;
9.16.19. A solução deve possuir recurso para controlar e corrigir erros (FEC) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;
9.16.20. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;
9.16.21. A solução deve suportar nativamente conectores com clouds públicas;
9.16.22. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;
9.16.23. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);
9.16.24. Deve implementar balanceamento de link por hash do IP de origem;
9.16.25. Deve implementar balanceamento de link por hash do IP de origem e destino;
9.16.26. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;
9.16.27. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;
9.16.28. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

9.17. FUNCIONALIDADE DE CONTROLADOR DE REDE SEM FIO

9.17.1. A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste termo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:
9.17.2. Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;
9.17.3. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;
9.17.4. A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;
9.17.5. Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
9.17.6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;
9.17.7. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
9.17.8. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;
9.17.9. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;
9.17.10. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;
9.17.11. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;
9.17.12. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;
9.17.13. A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;
9.17.14. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
9.17.15. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

9.17.16. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;
9.17.17. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;
9.17.18. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baeada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;
9.17.19. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;
9.17.20. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;
9.17.21. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;
9.17.22. A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;
9.17.23. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
9.17.24. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;
9.17.25. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
9.17.26. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
9.17.27. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
9.17.28. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;
9.17.29. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;
9.17.30. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
9.17.31. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
9.17.32. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
9.17.33. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;
9.17.34. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;
9.17.35. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;
9.17.36. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;
9.17.37. A solução deve suportar a configuração do BLE (Blueooth Low Energy) nos pontos de acesso que tenham este recurso;
9.17.38. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;
9.17.39. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;
9.17.40. A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;
9.17.41. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;
9.17.42. A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;
9.17.43. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;
9.17.44. A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;
9.17.45. Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;
9.17.46. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
9.17.47. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
9.17.48. A solução deve permitir a configuração de múltplas chaves de autenticação PSK para utilização em um determinado SSID;
9.17.49. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

9.17.50. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;
9.17.51. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;
9.17.52. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
9.17.53. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;
9.17.54. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
9.17.55. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;
9.17.56. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
9.17.57. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
9.17.58. A solução deve permitir a configuração do captive portal com endereço IPv6;
9.17.59. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;
9.17.60. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;
9.17.61. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
9.17.62. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;
9.17.63. A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;
9.17.64. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
9.17.65. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado;
9.17.66. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
9.17.67. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
9.17.68. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;
9.17.69. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
9.17.70. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
9.17.71. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;
9.17.72. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
9.17.73. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);
9.17.74. A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;
9.17.75. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;
9.17.76. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;
9.17.77. A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
9.17.78. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
9.17.79. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;
9.17.80. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;
9.17.81. A solução deve possuir ferramentas de diagnósticos e debug;
9.17.82. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;
9.17.83. A solução deve suportar comunicação com elementos externos através de REST API;
9.17.84. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo.

9.18. FUNCIONALIDADE DE CONTROLADOR DE REDE CABEADA

9.18.1. Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:
9.18.2. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;
9.18.3. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;
9.18.4. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;
9.18.5. Deve montar a topologia da rede de maneira automática;
9.18.6. Deve ser capaz de configurar os switches da rede;
9.18.7. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;
9.18.8. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
9.18.9. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

9.18.10. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
9.18.11. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;
9.18.12. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
9.18.13. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;
9.18.14. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
9.18.15. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
9.18.16. Deve ser capaz de configurar parâmetros SNMP dos switches;
9.18.17. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;
9.18.18. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
9.18.19. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;
9.18.20. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;
9.18.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
9.18.22. Deve prover indicadores de saúde dos elementos críticos do ambiente;
9.18.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
9.18.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede.

9.19. CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE

9.19.1. Solução baseada em appliance. Para maior segurança, não serão aceitos equipamentos de propósito genérico (PCs ou servidores) sobre os quais poderiam instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN Solaris, Apple OS-X ou GNU/Linux;
9.19.2. Poderá ser entregue em equipamento único ou com composição de equipamentos.
9.19.3. Deverá possuir licenças de Garantia, Atualizações de firmware, VPN, SD-WAN, pelo período exigido;
9.19.4. Capacidade mínima:
9.19.4.1. Firewall com capacidade mínima de processamento de 6 (seis) Gbps;
9.19.4.2. IPS com capacidade mínima de processamento de 1.4 Gbps;
9.19.4.3. Proteção a ameaças avançadas (Threat Protection) com capacidade mínima de processamento de 680 (seiscentos e oitenta) Mbps;
9.19.4.4. Inspeção SSL Throughput com capacidade mínima de processamento de 600 (seiscentos) Mbps;
9.19.4.5. VPN com capacidade de, pelo menos, 6 (seis) Gbps de tráfego IPSec;
9.19.4.6. VPN SSL com capacidade de, pelo menos, 900 (novecentos) Mbps de tráfego;
9.19.4.7. Deverá suportar 650.000 (seiscentos e cinquenta mil) conexões simultâneas;
9.19.4.8. Deverão ser licenciados para suportar, pelo menos, 150 (cento e cinquenta) usuários de VPN SSL;
9.19.4.9. Deverá suportar, pelo menos, 33.000 (trinta e três mil) novas conexões por segundo;
9.19.4.10. Deverá suportar, pelo menos, 190 (cento e noventa) túneis de VPN Site-Site;
9.19.4.11. Deverá suportar, pelo menos, 350 (trezentos e cinquenta) túneis de VPN Client-Site;

9.20. INTERFACES DE REDE:

9.20.1. Deverá possuir, pelo menos, 10 (dez) interfaces RJ 45.
9.20.2. Todos os equipamentos que acompanharem a solução devem suportar operar em modo de alta disponibilidade ativo-ativo e estar licenciados para operar desta forma.
9.20.3. Deverá possuir licença para número ilimitado de usuários e endereços IP.
9.20.4. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Wireless, ao menos, 6 (seis) Pontos de Acesso sem fio.
9.20.5. Deverá ser capaz de gerenciar, via funcionalidade de Controladora Switch, ao menos, 6(seis) equipamentos.
9.20.6. Deverá estar licenciado para permitir número ilimitado de estações de rede e usuários.
9.20.7. Deverá incluir licença para a funcionalidade de VPN SSL.
9.20.8. Deverá ser fornecida toda documentação técnica, bem como manual de utilização, em português do Brasil ou em inglês.

ITEM 10 - TRANSCEIVER SFP+ 10GBase-SR

10.1. Transceiver SFP+ para conexão de fibras ópticas multimodo;
10.2. Deve ser compatível com o padrão 10GBase-SR para fibras ópticas de até 300m;
10.3. Deve ter velocidade de 10GbE;
10.4. Deve ser do mesmo fabricante e compatível com os firewalls, switches concentrador e de acesso deste processo.

ITEM 11 - TRANSCEIVER SFP+ 10GBase-LR

11.1. Transceiver SFP+ para conexão de fibras ópticas monomodo;
11.2. Deve ser compatível com o padrão 10GBase-LR para fibras ópticas de até 10km;
11.3. Deve possuir conector LC;
11.4. Deve ter velocidade de 10GbE;
11.5. Deve ser do mesmo fabricante e compatível com os firewalls, switches concentrador e de acesso deste processo.

ITEM 12 - TRANSCEIVER SFP 1000Base-LX

12.1. Transceiver SFP para conexão de fibras ópticas monomodo;
12.2. Deve ser compatível com o padrão 1000Base-LX para fibras ópticas de até 10km;
12.3. Deve possuir conector LC;
12.4. Deve ter velocidade de 1GbE;
12.5. Deve ser do mesmo fabricante e compatível com os firewalls, switches concentrador e de acesso deste processo.

ITEM 13 - TRANSCEIVER SFP 1000Base-SX
13.1. Transceiver SFP para conexão de fibras ópticas multimodo;
13.2. Deve ser compatível com o padrão 1000Base-SX para fibras ópticas de até 300m;
13.3. Deve possuir conector LC;
13.4. Deve ter velocidade de 1GbE;
13.5. Deve ser do mesmo fabricante e compatível com os firewalls, switches concentrador e de acesso deste processo.

ITEM 14 – SOLUÇÃO DE ZERO TRUST NETWORK ACCESS
14.1. A solução de ZTNA deve ser composta pelos agentes a serem instalados nas máquinas dos usuários finais, bem como por um proxy de acesso, o qual concentrará as requisições dos agentes para acesso às aplicações corporativas;
14.2. A solução de ZTNA deve prover um método de controlar o acesso identificando o dispositivo do usuário, autenticação e postura com base em tags de Zero Trust;
14.3. A solução de ZTNA deve controlar o acesso por sessão, validando o usuário e dispositivo, bem como estabelecendo um túnel criptografado de modo automático para cada sessão;
14.4. A solução de ZTNA deve ser compatível e se integrar aos "FirewallS de Próxima Geração (NGFW)," considerando os modelos FortiGate 601E, FortiGate 201F e FortiGate 61F, em uso no TRE;
14.5. A solução de proxy de acesso deve prover suporte a um método de publicação de aplicações corporativas sem necessidade de agente, tal como mediante um portal web SSL a ser acessado por cada usuário;
14.6. Deve permitir o gerenciamento dos agentes remotamente, a partir de uma console central do próprio fabricante a ser disponibilizada em nuvem;
14.7. A solução deve ser escalável até 50.000 agentes;
14.8. O licenciamento deve se basear no número de agentes registrados na console de gerenciamento central do mesmo fabricante;
14.9. Deve ser compatível com pelo menos os seguintes sistemas operacionais: Microsoft Windows: 7 (32 e 64 bits), 8.1 (32 e 64 bits), 10 (32 e 64 bits) e 11 (64 bits); Microsoft Windows Server: 2008 R2, 2012, 2012 R2, 2016, 2019 e 2022; Mac OS X: versões 13, 12, 11 e 10.15; Linux: Ubuntu 18.04 e posterior, Debian 11 e posterior, CentOS Stream 8, CentOS 7.4 e posterior, RedHat 7.4 e posterior, Fedora 36 e posterior;
14.10. A solução de ZTNA deve dispor de mecanismos para analisar a requisição TLS Client hello e o cabeçalho HTTP User-Agent para determinar e controlar se a requisição está partindo de um dispositivo não passível de gerenciamento pela console central, tal como um dispositivo móvel;
14.11. A comunicação de controle entre os agentes e a console central deve ser criptografada e acontecer através de TCP e TLS 1.3;
14.12. Tanto mediante agente ou sem agente deve ser possível habilitar MFA (autenticação multifator) no processo de autenticação dos usuários;
14.13. A console central deve emitir, assinar e instalar automaticamente um certificado para os agentes contendo ID único de cada agente, número de série do certificado e número de série da console central. O certificado emitido deverá ser único por agente e deverá ainda ser compartilhado com o proxy de acesso;
14.14. Deve ser possível revogar o certificado de um agente por meio da console central;
14.15. O certificado emitido deve ser utilizado no processo de autenticação via ZTNA para identificar o dispositivo do usuário final junto ao proxy de acesso;
14.16. No passo de identificação do dispositivo mediante certificado deve ser possível averiguar se o identificador único do agente e número do certificado coincidem com o que o proxy de acesso conhece. Caso algum desses dados estejam diferente, o acesso deverá ser bloqueado por padrão;
14.17. Deve ser possível configurar o idioma que o agente utiliza para, pelo menos, inglês, português, espanhol ou ainda usar o idioma do sistema operacional;
14.18. A solução deve prover backup automático diariamente, permitindo que em um evento crítico seja possível restaurar os dados de até cinco dias anteriores ao ocorrido;
14.19. Deve ser possível determinar para quais funcionalidades o log deve estar habilitado e permitir que esses dados sejam enviados para a console central;
14.20. Deve suportar pelo menos os seguintes níveis de log: emergência, alerta, crítico, erro, aviso, informativo, debug;
14.21. Deve ser possível exportar os logs diretamente a nível de agente;
14.22. Deve ser possível verificar as violações de filtro web diretamente no agente, especificando ainda a URL, categoria, quando a violação ocorreu e usuário;
14.23. Deve ser possível exigir uma senha para desconectar o agente da console central;
14.24. Deve ser possível determinar quando o filtro web entrará em ação no agente, se o mesmo deverá estar sempre ativo ou somente quando o usuário estiver fora da rede corporativa;
14.25. Deve existir a possibilidade de restringir o usuário de realizar backup da configuração do agente;
14.26. Deve ser possível evitar que o usuário realize um shutdown do agente após estar registrado à console central;
14.27. Deve ser possível enviar os logs para uma ferramenta de consolidação de logs do mesmo fabricante, visando consolidar os logs do proxy de acesso ZTNA em conjunto com os logs dos agentes. Deve ser possível ainda atribuir tags aos end-points de acordo com o indíce de comprometimento detectado pela solução de consolidação de logs, desde que haja licenciamento instalado para tal;
14.28. Deve ser possível configurar o agente para usar Proxy;
14.29. O agente deve permitir a configuração local via XML (eXtensible Markup Language);
14.30. Deve existir a possibilidade de criar um convite para que os usuários realizem o registro do agente à console central;
14.31. Este convite deve gerar um código a ser inserido no passo de registro do agente e deve ser possível ainda adicionar um passo de verificação da autenticação do usuário, podendo associar a autenticação via base de dados local, LDAP e SAML;
14.32. Deverá ser possível enviar uma notificação por e-mail contendo o código de registro para os usuários finais informados, bem como um link para download do instalador do agente;
14.33. Deve ser possível especificar a validade do código de registro;
14.34. A console central de agentes deve dispor de métodos para determinar se um usuário está on-net ou off-net, ou seja, dentro ou fora da rede corporativa. Deve ser possível ainda criar perfis de configurações distintos para os usuários on-net e off-net;
14.35. A solução deve suportar casos de uso utilizando IPv6 puro, bem como IPv6 em conjunto com IPv4;
14.36. Deve ser possível agrupar agentes em grupos;

14.37. Deve ser possível atribuir grupos de agentes a perfis de políticas específicos;
14.38. Deve ser possível atribuir um nível de prioridade a um perfil de política visando priorizar qual política será utilizada caso um grupo de agentes esteja associado a mais de um perfil de política;
14.39. A console central deve apresentar um resumo das informações de cada end-point, tais como nome do dispositivo, sistema operacional, IP privado, endereço mac, IP público, estado da conexão com a console central, zero trust tags associadas, detalhes da conexão de rede cabeada e WiFi, detalhes do hardware como modelo do dispositivo, fabricante, CPU, RAM, número de série e capacidade de armazenamento. Deve permitir ainda facilmente ver detalhes de qual política está associada com cada agente, qual versão de agente está em uso em um respectivo end-point, número de série do agente, identificador único e número de série do certificado emitido para o processo de ZTNA;
14.40. O proxy de acesso deve atuar como proxy reverso para aplicações baseadas em HTTP, HTTPS, RDP, SMB, CIFS, SSH, SMTP, SMTPS, IMAP, IMAPS, POP3 e POP3S;
14.41. Para aplicações HTTP e HTTPS deve ser possível realizar um balanceamento de carga entre os servidores cadastrados usando algoritmos como round robin, por peso, baseado no host field do cabeçalho HTTP ou baseado em disponibilidade do servidor;
14.42. Para regras de encaminhamento de tráfego TCP, deve ser possível vincular o servidor com um FQDN visando ofuscar o endereço IP privado do servidor. Deste modo, o agente deve manipular o host file do end-point visando criar entradas DNS;
14.43. Deve ser possível definir um pool de IPs no proxy de acesso como IPs de origem para comunicação interna com as aplicações privadas;
14.44. A console central deve permitir mapear as regras de destinos de ZTNA a serem sincronizadas com os end-points e permitir ainda definir para qual tráfego deve ser aplicada criptografia, tal como para tráfego HTTP sem criptografia nativa;
14.45. Deve permitir criação de regras de conformidade que avaliem à postura do dispositivo e auxiliem o administrador no controle de acesso à recursos da infraestrutura, impedindo que um cliente não conforme possa se conectar a redes críticas;
14.46. As regras de conformidade devem gerar tags que são sincronizadas entre os elementos da solução de ZTNA visando controlar a postura de um determinado end-point diretamente no proxy de acesso;
14.47. A postura deve ser monitorada continuamente para que, caso ocorra uma alteração, o proxy de acesso termine e passe a bloquear a conexão em desacordo com as regras de compliance definidas;
14.48. Deve ser possível construir tags com verificações no end-point, as quais podem variar de acordo com o suporte ao sistema operacional, tais como se o end-point está logado no domínio, versão do sistema operacional, chave de registro, processo, nível de vulnerabilidade, CVEs, arquivos existentes em um caminho específico e até mesmo se o antivírus está instalado e sendo executado, além de ser possível validar se as assinaturas estão atualizadas;
14.49. A console central deve permitir exportar e importar tags entre sistemas diferentes por meio de um arquivo JSON;
14.50. Deve ser possível verificar quais end-points estão associadas com cada tag;
14.51. Deve ser possível criar regras no proxy de acesso determinando se um dispositivo necessita estar de acordo com uma ou mais de uma tag simultaneamente, caso a política possua vínculo com diversas tags;
14.52. Deve ser possível criar regras no proxy de acesso vinculando interface de origem, IP de origem, IP de destino, servidor ZTNA, tag ZTNA, grupo de usuários ou usuário;
14.53. Para validação da autenticação dos usuários em conjunto com as regras de proxy de acesso, a solução deve suportar SAML, LDAP, Radius ou base de dados local;
14.54. Deve possibilitar definir funções administrativas relacionadas às permissões dos end-points, de políticas e de configurações gerais;
14.55. Deve possibilitar aos usuários definirem suas identidades mediante inserção manual, vínculo com LinkedIn, Google ou Salesforce, podendo ainda notificá-los para que esse vínculo possa ser realizado;
14.56. A console central deve possuir funcionalidade de rastreamento de vulnerabilidades a nível de end-point, permitindo ainda definir o rastreamento no momento do registro, quando ocorrer uma atualização de uma assinatura vulnerável, bem como patches e atualizações de segurança a nível de sistema operacional;
14.57. Deverá ser possível agendar quando o rastreamento deve ocorrer ou vinculá-lo em conjunto com a janela de manutenção automática do Windows;
14.58. Deve permitir que o usuário inicie uma análise de vulnerabilidade sob demanda diretamente no agente;
14.59. Deve ser possível aplicar um patch automático com base no nível de criticidade definido, tal como atualizar automaticamente patches considerados críticos;
14.60. Caso não seja possível aplicar um patch automático para corrigir uma vulnerabilidade, requerendo assim um patch manual, deve ser possível excluir essa aplicação da verificação de compliance;
14.61. Deve ser possível excluir determinadas aplicações da verificação de compliance e até mesmo desabilitar o patch automático;
14.62. O agente deve dispor de um sistema de notificação do tipo pop-up visando alertar o usuário;
14.63. Deve fornecer informações sobre a vulnerabilidade, patches, versões afetadas, severidade, bem como o CVE correspondente;
14.64. Deve suportar a criação de várias versões de pacotes de instalação;
14.65. As vulnerabilidades encontradas devem ser exibidas diretamente no agente com um link para análise de mais detalhes, englobando nome da vulnerabilidade, severidade, produtos afetados, CVE IDs, descrição, informação do fabricante do software e, quando disponível, link para download do patch no site público do fabricante do software;
14.66. Os resultados da verificação de vulnerabilidades devem incluir pelo menos: lista de vulnerabilidades, número de vulnerabilidades classificadas como críticas, altas, médias e baixas, bem como disponibilizar ainda a possibilidade de aplicar a remediação imediatamente;
14.67. Deve possuir módulo para execução de filtro web a nível de end-point mediante uso do agente local, realizando a filtragem diretamente no end-point, podendo ainda ser possível bloquear, permitir, alertar ou monitorar o tráfego web com base na categoria de URL ou filtro de URL customizado;
14.68. O agente deve realizar consultas online ao centro de inteligência do próprio fabricante para determinar a categoria de uma determinada URL visando aplicar o controle de acesso à Internet;
14.69. Deve ser possível configurar o filtro de URL com base em caracteres curingas ou expressões regulares (RegEx) com as opções de permitir, bloquear ou monitorar;
14.70. O agente para Windows deve permitir inspeção de tráfego HTTPS mediante instalação de plugin disponibilizado pelo mesmo fabricante do agente, o qual deve ser compatível com Google Chrome, Mozilla Firefox e Microsoft Edge;
14.71. Deve ser possível configurar o proxy de acesso para atuar como CASB (Cloud Access Security Broker) em linha, inline do inglês, visando controlar o acesso a aplicações SaaS;

14.72. O proxy de acesso deve manter uma base de aplicações dinâmica, a qual deve ser compartilhada pelo centro de inteligência do fabricante da solução;
14.73. A solução deve estar dimensionada e licenciada para atender, no mínimo, 25 (vinte e cinco) endpoints.

ITEM 15 – BANCO DE HORAS TÉCNICA

15.1. Serviços especializados para novas demandas ou correção de problemas não previstos após instalação da solução;
15.2. Visando garantir o perfeito funcionamento da solução após implementação, mesmo após treinamento sobre as funcionalidades e operação assistida, deverá ser ofertado serviço de banco de horas técnica em caso de intercorrências que prejudiquem o bom funcionamento e que necessitem de intervenção no ambiente da CONTRATANTE por time técnico qualificado para tal resolução por parte da CONTRATADA;
15.3. O serviço deverá ser prestado preferencialmente de forma remota, com prazo de uso durante o período contratado de 12 meses para uso;
15.4. O serviço especializado será demandado através de Ordens de Serviço (OS) prevendo o quantitativo a serem consumidos, o período de execução e a descrição dos serviços a serem executados;
15.5. O pagamento deverá ser realizado de acordo com a quantidade prevista e vinculadas ao item da OS. Qualquer alteração na quantidade de horas deverá ser justificada e previamente aprovada pela CONTRATANTE;
15.6. Os serviços proporcionais de gerenciamento de projetos e liderança técnica deverão estar incluídos dentro do valor da hora;
15.7. O serviço especializado abrange as seguintes atividades, podendo através de livre acordo entre as partes através de comunicação formal abrangerem itens não contemplados neste edital:

15.7.1. Resolução de problemas críticos na infraestrutura de processamento, armazenamento, backup, firewall , virtualização e redes;
15.7.2. Revisões e/ou Alterações de configurações, novas instalações, atualização de versões de softwares ou firmwares;
15.7.3. Execução de testes programados de recuperação de desastres visando validar o plano de continuidade de negócios;
15.7.4. Treinamento para conscientização sobre ameaças cibernéticas.
15.7.5. Serviços consultivos, para apoiar a avaliar, melhorar e testar processos de resposta a incidentes críticos de segurança;
15.7.6. Serviço de consolidação em dashboard com inúmeros fatores de riscos externos, como : serviços e portas divulgados publicamente, credenciais vazadas, identificação de páginas web, domínios e perfis de redes sociais que tentem se passar por este TRE;
15.7.7. Serviço de Implantação e Configuração para Solução De Segurança e Gerência De Redes
15.7.8. Serviço de Implantação e Configuração para Unidade Centralizada de Armazenamento de Logs e Relatoria;
15.7.9. Serviços Profissionais de Implantação e Configuração Unidade de Gerência Centralizada de Equipamentos
15.7.10. Treinamento para Solução de Segurança e Gerência de Redes NGFW
15.7.11. Treinamento de Unidade de Gerência Centralizada de Equipamentos
15.7.12. Treinamento de Unidade Centralizada de Armazenamento de Logs e Relatoria Migrações de dados;
15.7.13. Diagnóstico de problemas de desempenho e planejamento de capacidade;
15.7.14. Recuperação de dados através de Software de Backup e Replicação
15.7.15. Recuperação de solução de segurança de dados em ambiente VMware.
15.7.16. Implementação de regras de segurança;
15.7.17. Configurações em ativos de rede;
15.7.18. Elaboração de documentação técnica e de usuário;
15.7.19. Transferência de conhecimentos relacionados ao desenvolvimento, implantação e manutenção no ambiente do CONTRATANTE.
15.7.20. Levantamento de informações junto aos usuários, objetivando a definição e elaboração de regras e políticas.
15.7.21. Corrigir ou apoiar em problemas e defeitos em funcionalidades já existentes;
15.7.22. Realização de operação assistida e monitoramento de ambientes entregues com a solução.
15.7.23. Orientar na utilização dos softwares instalados no CONTRATANTE com a utilização das melhores práticas e orientações dos fabricantes;
15.7.24. Apoiar na atualização, instalação e/ou reinstalação de novas versões e dos produtos instalados no CONTRATANTE minimizando impactos;
15.7.25. Apoiar na configuração/parametrização do sistema em novas máquinas;
15.7.26. Orientar no levantamento de informações que possibilite a identificação de novas necessidades, detectadas no ambiente do CONTRATANTE;
15.7.27. Diagnosticar o bom funcionamento das ferramentas instaladas, garantindo a máxima utilização dos recursos oferecidos;
15.7.28. Identificar e elaborar proposição de melhoria em performance, desempenho, tunning, disponibilidade e confiabilidade em ambientes;
15.7.29. Otimizar a reinstalação e/ou adaptação das ferramentas em outros equipamentos que não seja onde originalmente os sistema e produtos foram instalados;
15.7.30. Definir metodologia, elaborar relatórios e projetos e acompanhar a configuração e utilização de solução de alta disponibilidade, repassando aos técnicos da TI do CONTRATANTE as melhores práticas para uso da solução, quanto a parametrização e configuração dos componentes e ferramentas utilizadas no CONTRATANTE;
15.7.31. Esclarecer dúvidas e orientar os técnicos de TI do CONTRATANTE, sobre integração das soluções, abrangendo as diversas plataformas existentes no ambiente computacional do CONTRATANTE.
15.7.32. Apoiar no planejamento, na execução e na avaliação das mudanças no ambiente;
15.7.33. Analisar patches, correções e novas versões e sugerir a aplicação ou não dos mesmos no ambiente;
15.7.34. Apoiar no planejamento, na execução e na avaliação das atualizações de versões e aplicação de patches da ferramenta;
15.7.35. Apoiar no planejamento, na execução e na avaliação de implantação de novas aplicações ou atualização de aplicações no ambiente;

15.8. Como condição para atender os requisitos do ITEM do presente lote, a licitante vencedora deverá apresentar até a assinatura do contrato, os documentos da qualificação técnico-operacional em processos de serviços de TI, comprovando possuir aderência aos padrões de gestão qualidade de serviços de tecnologia da informação e comunicação (TIC) previstos na ISO NBR 20.000. Esta maturidade deverá ser comprovada por meio da apresentação de certificados válidos de avaliação de maturidade, do tipo do CMMI-Svc nível 2 ou superior, ou MPS.Br-Serviços Nível F ou superior.
15.9. A comprovação do item anterior imediato, no caso do CMMI-Svc, se dará por meio de cópia autenticada do certificado emitido por uma agência certificadora independente (agências credenciadas pelo Software Engineering Institute - http://www.sei.cmu.edu) ou seu representante no Brasil;

15.10. Para a certificação MPS/BR-Serviços, a comprovação se dará por meio de cópia autenticada do certificado de qualidade MPS-BR-Sv emitido pela SOFTEX ou parceiro autorizado.
15.11. A qualquer tempo, o time técnico da CONTRATANTE poderá realizar visita às instalações da CONTRATADA para comprovar a adoção de processos aderentes à norma ISO NBR 20.000 na execução dos serviços previstos neste edital
15.12. A licitante deverá possuir uma ferramenta de SERVICE DESK on-line e que siga as melhores práticas da certificação ITIL para a abertura e gerenciamento de chamados na utilização dos bancos de horas, a fim de acompanhar o tempo de resolução para cada atividade (SLA), bem como disponibilizá-los em filas de priorizações para cada ocorrência, serviço e/ou incidente.
15.13. A ferramenta mencionada deverá permitir que a CONTRATANTE realize abertura de chamados através de e-mail, portal na Internet e/ou aplicativo de celular, sendo que cada chamado deverá possuir um código de identificação único que permita a sua rápida identificação.
15.14. O sistema deverá permitir o acompanhamento em tempo real pela CONTRATANTE dos chamados abertos e seus respectivos status, além de permitir a visualização do histórico de todos os chamados finalizados.
15.15. Para melhor gerenciamento dos chamados pela CONTRATADA, o sistema deverá possuir um painel (dashboard) que possua gráficos e outros tipos de visualizadores, além de permitir a geração de relatórios conforme necessidade e solicitação da CONTRATANTE.
15.16. Para fins de comprovação, o licitante deverá informar o nome da ferramenta de *service desk* utilizada.
15.17. Todo processo do serviço realizado deverá ser demonstrado em relatórios com todos os seus detalhes da sua execução.
15.18. Após a abertura de um chamado no sistema, o primeiro atendimento deverá ocorrer de forma remota para melhor entendimento do cenário e sua possível solução. Todavia, caso o atendimento remoto não seja suficiente para conclusão do chamado, então o atendimento deverá ser realizado de forma on-site, ou seja, de forma presencial no endereço da CONTRATANTE.
15.19. Quanto remoto, o atendimento será feito por ferramenta que irá contabilizar o tempo de acesso e trabalho, a fim de validar a consumação do banco de horas;

ITEM 16 – SOLUÇÃO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA DE SEGURANÇA (SOAR)
16.1. CASE MANAGEMENT

16.1.1. Alertas e incidentes devem ser tratados separadamente, cada um em seu próprio módulo na interface do usuário;
16.1.2. Atributos de cada módulo (Campos), como nome, gravidade, do módulo Alerta, deve ser personalizável para que os usuários possam adicioná-los ou removê-los. Além disso, os usuários devem poder criar, modificar e excluir seus próprios atributos personalizados em qualquer módulo do sistema;
16.1.3. A solução deve permitir que cada registro seja correlacionado e vinculado a qualquer outro registro no sistema, incluindo tipos personalizados de registros que os próprios usuários definem;
16.1.4. A solução deve fornecer a capacidade de agregar registros semelhantes com base em valores de campo semelhantes;
16.1.5. A solução deve ter um mecanismo de previsão baseado em aprendizado de máquina que prevê valores de campos com base em dados históricos. O escopo da previsão de aprendizado de máquina deve abranger todos os módulos do produto, incluindo os built-in (como alertas, incidentes, indicadores) e personalizados;
16.1.6. A solução deve incluir um recurso de detecção de e-mail de phishing baseado em IA;
16.1.7. A visualização de cada módulo deve ser personalizável por meio de um modelo de visualização que define a posição de cada campo e widget;
16.1.8. O sistema deve fornecer uma funcionalidade de pesquisa global que permita ao analista pesquisar palavras-chave em todo o sistema em todos os módulos;
16.1.9. A interface Web para o usuário deve oferecer a possibilidade de vincular vários registros a um ticket ou criar novos registros todos juntos e vinculá-los ao ticket atual. Os registros podem ser, mas não limitados a: Artefatos, Tarefas, Sala de Guerra, Usuários, Campanhas, Buscas, Ativos, Alertas, Anexos, E-mails e Incidentes;
16.1.10. Os tickets devem ter um atributo de prioridade que possa ser usado para classificá-los enquanto os exibe na interface do usuário da Web;
16.1.11. O escalonamento de tickets deve ser possível manualmente por meio da interface Web ou automaticamente por meio de um fluxo de trabalho de automação que pode aplicar qualquer lógica como condição antes de escalonar o ticket;
16.1.12. Deve incluir um gerenciamento de crises da sala de guerra para permitir a colaboração entre equipes durante as crises; a sala de guerra deve poder ser criada manualmente ou escalando um ticket T1 ou T2;
16.1.13. Tickets, artefatos, anexos, e módulos customizados devem dar aos analistas um meio de comunicar por texto (comentários) cada mensagem deixada por um analista, ou um workflow de automação deve permanecer como atributo do registro onde foi criado. Além disso, os comentários devem suportar as funcionalidades abaixo;
16.1.14. Os comentários podem ser texto simples ou rich text;
16.1.15. Os analistas podem ser marcados em um comentário para atrair sua atenção;
16.1.16. Um comentário pode ser usado para executar ações;
16.1.17. Comentários são compatíveis com tags genéricas;
16.1.18. Os comentários suportam anexos de arquivos;
16.1.19. Comentários são compatíveis com RBAC;
16.1.20. O sistema deve permitir que o analista execute a Análise de Causa Raiz com uma média de correlação gráfica;
16.1.21. A correlação gráfica deve estar disponível para diferentes tipos de registro, como ativos, vulnerabilidades, alertas e incidentes;
16.1.22. A solução deve se integrar ao framework MITRE ATTACK fornecendo enriquecimento tático, análise de ameaças, investigação de incidentes e sugestões de remediação;
16.1.23. O sistema deve permitir que o analista realize a Análise Pós-Incidente (PIA – relacionada ao tratamento de incidentes);
16.1.24. O sistema deve suportar tíquetes de mapeamento para fases da cadeia de morte cibernética;
16.1.25. A solução deve ter um recurso de gerenciamento de filas personalizável que ofereça suporte a atribuições automatizadas de alertas/incidentes/tarefas para vários grupos de usuários;
16.1.26. A solução deve oferecer suporte a um sistema de rastreamento de Acordo de Nível de Serviço configurável dentro da estrutura de gerenciamento de caso para que o tempo de conclusão de vários marcos possa ser identificado e relatado;
16.1.27. O gerenciamento de casos deve oferecer suporte a anexos de arquivo;
16.1.28. A solução deve ser capaz de extrair artefatos (IP, URL, Domínio) de mais de 1550 tipos de arquivos, incluindo MS Office e PDFs. Os artefatos extraídos devem estar vinculados ao registro do arquivo de onde foram extraídos;

16.1.29. A solução deve ser capaz de extrair metadados de arquivos (autor, timestamp) juntamente com uma visualização de conteúdo como texto ou HTML de mais de 1550 tipos de arquivos, incluindo MS Office e PDFs;
16.1.30. A solução deve permitir que o analista edite campos diretamente na WebUI se o RBAC estiver configurado para;
16.1.31. As notificações devem ser flexíveis e usar vários canais, como interface do usuário, e-mail e várias integrações com serviços de conferência, como MS Teams e Slacks;
16.1.32. Filas de emissão de bilhetes, gerenciamento de turnos e entrega devem ser um recurso integrado. A solução deve fornecer um sistema de filas onde os analistas são designados com base em sua disponibilidade (turno);
16.1.33. Deve permitir que os usuários definam condições para controlar a visibilidade dos objetos na interface do usuário. Isso não está relacionado à filtragem de registros, mas às condições de exibição para objetos de página específicas, como guias;
16.1.34. Solução deve criar uma linha do tempo automática para alertas, incidentes e salas de guerra.

16.2. AUTOMATION WORKFLOWS (PLAYBOOKS)

16.2.1. A quantidade mínima de manuais que o fornecedor deve fornecer, abrangendo casos de uso, amostras e informações adicionais relacionadas a conectores, precisa exceder 4.500 unidades;
16.2.2. Os playbooks necessitam ser organizados em diretórios, permitindo a exportação ou importação completa do diretório de playbooks por meio da interface WebUI;
16.2.3. É fundamental que os playbooks possuam atributos configuráveis que priorizem a execução de determinados playbooks em relação a outros na sequência, de acordo com sua relevância;
16.2.4. Os manuais precisam incluir gatilhos condicionais, ativando-os apenas sob condições predefinidas. Os seguintes operadores condicionais devem ser compatíveis:
16.2.4.1. Igual;
16.2.4.2. Diferente;
16.2.4.3. Menor que/Menor ou igual a;
16.2.4.4. Maior que/Maior ou igual a;
16.2.4.5. Contido na lista;
16.2.4.6. Não contido na lista;
16.2.4.7. Nulo.
16.2.5. Os playbooks devem ser projetados para serem ativados pelos seguintes mecanismos:
16.2.5.1. Manualmente, pelo analista através da WebUI;
16.2.5.2. Na criação/atualização/exclusão de registros (Alertas, indicadores, incidentes);
16.2.5.3. Por meio de API, em resposta a solicitações HTTP com parâmetros específicos;
16.2.5.4. Referenciamento direto, permitindo que um playbook inicie outro, fornecendo os parâmetros necessários;
16.2.6. A interface de usuário gráfica para a criação de playbooks deve oferecer uma ferramenta de design intuitiva, com funcionalidades de arrastar e soltar componentes, além de painéis auxiliares para consulta de variáveis disponíveis e manipulação de dados;
16.2.7. O editor de playbooks deve permitir o desfazer e refazer de ações, possibilitando a recuperação ou remoção de etapas previamente configuradas;
16.2.8. É essencial que os usuários possam testar a execução dos playbooks diretamente do editor, utilizando registros reais do ambiente ou dados do último teste executado;
16.2.9. Deve ser viável exportar e importar playbooks individualmente, contemplando diferentes versões de um mesmo playbook;
16.2.10. O sistema deve suportar a criação, modificação e exclusão de variáveis globais, acessíveis por todos os playbooks e editáveis tanto via WebUI quanto dentro dos próprios playbooks;
16.2.11. A visualização do histórico de execução dos playbooks, exibindo entradas, saídas e configurações de cada etapa, é uma funcionalidade obrigatória;
16.2.12. A configuração do nível de log para os playbooks deve ser ajustável tanto globalmente (para todo o sistema) quanto individualmente (para cada playbook);
16.2.13. Ferramentas de depuração devem estar integradas ao editor de playbooks, facilitando o diagnóstico e a correção de falhas, com base nos dados de execuções anteriores ou informações fornecidas pelo analista;
16.2.14. O controle de acesso baseado em funções (RBAC) deve abranger tanto os manuais quanto os fluxos de trabalho de automação;
16.2.15. O sistema deve fornecer mensagens de erro detalhadas para falhas na execução dos playbooks, permitindo a retomada do processo a partir do ponto de falha;
16.2.16. As etapas de decisão nos playbooks devem ser suficientemente versáteis para admitir condições complexas, que envolvam operações de aritmética, comparação e lógica, tais como:
16.2.16.1. Igualdade;
16.2.16.2. Desigualdade;
16.2.16.3. Maior que;
16.2.16.4. Maior ou igual a;
16.2.16.5. Menor que;
16.2.16.6. Menor ou igual a;
16.2.16.7. Operadores lógicos "E", "OU" e "NÃO";
16.2.16.8. Operações de adição, subtração, divisão, módulo, multiplicação e potenciação.
16.2.17. Deve ser possível aplicar condições complexas, como cálculos e comparações lógicas, sem necessidade de codificação explícita em linguagens de programação;
16.2.18. Em casos de falha ao atender todas as condições estabelecidas, a etapa de tomada de decisão deve oferecer a opção de prosseguir para uma próxima etapa padrão;
16.2.19. Os playbooks devem ter a capacidade de ser invocados por outros playbooks, ampliando a modularidade e reutilização das automações;
16.2.20. A integração da linguagem Python nos playbooks deve ser facilitada, suportando formatação automática e destaque de sintaxe, permitindo que o administrador do sistema SOAR restrinja os módulos Python utilizáveis;
16.2.21. O gerenciamento de conflitos de registros é uma funcionalidade requerida, possibilitando aos usuários definir quais campos podem ser sobrescritos em caso de divergência;

16.2.22. A interface WebUI deve incluir um editor de texto rico, permitindo a edição de conteúdo formatado com inclusão de tabelas, imagens e vídeos;
16.2.23. As etapas de playbook devem ser configuráveis para interromper a execução do playbook em caso de erro em uma etapa específica ou prosseguir, repassando a mensagem de erro para a próxima etapa;
16.2.24. A gestão dos playbooks deve oferecer funcionalidades de edição em massa, incluindo alteração de status, clonagem, realocação para diferentes grupos, ajuste do nível de log e exportação;
16.2.25. A escalabilidade dos playbooks é fundamental, devendo ser possível programar sua execução em intervalos específicos e prevenir sobreposições de execução;
16.2.26. No editor de playbooks, as funcionalidades de clonagem, cópia, colagem, alinhamento e exclusão de etapas ou grupos de etapas devem ser disponibilizadas para otimizar o processo de criação e edição;
16.2.27. A captura de dados e aprovações por e-mail, com mecanismos de ação baseados em temporizadores, amplia as capacidades de interação e automação dos playbooks;
16.2.28. O versionamento de playbooks é uma funcionalidade essencial, permitindo o rastreamento e gestão de diferentes versões de um mesmo playbook ao longo do tempo;
16.2.29. A solução deve oferecer mecanismos para ajustar as prioridades entre playbooks concorrentes, garantindo a execução eficiente de tarefas críticas;
16.2.30. A documentação e tutoriais para o desenvolvimento e utilização de playbooks devem ser abrangentes, incluindo exemplos práticos, melhores práticas e orientações detalhadas para configuração e solução de problemas;
16.2.31. A solução deve possibilitar a busca no histórico de playbooks executados, bem como acessar KPIs referentes à quantidade de playbooks realizados e ao número de ações tomadas;
16.2.32. A solução deve contar com suporte à criação automática de playbooks por meio de inteligência artificial. Por exemplo, um analista de segurança pode solicitar à IA para desenvolver um playbook que realize o enriquecimento de um endereço IP considerando as fontes X, Y e Z. Após a criação, o playbook gerado pela IA pode ser ajustado pelo analista;
16.2.33. A solução deve ser capaz de sugerir a execução de playbooks específicos para a remediação de ameaças identificadas em alertas e incidentes, utilizando inteligência artificial para tal;
16.2.34. A solução deve permitir a realização de simulações de ataques com o objetivo de avaliar a reação da equipe do SOC a incidentes. Deve ser possível instalar diversos cenários de simulação e repetir o mesmo cenário várias vezes;
16.2.35. A solução deve realizar automaticamente a triagem de alertas, prosseguir com o enriquecimento de indicadores extraídos, e potencialmente ajustar a severidade dos alertas com base na gravidade detectada em seu conteúdo, tudo de forma automática.
16.2.36. A solução deve facilitar a redução do MTTR (Tempo Médio de Resposta) por meio de playbooks pré-configurados para a resposta;
16.2.37. Os playbooks devem poder ser ativados por sistemas externos à solução por meio de API;
16.2.38. A solução deve suportar playbooks que requerem aprovação em determinado momento para prosseguir com as etapas subsequentes;
16.2.39. A solução deve permitir Playbooks que fazem referência a outros playbooks (playbooks aninhados).

16.3. LICENCIAMENTO

16.3.1. O licenciamento deve ser baseado no appliance e no número de usuários e não no número de playbooks ou em qualquer outra métrica operacional;
16.3.2. A licença deve suportar usuários simultâneos, independentemente de quantos usuários sejam criados no sistema;
16.3.3. A solução deve estar licenciada para 02 (dois) usuários simultâneos;
16.3.4. A solução deve suportar licenciamento quando implantada em redes air-gapped;
16.3.5. A solução deve ter uma licença de teste que possua limitações, mas não a tempo, deve ser gratuita, podendo ser utilizada para fins de desenvolvimento;
16.3.6. O Playbook Editor deve permitir que os usuários criem vários grupos recolhíveis de etapas e notas para melhorar a legibilidade;
16.3.7. Os playbooks devem oferecer suporte a uma etapa de espera configurável com uma quantidade de tempo definida ou uma condição que, se atendida ou um tempo limite configurável atingido, o playbook encerrará a espera e prosseguirá para a próxima etapa;
16.3.8. A solução deve fornecer um portal de conteúdo público e de dentro de sua interface de usuário da Web para baixar e consumir componentes do produto, como:
16.3.8.1. Painéis;
16.3.8.2. Relatórios;
16.3.8.3. Manuais;
16.3.8.4. Widgets personalizados;
16.3.8.5. Integrações (conectores);
16.3.8.6. Módulos e extensões do produto.
16.3.9. A solução deve ter pelo menos 390 (trezentos e noventa) Integrações com sistemas de terceiros, como por exemplo, soluções de SIEM, serviços de inteligência de ameaças e firewalls;
16.3.10. O sistema deve ter um mecanismo de atualização de conteúdo in-life independente das atualizações de firmware da solução. As integrações com sistemas de terceiros devem ter suas próprias atualizações utilizáveis em qualquer versão suportada do firmware da solução;
16.3.11. A interface do usuário da Web deve incluir assistentes para auxiliar os usuários na criação de conteúdo, seja esse conteúdo uma integração, uma extensão de produto ou um widget personalizado;
16.3.12. Cada integração deve ser documentada online;
16.3.13. O fornecedor deve fornecer um SDK de integração para permitir que os clientes desenvolvam suas próprias integrações;
16.3.14. O sistema deve fornecer um assistente de ingestão de dados amigável para configurar a ingestão de dados de sistemas de terceiros.

16.4. INTEGRATIONS/CONTENT

16.4.1. O sistema deve oferecer um painel de status que mostre a condição atual de todas as integrações estabelecidas com sistemas externos, garantindo que estão funcionando corretamente;
16.4.2. As funcionalidades oferecidas pelos conectores devem ser controladas por meio de Controle de Acesso Baseado em Funções (RBAC), assegurando que apenas usuários com permissões adequadas possam executar ações específicas;

16.4.3. Deve ser possível para um analista executar ações disponíveis nos conectores diretamente através da interface do SOAR na Web, sem a necessidade de recorrer a playbooks para automação;
16.4.4. A plataforma deve incluir um assistente para facilitar aos usuários o processo de criação de suas próprias integrações, permitindo também a edição de integrações existentes diretamente pelo WebUI, sem necessidade de um IDE externo;
16.4.5. Deve ser permitido instalar novas integrações localmente na solução, ampliando a capacidade de personalização conforme a necessidade do usuário;
16.4.6. A solução deve suportar múltiplas configurações para um único conector, permitindo, por exemplo, diferentes configurações para cada instância de um firewall, cada uma com suas próprias credenciais ou APIs de acesso;
16.4.7. Cada conector deve ser acompanhado de documentação detalhada, que inclua casos de uso e instruções para instalação;
16.4.8. Deve ser possível ao analista desenvolver seus próprios conectores, caso a solução não forneça os necessários para atender suas demandas específicas;
16.4.9. A solução já deve incluir uma variedade de conectores prontos para uso imediato, abrangendo categorias como produtos de rede e firewall, gestão de tickets, gestão de logs e SIEM, gestão de vulnerabilidades, segurança de endpoints, feeds de inteligência de ameaças, DevOps, provedores de nuvem, sandboxing, segurança de email, investigação de incidentes, análise de big data, segurança web, detecção de ameaças, gestão de identidade, soluções de bancos de dados, e outros;
16.4.10. A solução deve ser compatível com os principais SIEMs do mercado, incluindo IBM Qradar, Splunk, FortiSIEM, ArcSight (ou sua denominação atual), LogRhythm, RSA NetWitness e Rapid7;
16.4.11. Deve ser possível importar Processos de Fluxos de Trabalho (workflows) de sistemas como Flowable, Camunda e Signavio, entre outros;
16.4.12. A solução deve ser capaz de enviar mensagens de Syslog para dispositivos externos, fornecendo informações sobre o estado do sistema, execução de playbooks e saúde dos sistemas internos.

16.5. THREAT INTELLIGENCE

16.5.1. O fabricante da solução deve fornecer seu próprio serviço de inteligência de ameaças gratuitamente, integrado nativamente com o SOAR proposto;
16.5.2. A solução deve contar com um módulo de gerenciamento de inteligência de ameaças que inclua um painel de controle de informações de ameaças com estatísticas sobre: Feeds ativos, observáveis de alta confiança e fontes de feed;
16.5.3. Integração com múltiplas fontes de CTI (Inteligência de Ameaças Cibernéticas);
16.5.4. Os feeds de ameaças devem apresentar seus dados correlacionados com outros indicadores, a estrutura do MITRE e as solicitações de inteligência de prioridade. Além disso, cada indicador deve ter um widget gráfico de correlação que mostra graficamente todos os relacionamentos;
16.5.5. O gerenciamento de casos deve permitir que analistas solicitem requisitos de Inteligência de Ameaça prioritária para indicadores desconhecidos, criando tarefas para rastrear essas solicitações. A solução deve fornecer um framework que permita aos analistas responderem com um relatório de ameaças detalhado para o PIR solicitado;
16.5.6. A solução deve funcionar como um serviço de Inteligência de Ameaças para sistemas de terceiros, permitindo que coleções ou indicadores específicos sejam buscados do SOAR por SIEMs, EDRs e NGFWs via TAXII e CSV sobre HTTP;
16.5.7. Deve ser possível importar e exportar indicadores em massa diretamente da interface Web;
16.5.8. A solução deve ser suficientemente flexível para permitir o cálculo da reputação de indicadores com base em dados de múltiplas fontes de Inteligência de Ameaças;
16.5.9. A partir de um alerta ou indicador, deve ser possível abrir um PIR (Requisito de Inteligência de Prioridade) para a equipe de Inteligência de Ameaças;
16.5.10. A solução deve permitir a criação de conjuntos de dados a partir do conjunto de IOCs monitorados, como por exemplo, filtrar e exportar um conjunto de dados relacionado a Comando e Controle e Botnets.

16.6. DEPLOYMENT & ARCHITECTURE

16.6.1. A solução deve suportar implantação on-premise como um software appliance ou como um software;
16.6.2. A solução deve estar disponível em Nuvens Públicas;
16.6.3. A solução deve estar disponível como um serviço em nuvem;
16.6.4. A solução deve permitir backup e restauração da configuração e dos dados do sistema;
16.6.5. Solução deve ter a capacidade de criar módulos de produtos personalizados a partir da GUI da web, um módulo é um subsistema para gerenciar um novo tipo de registro, como: Alertas, Incidentes e indicadores;
16.6.6. O sistema deve ser escalável e resiliente. Deve ser possível agrupar vários nós (mais de 2) em uma configuração Ativa/Ativa;
16.6.7. A solução deve ter um proxy reverso para que os componentes remotos se comuniquem com os centrais para evitar ter que publicar os componentes centrais diretamente na WAN. O proxy reverso deve suportar alta disponibilidade;
16.6.8. A solução deve permitir a execução de ações de remediação e coleta de dados na rede segmentada por meio de um agente SOAR implantado no segmento de rede remoto, os agentes devem suportar atualizações automáticas;
16.6.9. O sistema deve permitir o uso de banco de dados interno e externo;
16.6.10. A solução deve incluir um aplicativo móvel para gerenciamento e monitoramento remoto;
16.6.11. A solução deve suportar integração de saída com um sistema NMS que, por padrão, monitore a lista abaixo pronta para uso (sem configuração):
16.6.11.1. CPU (Uso em %)
16.6.11.2. Disco (Uso em % para cada volume lógico e também para partição /boot)
16.6.11.3. E/S (solicitações de leitura e gravação/s para discos)
16.6.11.4. Largura de banda da placa de rede incluindo interface loopback(lo) (kb/s)
16.6.11.5. Uso de RAM (%)
16.6.11.6. NTP (Diferença entre NTP e máquina em segundos)
16.6.11.7. Servidor Web (conexões perdidas, solicitações por segundo, conexões manipuladas, etc)
16.6.11.8. Banco de dados (ativo conexões, blocos lidos do disco (blocos/min), taxa de acerto do cache do buffer (%), total de transações (tx/min)
16.6.11.9. MTA (número de solicitações, tamanho da fila do MTA)
16.6.11.10. Expiração da licença SOAR

16.6.11.11. Expiração dos certificados SOAR
16.6.11.12. Saúde dos conectores configurados SOAR (para cima/para baixo)
16.6.11.13. SOAR Playbook fila
16.6.12. Solução deve permitir a comunicação segura entre seus elementos;
16.6.13. Solução deve permitir a criação de filas de trabalho e organização de turnos e camadas de analistas (N1, N2, N3). A atribuição de alertas e incidentes aos analistas pode ser feita por um gestor ou de forma automática pela solução.

16.7. AUDIT

16.7.1. O sistema deve fornecer uma trilha de auditoria de todo o sistema, abrangendo tanto o sistema (como login, logoff, instalações) e eventos de dados (como criação de registro, atualização e exclusão);
16.7.2. O sistema deve permitir o encaminhamento de eventos para um servidor de log ou solução SIEM. Os protocolos a seguir devem ser compatíveis com um nível de log configurável:
16.7.2.1. UDP;
16.7.2.2. TCP, TCP/TLS;
16.7.2.3. RELP, RELP/TLS;
16.7.6. O sistema deve manter um widget de cronograma de registro de auditoria rastreando cada evento de registro com detalhes de cada alteração.

16.8. USER MANAGEMENT & RBAC

16.8.1. O sistema deve oferecer um controle de acesso baseado em funções (RBAC) detalhado e adaptável. Administradores devem ter a capacidade de especificar direitos de acesso para cada tipo de registro em um nível de campo. Por exemplo, o campo do endereço IP de origem;
16.8.2. A solução precisa suportar a administração do relacionamento entre grupos de usuários, onde um grupo pode herdar o escopo de acesso de outro(s) grupo(s) em uma estrutura hierárquica de pai, irmão e filho, permitindo que cada nível superior acesse os níveis inferiores;
16.8.3. A solução deve facilitar a colaboração entre analistas por meio de pesquisas compartilhadas, comentários em alertas e incidentes, entre outras funcionalidades;
16.8.4. A solução deve oferecer autenticação por meio de autenticação de dois fatores (MFA);
16.8.5. A solução deve suportar a autenticação externa de usuários utilizando LDAP, SAML (SSO).

16.9. DASHBOARDS

16.9.1. O sistema deve fornecer vários painéis configuráveis que se integram ao RBAC com controle de acesso por função;
16.9.2. O sistema deve fornecer um mecanismo para destacar alertas que estão se aproximando de violações de SLA;
16.9.3. O painel deve exibir informações específicas do analista, como alertas e tarefas atribuídas ao analista;
16.9.4. O sistema deve calcular um ROI estimado e permitir que isso seja exibido em um painel;
16.9.5. Deve ser possível importar e exportar modelos de painel;
16.9.6. O sistema deve fornecer painéis focados em funções, como; analista de nível 1, analista de nível 2, gerente de SOC;
16.9.7. O sistema deve medir métricas de SOC, relevantes, como tempo médio para identificação, confirmação, contenção, erradicação, recuperação. Deve ser possível ainda exibir essas métricas em um painel;
16.9.8. A solução deve ter um painel dedicado para monitorar o status de integridade/disponibilidade de cada integração e também a integridade do sistema do próprio SOAR;
16.9.9. A solução deve fornecer uma estrutura de desenvolvimento de painel baseada em HTML/JSON/JS para permitir que os usuários criem seus widgets de painel personalizados e os importem para a solução SOAR;
16.9.10. Solução deve ter suporte a Inteligência Artificial Generativa, permeando os módulos da solução. Analista deve ser capaz de fazer perguntas, requerir sugestões, interagir com a Inteligência artificial;
16.9.11. Solução deve permitir ao analista criar novos módulos e customizar dashboards;
16.9.12. Solução deve possuir sistema de Ajuda, que permite ao analista ou usuário tirar dúvidas. Além disso, solução deve ter disponível documentação completa, incluindo como construir playbooks, conectores, como customizar o dashboard, como gerenciar a força de trabalho do SOC, como configurar a solução;
16.9.13. Solução deve permitir monitorar a saúde do sistema através de dashboard específico para essa função;
16.9.14. Solução deve trazer dashboard com métricas (KPIs) de segurança e eficiência do SOC (tempo salvos com playbooks, retorno do investimento);
16.9.15. Os dashboards devem permitir auto-refresh;
16.9.16. Todas as ações da solução devem ser feitas na mesma interface (não desejamos duas interfaces / sistemas distintos).

16.10. REPORTING e NOTIFICATIONS

16.10.1. O sistema deve fornecer relatórios gráficos personalizados;
16.10.2. Deve ser possível agendar relatórios para serem executados em um horário definido pelo usuário;
16.10.3. Os relatórios devem estar disponíveis em formato PDF ou CSV;
16.10.4. Deve ser possível enviar relatórios programados para um destinatário de e-mail;
16.10.5. A solução deve permitir um controle programático dos relatórios, para que um analista possa criar um playbook para automatizar o processo de geração dos mesmos;
16.10.6. O acesso à funcionalidade de relatório deve ser controlado pela função RBAC;
16.10.7. O sistema deve ter uma trilha de auditoria que identifique a atividade do relatório, incluindo download do mesmo;
16.10.8. Deve ser possível incluir uma variedade de gráficos e métricas em relatórios personalizados;
16.10.9. Além da exportação automatizada de registros por meio de playbooks, a interface do usuário deve ter um meio que permita aos usuários baixar alguns/todos os registros para sua estação de trabalho;
16.10.10. Solução permite customizar Email Templates que são enviados pelo time de SOC;
16.10.11. Solução deve ter flexibilidade para envio de notificações externas.

ITEM 17 - TREINAMENTO OFICIAL - SWITCHES

17.1. Deve ser fornecido voucher de treinamento oficial do fabricante de administração e otimização do ambiente, com validade de, no mínimo, 01 ano, a ser realizado, preferencialmente, na modalidade à distância ou presencial, caso haja disponibilidade de turma e interesse da CONTRATANTE;

17.2. O treinamento deverá abarcar as configurações básicas e avançadas da solução, envolvendo, no mínimo, os seguintes tópicos:
- 17.2.1. Switches gerenciáveis;
- 17.2.2. Fundamentos de switches;
- 17.2.3. Design de Layer 2;
- 17.2.4. Segurança em Layer 2;
- 17.2.5. Recursos avançados de configuração de switches;
- 17.2.6. Monitoramento;
- 17.2.7. Troubleshooting.

ITEM 18 - TREINAMENTO OFICIAL - ACCESS POINTS

18.1. Deve ser fornecido voucher de treinamento oficial do fabricante de administração e otimização do ambiente, com validade de, no mínimo, 01 ano, a ser realizado, preferencialmente, na modalidade à distância ou presencial, caso haja disponibilidade de turma e interesse da CONTRATANTE;

18.2. O treinamento deverá abarcar as configurações básicas e avançadas da solução, envolvendo, no mínimo, os seguintes tópicos:
- 18.2.1. Introdução à configurações integradas de rede sem fio;
- 18.2.2. Controladora de rede sem fio;
- 18.2.3. Perfis de Access Points;
- 18.2.4. Troubleshooting.

ITEM 19 - TREINAMENTO OFICIAL - CONTROLE DE ACESSO À REDE

19.1. Deve ser fornecido voucher de treinamento oficial do fabricante de administração e otimização do ambiente, com validade de, no mínimo, 01 ano, a ser realizado, preferencialmente, na modalidade à distância ou presencial, caso haja disponibilidade de turma e interesse da CONTRATANTE;

19.2. O treinamento deverá abarcar as configurações básicas e avançadas da solução, envolvendo, no mínimo, os seguintes tópicos:
- 19.2.1. Configuração inicial;
- 19.2.2. Implementar a visibilidade de rede;
- 19.2.3. Identificar e classificar intrusos;
- 19.2.4. Visibilidade, Troubleshooting e Logging;
- 19.2.5. Políticas de segurança;
- 19.2.6. Integração de dispositivos de segurança e resposta automática.

ITEM 20 - TREINAMENTO OFICIAL - INFRAESTRUTURA E SEGURANÇA

20.1. Deve ser fornecido voucher de treinamento oficial do fabricante de administração e otimização do ambiente, com validade de, no mínimo, 01 ano, a ser realizado, preferencialmente, na modalidade à distância ou presencial, caso haja disponibilidade de turma e interesse da CONTRATANTE;

20.2. O treinamento deverá abarcar as configurações básicas e avançadas da solução, envolvendo, no mínimo, os seguintes tópicos:
- 20.2.1. Políticas de Firewall;
- 20.2.2. Network Address Translation;
- 20.2.3. Autenticação no Firewall;
- 20.2.4. Monitoramento e Log;
- 20.2.5. Web Filters;
- 20.2.6. Controle de Aplicações;
- 20.2.7. Antivírus;
- 20.2.8. Prevenção de intrusão e negação de serviço;
- 20.2.9. Configurações IPS/IDS;
- 20.2.10. Roteamento;
- 20.2.11. SSO ;
- 20.2.12. ZTNA;
- 20.2.13. IPSec VPN;
- 20.2.14. SSL VPN;
- 20.2.15. Alta disponibilidade;
- 20.2.16. Diagnósticos.

ITEM 21 - TREINAMENTO OFICIAL - GERENCIAMENTO E RELATORIA

21.1. Deve ser fornecido voucher de treinamento oficial do fabricante de administração e otimização do ambiente, com validade de, no mínimo, 01 ano, a ser realizado, preferencialmente, na modalidade à distância ou presencial, caso haja disponibilidade de turma e interesse da CONTRATANTE;

21.2. O treinamento deverá abarcar as configurações básicas e avançadas da solução, envolvendo, no mínimo, os seguintes tópicos:
- 21.2.1. Introdução e configuração inicial de sistema de relatoria;
- 21.2.2. Administração e gerenciamento de sistema de relatoria;
- 21.2.3. Alta disponibilidade de sistema de relatoria;
- 21.2.4. Gerenciamento de dispositivos em sistema de relatoria;
- 21.2.5. Análise de logs e gerenciamento de relatórios;
- 21.2.6. Introdução e configuração inicial em sistema de gerenciamento centralizado;
- 21.2.7. Administração e gerenciamento em sistema de gerenciamento centralizado;
- 21.2.8. Registro de dispositivos;
- 21.2.9. Configuração e instalação em nível de dispositivo;
- 21.2.10. Políticas e objetos em sistema de gerenciamento centralizado;
- 21.2.11. Diagnósticos e troubleshooting em sistema de gerenciamento centralizado.

ITEM 22 - TREINAMENTO OFICIAL - SOLUÇÃO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA DE SEGURANÇA (SOAR)

22.1. Deve ser fornecido voucher de treinamento oficial do fabricante de administração e otimização do ambiente, com validade de, no mínimo, 01 ano, a ser realizado, preferencialmente, na modalidade à distância ou presencial, caso haja disponibilidade de turma e interesse da CONTRATANTE;

22.2. O treinamento deverá abarcar as configurações básicas e avançadas da solução, envolvendo, no mínimo, os seguintes tópicos:
22.2.1. Introdução ao SOAR;
22.2.2. Gerenciamento de dispositivos;
22.2.3. Configuração do sistema;
22.2.4. Alta disponibilidade;
22.2.5. Buscas, Salas de Guerra e Atualizações;
22.2.6. Monitoramento de sistema e troubleshooting;

ITEM 23 – SEVIÇO DE IMPLANTAÇÃO - UST

23.1. O quantitativo de Unidade de Serviço Técnico (UST) será determinado de acordo com a atividade a ser realizada, nos termos definidos na presente especificação técnica;

23.2. Visando simplificar a visualização das necessidades de UST para implantação, abaixo consta quadro resumo de utilização de USTs, por tipo de Serviço de Implantação:

ATIVIDADE	UST'S
Planejamento de Implantação e Hands On	20
Instalação de Ativos de Rede	1
Instalação de Ativos de Segurança	1
Instalação de Solução de Controle de Acesso à Rede	25

23.3. PLANEJAMENTO DE IMPLANTAÇÃO E HANDS ON

23.3.1. O Planejamento de Implantação e Hands On deverá, pela sua complexidade, utilizará 20 USTs;
23.3.2. O Planejamento de Implantação compreende, entre outros, os seguintes procedimentos:
23.3.2.1. Análise de topologia e arquitetura da rede, considerando os firewalls, switches, access points, VLANs e outros componentes relevantes da infraestrutura da CONTRATANTE;
23.3.2.2. Análise de acesso à Internet, sites remotos, serviços de rede oferecidos aos usuários internos e externos;
23.3.2.3. Análise das regras de firewall existentes e aplicadas à solução ofertada e avaliação de melhores práticas, para implementação da solução;
23.3.2.4. Apresentação de plano de implantação, com descritivo de todos os serviços a serem executados e topologia física e lógica a ser implementada;
23.3.2.5. Geração de relatório e entrega de documentação da instalação, com as configurações efetuadas e as decisões tomadas, diagramas e topologias, em formato legível e tecnicamente fundamentado;
23.3.3. A CONTRATADA deverá realizar repasse de conhecimento, do tipo "Hands On" sobre a solução de Firewall, incluindo instalação, configuração básica e avançada, troubleshoot, monitoramento e gerenciamento;
23.3.3.1. O repasse de conhecimento será ministrado para um total de 6 (seis) participantes da CONTRATANTE
23.3.3.2. A CONTRATADA deverá fornecer todo material audiovisual, didático e, caso necessário, outros equipamentos eletrônicos para a realização dos repasses de conhecimento, além de impressos;
23.3.3.3. Deverá ter caráter prático e se baseará no sistema contratado e instalado na CONTRATANTE;
23.3.3.4. Todos os demais custos, ônus, obrigações e encargos para o treinamento devem ser arcados pela CONTRATADA.
23.3.4. Após a implementação, deverá ser fornecido documento "as-built", que descreve os principais elementos de implementação da configuração implantada e os resultados da verificação do sistema de base

23.4. INSTALAÇÃO DE ATIVOS DE REDE

23.4.1. Os ativos de rede abrangem a instalação e configuração dos equipamentos indicados no item 4, 5, 6, 7, e 8;
23.4.2. Será utilizada 1 (uma) UST para cada equipamento indicado no item 2.4.1 instalado pela CONTRATADA;
23.4.2.1. Não necessariamente será utilizada 1 (uma) UST para cada equipamento adquirido, somente será utilizada a UST para os equipamentos que a CONTRATADA realizar o serviço de instalação e configuração.
23.4.3. Os serviços de instalação e configuração compreendem, entre outros, os seguintes procedimentos:
23.4.3.1. SWITCH
23.4.3.1.1. Teste de energização;
23.4.3.1.2. Atualização de firmware;
23.4.3.1.3. Configuração de IP de Gerência;
23.4.3.1.4. Demais configurações necessárias para o perfeito funcionamento do equipamento.
23.4.3.2. ACCESS POINT
23.4.3.2.1. Energização;
23.4.3.2.2. Atualização de firmware;
23.4.3.2.3. Configuração de IP de Gerência;
23.4.3.2.4. Configuração de SSID;
23.4.2.2.5. Troca de senha de Administrador;
23.4.3.2.6. Demais configurações necessárias para o perfeito funcionamento do equipamento.

23.5. INSTALAÇÃO DE ATIVOS DE SEGURANÇA

23.5.1. Os ativos de segurança abrangem a instalação e configuração do equipamento indicado no item 9;
23.5.2. Será utilizada 1 (uma) UST para cada equipamento indicado no item 2.5.1 instalado pela CONTRATADA;
23.5.2.1. Não necessariamente será utilizada 1 (uma) UST para cada equipamento adquirido, somente será utilizada a UST para os equipamentos que a CONTRATADA realizar o serviço de instalação e configuração.
23.5.3. Os serviços de instalação e configuração compreendem, entre outros, os seguintes procedimentos:
23.5.2.1. FIREWALL
23.5.2.1.1. Teste de energização;
23.5.2.1.2. Atualização de firmware;
23.5.2.1.3. Configuração de IP LAN;

23.5.2.1.3. Configuração de IP WAN;
23.5.2.1.3. Instalação das licenças;
23.5.2.1.3. Troca de senha de Administrador;
23.5.2.1.4. Demais configurações necessárias para o perfeito funcionamento do equipamento.

23.6. SOLUÇÃO DE CONTROLE DE ACESSO À REDE

23.6.1. A solução de controle de acesso á rede abrange a instalação e configuração da solução indicada no item 3;
23.6.2. Ao adquirir uma unidade do item 3, para sua implantação, será necessário o uso de 25 USTs;
23.6.3. Os serviços de instalação e configuração da Solução de Controle de Acesso à Rede compreende, entre outros, os seguintes procedimentos:

23.6.3.1. Configuração do sistema de controle de acesso à rede, de acordo com as exigências levantadas, com as devidas atualizações necessárias;
23.6.3.2. Implantação integral, com todas as funcionalidades disponíveis, da solução de controle de acesso à rede, de acordo com a quantidade contratada;
23.6.3.3. Devem ser realizados testes iniciais da solução de controle de acesso a rede no sistema de produção, para isso, deve-se incluir verificações básicas de saúde do ambiente, verificações de alta disponibilidade e verificações funcionais antes de colocar a solução em operação;
23.6.3.4. A contratada deverá fornecer suporte durante a implantação. Revisões menores ou ajustes finos podem ser feitos, se necessário para garantir o bom funcionamento;

23.7. É de responsabilidade da CONTRATADA, até a assinatura do CONTRATO, designar um profissional certificado como especialista em NETOWRK SECURITY, pelo Fabricante da solução, com certificação de segurança cibernética, validando sua capacidade de executar operações de alto nível e certificação de Operações de Segurança validando a sua capacidade de proteger redes, implantando, gerenciando e monitorando os produtos de operações de segurança;

24.1. GARANTIA E SUPORTE TÉCNICO

24.1. Período do serviço do fabricante com pelo menos 60 (sessenta) meses pelo fabricante com cobertura 24x07 (24 horas por dia, 07 dias por semana);
24.2. A CONTRATADA deve possuir suporte técnico remoto para a solução de problemas comuns de suporte;
24.3. A CONTRATADA deve realizar o primeiro atendimento em até 90 minutos após a abertura do chamado. A resolução total do problema deverá ocorrer em até 4 horas após a abertura do chamado. Este requisito visa garantir a rápida resposta e resolução de questões críticas de segurança, minimizando possíveis impactos operacionais.;
24.4. O FABRICANTE deverá possuir Central de Atendimento online para abertura dos chamados de garantia, comprometendo-se a manter estes registros constando a descrição do problema;
24.5. Todos os itens de software que vierem instalados de fábrica no equipamento ofertado deverão estar cobertos pela garantia e serviço de suporte do FABRICANTE;
24.6. Caso o licitante não seja o mesmo fabricante do equipamento ofertado, este deverá enviar juntamente com a sua proposta uma declaração do fabricante do equipamento informando que prestará o serviço de suporte e garantia nas condições e termos deste edital ou comprovar através de PART NUMBER do serviço contratado a ser ofertado;
24.7. O serviço de garantia e suporte deverá ser do FABRICANTE do equipamento ou por assistência técnica qualificada e indicada por este através de declaração.

25.2. OUTROS REQUISITOS

25.1. O(s) produto(s) ofertado(s) deverá(ão) ser novo(s), de primeiro uso, estar em linha de produção e pertencer à linha corporativa de produtos comercializados pelo(s) fabricante(s). Não serão aceitos equipamentos ou componentes que tenham sido descontinuados pelo fabricante ou que estejam listados para descontinuidade futura (end-of-life) na data da análise das propostas.
25.2. É obrigatória a comprovação técnica de todas as características exigidas para os equipamentos e softwares aqui solicitados, independente da descrição da proposta do fornecedor, através de documentos que sejam de domínio público cuja origem seja exclusivamente do fabricante dos produtos, como catálogos, manuais, ficha de especificação técnica, informações obtidas em sites oficiais do fabricante através da internet, indicando as respectivas URL (Uniform Resource Locator). A simples repetição das especificações do termo de referência sem a devida comprovação acarretará a desclassificação da empresa proponente.
25.3. Sob pena de desclassificação, a proposta cadastrada deverá possuir todas as reais características do(s) equipamento(s) ofertado(s), assim como informar marca e modelo do equipamento. O simples fato de “COPIAR” e “COLAR” o descritivo contido no edital não será caracterizado como descritivo da proposta.
25.4. Deverão ser informados todos os componentes relevantes da solução proposta com seus respectivos códigos do fabricante (marca, modelo, fabricante e part numbers), descrição e quantidades.
25.5. Deverão ser fornecidos, em papel impresso ou meio digital, manuais técnicos do usuário e preferencialmente contendo todas as informações sobre os produtos com as instruções para instalação, configuração, operação e administração, assim como o fabricante deverá possuir o catálogo ou descrição do modelo ofertando na Internet para consulta.
25.6. Apresentação de no mínimo um atestado emitido por pessoa jurídica de direito público ou privado, comprovando que a proponente fornece/forneceu bens compatíveis com os objetos da licitação emitidos em papel timbrado, com assinatura, identificação e telefone do emitente.
25.7. Todos os SUBITENS do ITEM deverão ser fornecidos, instalados e configurados de forma que a solução final entregue esteja disponível para pleno funcionamento.

ANEXO II DO TERMO DE REFERÊNCIA
TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE

PREGÃO ELETRÔNICO
TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ

Política de Segurança da Informação do Tribunal Regional Eleitoral do Amapá

Eu, _____, inscrito(a) sob RG nº _____ e CPF nº_____, representante da empresa _____, estabelecida no endereço _____, inscrita no CNPJ/MF com o n.º _____, em razão da execução das atividades previstas do Contrato TRE/AP nº _____, firmo o presente TERMO DE RESPONSABILIDADE E CONFIDENCIALIDADE, mediante as estipulações consignadas neste instrumento:

1. O subscritor declara expressamente por este ato, ter conhecimento e ciência:

1.1. Da Política de Segurança da Informação e Comunicação do TRE-AP, constante da Resolução TRE-AP nº 570/2022, disponível em https://www.tre-ap.jus.br/transparencia-e-prestacao-de-contas/governanca-de-tecnologia-da-informacao-e-comunicacao/politicas-normas-e-processos, podendo ser solicitada à Secretaria de Gestão de Pessoas (SGP) ou de Secretaria de Tecnologia da Informação (STI) do TRE/AP, em caso de indisponibilidade técnica pela internet, assumindo inteira responsabilidade em dar ciência da norma a seu(s) colaborador(es) e prezar pelo cumprimento da mesma, no que couber;

1.2. Da Política Geral de Privacidade e Proteção de Dados Pessoais do TRE-AP, constante da Resolução TRE-AP nº 571/2022, disponível em https://www.tre-ap.jus.br/transparencia-e-prestacao-de-contas/governanca-de-tecnologia-da-informacao-e-comunicacao/politicas-normas-e-processos, podendo ser solicitada à Secretaria de Gestão de Pessoas (SGP) ou de Secretaria de Tecnologia da Informação (STI) do TRE/AP, em caso de indisponibilidade técnica pela internet, assumindo inteira responsabilidade em dar ciência da norma a seu(s) colaborador(es) e prezar pelo cumprimento da mesma, no que couber;

1.3. De que todos os acessos efetuados, trabalhos desenvolvidos, informações manipuladas, arquivos, conteúdos, conexões, acesso remoto, mensagens eletrônicas e acesso à internet, podem ser verificados e auditados pelos colaboradores efetivos do TRE-AP com atribuição para tal, a qualquer momento, independente de aviso prévio, podendo ainda revogar as autorizações que lhe tenham sido concedidas;

1.4. De que todos os ambientes físicos e lógicos do TRE-AP são monitorados para garantir a proteção e guarda das informações e dos Recursos de Tecnologia de Informação e Comunicação;

1.5. De que não deve publicar ou divulgar, por quaisquer meio, segredos ou informações sigilosas que forem acessadas, obtidas ou geradas em decorrência do exercício do cargo ou dos serviços contratados, sem permissão prévia e por escrito do TRE-AP, sendo obrigado a ressarcir as perdas e danos experimentados pelo TRE-AP, sem prejuízo das penalidades administrativas, civis e criminais previstas em lei. Esse compromisso permanecerá inclusive após o término ou rescisão do vínculo;

1.6. De que quaisquer violações à Política de Segurança, Normas e procedimentos correlatos são passíveis de penalidades administrativas, sem prejuízo de ações legais cabíveis.

2. Este Termo tem natureza irrevogável e irretratável, vigorando a partir da data de sua assinatura.

E por estar de acordo com o inteiro teor deste Termo, o assina nesta data, para que produza seus jurídicos e legais efeitos.

_____, [DIA] de [MÊS] de [ANO].

_____
ASSINATURA DO XX

ANEXO III DO TERMO DE REFERÊNCIA
DOCUMENTO DE FORMALIZAÇÃO DE DEMANDA - DFD

1. OBJETO A SER CONTRATADO
Aquisição de equipamentos de comunicação de dados e segurança para redes de computadores.

2 - IDENTIFICAÇÃO DA UNIDADE DEMANDANTE	
Unidade/Setor:	Coordenadoria de Infraestrutura
Responsável(eis):	Jimmy Almendra Macedo

3. JUSTIFICATIVA DA NECESSIDADE DA CONTRATAÇÃO
A crescente necessidade de Tecnologia da Informação e Comunicação no judiciário torna imperativo para o cumprimento da sua missão institucional uma infraestrutura de rede robusta, capaz de sustentar o fluxo de dados de maneira confiável, resiliente e segura. No contexto do TRE-AP, a situação não é diferente. As crescentes demandas, que incluem a utilização de diversos sistemas como PJe, SEI, acesso à Internet, videoconferências, transmissões de vídeo, entre outros, tornam virtualmente impossível a execução das atividades das diversas áreas deste Tribunal sem uma comunicação eficaz na rede de dados. Ainda, com a crescente necessidade de Tecnologias da Informação e Comunicação, cresce também a importância dos dados que trafegam pela rede, o que demanda uma atenção especial em relação à segurança da informação, sobretudo no âmbito deste Tribunal, visto que tem como missão a garantia da legitimidade do processo eleitoral, a fim de fortalecer a democracia.

Sendo assim, considerando que a atual infraestrutura de telecomunicações, notadamente em relação aos switches e pontos de acesso de rede sem fio, se encontram em fim de garantia, é salutar que sejam realizados os presentes estudos, a fim de avaliar solução de telecomunicações, bem como de segurança da informação, capaz de atender às demandas do TRE-AP, visando o fortalecimento da gerência de rede e ativos de rede, bem como a segurança da informação neste Tribunal.

4. QUANTIDADE A SER CONTRATADA E JUSTIFICATIVA

Nº Item	Descrição	Unidade de medida (R$, metro, litro, un., postos de trabalho, etc.)	Quantidade	Justificativa
1	Solução de Gerenciamento Centralizado de Configuração	unitário	2	Atualizar a topologia de rede, implementar mecanismos de segurança, aumentar a robustez, disponibilidade, confiabilidade e eficiência da rede de dados
2	Solução de Logs e Relatoria		2	
3	Solução de Controle de Acesso à Rede (100 endpoints)		10	
4	Switch Core		4	
5	Switch de Distribuição		10	
6	Switch de Acesso - Tipo 1 (48 Portas)		40	
7	Switch de Acesso - Tipo 2 (24 Portas)		25	
8	Access Point		100	
9	Firewall de Nova Geração (NGFW)		15	
10	Transceiver SFP+ 10GBase-SR		50	
11	Transceiver SFP+ 10GBase-LR		10	
12	Transceiver SFP 1000Base-LX		10	
13	Transceiver SFP 1000Base-SX		30	
14	Solução de ZTNA (Pacote de 25 dispositivos)		10	
15	Banco de Horas Técnicas		200	Opção de utilizar suporte técnico especializado
16	Solução de Gerenciamento de Eventos e Informações de Segurança (SIEM)		1	Fornecer visibilidade em tempo real sobre sua postura de segurança e infraestrutura de TI
17	Solução de Orquestração, Automação e Resposta de Segurança (SOAR)		1	
18	Treinamento Oficial - Switches		4	Qualificar, desenvolver habilidades e conhecimentos aos profissionais.
19	Treinamento Oficial - Access Points		4	
20	Treinamento Oficial - Controle de Acesso à Rede		4	
21	Treinamento Oficial - Infraestrutura e Segurança		4	
22	Treinamento Oficial - Gerenciamento e Relatoria		4	
23	Treinamento Oficial - Solução de Gerenciamento de Eventos e Informações de Segurança (SIEM)		4	
24	Treinamento Oficial - Solução de Orquestração, Automação e Resposta de Segurança (SOAR)		4	
25	Implantação com Hands On - UST		225	Possibilitar que as instalações e configurações sejam executados por profissionais qualificados pelo fabricante dos dispositivos

5. PREVISÃO DA DATA EM QUE DEVE SER ENTREGUE O BEM OU INICIADA A PRESTAÇÃO DOS SERVIÇOS

Data: ___/___/___

Justificativa: *Vencimento do contrato anterior, ou, data de realização do evento...*

(X) Não se aplica

6. ALINHAMENTO ESTRATÉGICO

A contratação está alinhada a algum objetivo do Plano Estratégico do TRE/AP?

(X) Sim - Qual(is)?
( ) Garantia dos Direitos da Cidadania
( ) Fortalecimento da Relação Institucional do Poder Judiciário com a Sociedade
(X) Agilidade e Produtividade na Prestação Jurisdicional
(X) Enfrentamento à Corrupção, à Improbidade Administrativa e aos Ilícitos Eleitorais
(X) Promoção da Sustentabilidade
(X) Aperfeiçoamento da Gestão Administrativa e da Governança Judiciária
( ) Aperfeiçoamento da Gestão de Pessoas
(X) Aperfeiçoamento da Gestão Orçamentária e Financeira
(X) Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados

( ) Não

Nota(s):
1. *Planejamento Estratégico 2021/2026 - TRE/AP*

7. PREVISÃO NO PLANO DE AQUISIÇÕES ANUAL

A contratação está prevista no Plano de Compras do TRE/AP?

(X) Sim. Indicação: Anexo III - Orçamento de Cibersegurança, Item 2
( ) Não. Justificativa:

Nota(s):
1. *Plano de Contratações 2023 - TRE/AP*
2. *Plano de Compras 2023 - TRE/AP*

8. INFORMAÇÕES ADICIONAIS

A contratação exigirá:
8.1. Equipe de Planejamento:
( ) Não. Justificativa:
(X) Sim. Composição:

Nome	**Tipo de Integrante (Solicitante, Demandante, técnico e administrativo)**	**Unidade/Setor**
Jimmy Almendra Macedo	Demandante	STI/CINF
Renan Coutinho Diniz	Técnico	STI/CINF/SGIRC
Juarez do Carmo Benício Dias	Administrativo	SAO/CMP/SPAT

8.2. Estudo Técnico Preliminar:
( ) Não. Justificativa:
(X) Sim.

8.3. Mapa de riscos:
( ) Não. Justificativa:
(X) Sim.

8.4. Equipe de Fiscalização de contrato:
(X) Não. Justificativa: Será composta no transcorrer do processo.
( ) Sim. Composição:

Integrante	**Titular**	**Substituto**	**Unidade**
Gestor:			
Fiscal Técnico:			
Fiscal Administrativo:			
Observado o Princípio da Segregação de Funções?		( ) Sim ( ) Não. Justificativa:	

8.5. A contratação será processada por Dispensa Eletrônica?
( ) Sim.
(X) Não. Justificativa:

8.6. Tratando-se de contratação com fundamento nos incisos I e II do artigo 75 da Lei nº 14.133/2021, a estimativa de preços será realizada concomitantemente à seleção da proposta economicamente mais vantajosa? (X) Sim (Justificar e informar a fonte orçamentária para cobertura da futura despesa, nos moldes adotado por este Tribunal). ( ) Não.

9. RESPONSÁVEL PELA FORMALIZAÇÃO DA DEMANDA
.Jimmy Almendra Macedo Coordenador de Infraestrutura

ANEXO IV DO TERMO DE REFERÊNCIA
INFORMAÇÃO CONCLUSIVA DO VALOR ESTIMADO - ICVE

INFORMAÇÃO CONCLUSIVA DO VALOR ESTIMADO **- ICVE**

Valor estimado da contratação	R$ __ (_____)
Forma de aquisição	(x) Pregão Eletrônico ou Concorrência. ( ) Outra. ( ) Aquisição direta: ( ) Inexigibilidade. ( ) Dispensa de licitação.
Classificação da contratação	( ) obras e serviços de engenharia ou de serviços de manutenção de veículos automotores; ( ) outros serviços e compras ( ) serviços com dedicação de mão de obra exclusiva; (x) SOLUÇÕES DE TIC (Resolução CNJ nº 468/2022), quando aplicável.
Objeto (*Descrição sucinta do objeto que será estimado*)	Registro de Preços para aquisição de Ativos de Rede e Segurança da Informação, incluindo Switches, Access Points, Firewalls, Soluções de Gerenciamento, Controle de Acesso, Autenticação e acessórios necessários, com garantia de pelo menos 60 (sessenta) meses, instalação, configuração da solução e treinamento, visando atender as demandas do TRE-AP e demais participantes.
Servidor ou servidores responsáveis pela estimativa de preços:	Servidor 1: Renan Coutinho Diniz, Lotação: Seção de Gestão de Infraestrutura e Redes Servidor 2: _____, Lotação: _____ Servidor 3: _____, Lotação: _____
Norma utilizada para a estimativa de preços	(**x**) Instrução Normativa SG/ME nº 65, de 07 de julho de 2021. ( ) Outra norma/fonte/critério de pesquisa de preços (*JUSTIFICAR*):
Critérios: (situações específicas de cada objeto)	**A cotação de preços observou as condições comerciais praticadas, na forma do art. 4º da IN SG/ME nº 65/21?** (x) **Sim.** ( ) **Não.** Listar quais não foram e justificar. Pode haver alguma que não se aplica, se for o caso, identificar também: ***Nota(s):*** ***1. Condições:*** *prazos e locais de entrega, instalação e montagem do bem ou execução do serviço, quantidade contratada, formas e prazos de pagamento, fretes, garantias exigidas e marcas e modelos, quando for o caso, observadas a potencial economia de escala e as peculiaridades do local de execução do objeto.* ***2.*** *No caso de* ***previsão de matriz de alocação de riscos*** *entre o contratante e o contratado, o cálculo do valor estimado da contratação poderá considerar taxa de risco compatível com o objeto da contratação e os riscos atribuídos ao contratado, podendo ser utilizada a metodologia estabelecida no Caderno de Logística, elaborado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia ou metodologia, desde que em harmonia com a Política de Gestão de Riscos adotada no âmbito da Justiça Eleitoral do Amapá.*
Parâmetros adotados na estimativa de preços	**I - ASSINALAR quais parâmetros do art. 5º da IN SG/ME nº 65/21 foram utilizados:** **( ) Inciso 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; **(x) Inciso 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; **( ) Inciso 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; **(x) Inciso 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 **( ) Inciso 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. ***Nota(s):*** ***1. Excepcionalmente**, será admitido o preço estimado com base em orçamento fora do prazo estipulado neste inciso II, desde que devidamente justificado nos autos pelo agente responsável e observado o índice de atualização de preços correspondente.* ***2. Tratando-se de bens ou serviços para os quais, de forma justificada no processo, não foi possível estimar os preços com os parâmetros definidos acima**, poderá a unidade simplificar sua estimativa inicial por outros meios idôneos, entre eles:* *( ) último valor contratado pelo órgão, atualizado até a data da estimativa pelo critério previsto no contrato; não havendo, pelo índice setorial específico aplicável e, na falta desse, pelo Índice Nacional de Preços ao Consumidor Amplo - IPCA divulgado pelo IBGE;* *( ) pesquisa em sites especializados ou de domínio amplo, devendo ser observadas nessa pesquisa as regras do Caderno de Logística para pesquisa de preços editado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia;* *( ) consulta direta aos fornecedores potenciais, mesmo que por e-mail, WhatsApp, comprovada no processo, ou por telefone, neste caso caso certificadas no processo, no mínimo, as seguintes informações: nome do servidor que realizou a pesquisa; nome, número do Cadastro Nacional de Pessoas Jurídicas - CNPJ, praça da sede e o número do telefone da empresa pesquisada; nome do atendente e o valor obtido na pesquisa.* **II - A cotação de preços priorizou os parâmetros definidos nos incisos I e II:** (x) Sim ( ) Não (JUSTIFICAR): **III - Na pesquisa direta com fornecedores foram observados os requisitos listados no § 2º do art. 5 º da IN SG/ME nº 65/21**. (x) Sim, todos. ( ) Parcialmente ou não observado (JUSTIFICAR): **IV - Nos casos específicos de DISPENSA e INEXIGIBILIDADE de licitação:** (x) N/A **Foram observadas as regras do art. 5º da IN nº 65/2021?** (x) Sim. ( ) Não, adotado os seguintes critérios: ( ) valores de contratações de objetos idênticos, comercializados pela futura contratada, por meio da apresentação de notas fiscais emitidas para outros contratantes, públicos ou privados, no período de até 1 (um) ano anterior à data da contratação pela Administração, ou por outro meio idôneo; ( ) Excepcionalmente, como a futura contratada não comercializou o objeto anteriormente, a justificativa de preço foi realizada com objetos semelhantes de mesma natureza, com as especificações técnicas que demonstram similaridade com o objeto pretendido. APONTAR QUAIS: ( ) Caso não tenha utilizado a IN SG/ME nº 65/21 DESCREVER os critérios e parâmetros adotados na pesquisa de preços: _____ ***Nota(s):*** ***1. CONTRATAÇÃO DE ITENS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – TIC**: será admitido o preço estimado com base em orçamento fora do prazo estipulado neste inciso II, desde que devidamente justificado nos autos pelo agente responsável e observado o índice de atualização de preços correspondente.* ***2. CONTRATAÇÃO DE SERVIÇOS COM DEDICAÇÃO DE MÃO DE OBRA EXCLUSIVA**: na pesquisa de preço para obtenção do preço estimado relativo às contratações de prestação de serviços com regime de dedicação de mão de obra exclusiva, aplica-se o disposto na Instrução Normativa nº 5, de 26 de maio de 2017 - e suas eventuais alterações ou nova regulamentação expedida pelo Poder Executivo, salvo disposição superveniente em contrário expedida pelo Conselho Nacional de Justiça ou pelo Tribunal Superior Eleitoral, de observância obrigatória por este Regional - observando, no que couber, as regras deste anexo.*
Metodologia para obtenção da estimativa de preços	**Art. 6º da IN SG/ME nº 65/21:** **I - INSERIR como ANEXO I desta Informação o QUADRO com os preços obtidos e as fontes pesquisadas, linkadas com o número dos eventos no SEI.** (x) Não há grande variação entre os preços obtidos. ( ) Há grande variação entre os preços obtidos*. ***Nesse caso: ANALISAR de forma crítica os preços coletados e descritos no referido Anexo I, em especial, quando houver grande variação entre os valores apresentados (§ 4º do art. 6º da IN SG/ME nº 65/21)**. **a) foi acrescentado ou subtraído determinado percentual, de forma a aliar a atratividade do mercado e mitigar o risco de sobrepreço? (§ 2º do art. 6º da IN SG/ME nº 65/21)**: (x) Não. ( ) Sim, justificar: **b) há valores inexequíveis, inconsistentes ou excessivamente elevados?** (x) Não há valores com essas características. ( ) Sim; se forem desconsiderados, FUNDAMENTAR (§ 3º do art. 6º da IN SG/ME nº 65/21): **c) o preço estimado foi obtido com base única no inciso I do art. 5º (§ 6º do art. 6º da IN SG/ME nº 65/21):** (x) Não ( ) sim e observou o limite representado pela mediana do item nos sistemas consultados. ****Após os procedimentos acima, INSERIR COMO ANEXO II desta Informação NOVO QUADRO com os PREÇOS FINAIS ESTIMADOS para a licitação ou contratação direta**, as fontes pesquisadas - linkadas com o número do evento no SEI - decorrentes da média, mediana ou o menor dos valores obtidos na pesquisa de preços, desde que o cálculo incida sobre um conjunto de três ou mais preços, **OU** de forma excepcional e justificada abaixo, em número menor, desde que aprovado pela autoridade competente (§ 4º do art. 6º da IN SG/ME nº 65/21): ( ) N/A *****Para esta contratação serão utilizados outros critérios ou métodos?** Caso positivo, deverão ser devidamente justificados pelos responsáveis da informação conclusiva sobre o valor estimado e aprovados pela autoridade competente (§ 1º do art. 6º da IN SG/ME nº 65/21):

	( ) N/A
Publicação	**Valor estimado é sigiloso:** (x) Não, PUBLICAR. ( ) Sim. Desde que justificado, o orçamento estimado da contratação poderá ter caráter sigiloso, sem prejuízo da divulgação do detalhamento dos quantitativos e das demais informações necessárias para a elaboração das propostas, salvo na hipótese de contratação cujo critério de julgamento for por maior desconto (art. 24 da Lei nº 14.133/2021). JUSTIFICATIVA: ... ( ) Sim, hipóteses de informações cujo sigilo seja imprescindível à segurança da sociedade e do Estado (art. 13 da Lei 14.133/2021 e § 1º do art. 7º da Lei n. 12.527/2011). JUSTIFICATIVA: ... ***Nota(s):*** ***1.*** *Ainda que se trate de preço com divulgação restrita na fase de planejamento e da seleção do fornecedor, a publicação dos dados deste formulário ocorrerá após a finalização da contratação.*

ANEXO I - PREÇOS OBTIDOS NA PESQUISA

ITEM	DESCRIÇÃO	PREÇO ESTIMADO
1	Solução de Gerenciamento Centralizado de Configuração	R$ 24.591,06
2	Solução de Logs e Relatoria	R$ 107.473,00
3	Solução de Controle de Acesso à Rede	R$ 63.744,68
4	Switch Core	R$ 120.344,93
5	Switch de Distribuição	R$ 109.404,48
6	Switch de Acesso - Tipo 1 (48 Portas)	R$ 21.631,26
7	Switch de Acesso - Tipo 2 (24 Portas)	R$ 14.134,60
8	Access Point	R$ 4.647,01
9	Firewall de Nova Geração (NGFW)	R$ 19.521,83
10	Transceiver SFP+ 10GBase-SR	R$ 986,84
11	Transceiver SFP+ 10GBase-LR	R$ 1.700,92
12	Transceiver SFP 1000Base-LX	R$ 1.159,63
13	Transceiver SFP 1000Base-SX	R$ 590,15
14	Solução de ZTNA (Pacote de 25 dispositivos)	R$ 22.217,65
15	Banco de Horas Técnica	R$ 746,77
16	Solução de Orquestração, Automação e Resposta de Segurança (SOAR)	R$ 2.888,558,66
17	Treinamento Oficial - Switches	R$ 28.912,54
18	Treinamento Oficial - Access Points	R$ 18.942,72
19	Treinamento Oficial - Controle de Acesso à Rede	R$ 28.912,54
20	Treinamento Oficial - Infraestrutura e Segurança	R$ 25.974,90
21	Treinamento Oficial - Gerenciamento e Relatoria	R$ 14.061,60
22	Treinamento Oficial - Solução de Orquestração, Automação e Resposta de Segurança (SOAR)	R$ 18.942,72
23	Implantação com Hands On - UST	R$ 1.116,33

ANEXO II - PREÇOS CONSIDERADOS PARA A ESTIMATIVA FINAL

1. CARACTERIZAÇÃO DAS FONTES CONSULTADAS (Art. 3º, III)

1.1. CONTRATAÇÕES SEMELHANTES (0842130)

1.1.1. Universidade Tecnológica Federal do Paraná - ARP 01/2023
1.1.2. Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco - ARP 01/2023
1.1.3. Banco do Estado de Sergipe - ARP 25/2023
1.1.4. Secretaria de Estado da Educação e da Cultura de Sergipe - ARP 228/2023
1.1.5. Companhia de Saneamento de Sergipe - Pregão Eletrônico 22/2023
1.1.6. Tribunal Regional Eleitoral do Amapá - Contrato 21/2023
1.1.7. Assembleia Legislativa de Rondônia - ARP 08/2023
1.1.8. Tribunal de Justiça de Rondônia - ARP 44/2023
1.1.9. Governo do Distrito Federal - Pregão Eletrônico 16/2023
1.1.10. Fundação Universidade Federal de São João Del Rei - Pregão Eletrônico 33/2023
1.1.11. Companhia de Pesquisa de Recursos Minerais do Rio de Janeiro - Pregão Eletrônico 188/2023
1.1.12. Conselho Regional de Engenharia, Arquitetura e Agronomia de Minas Gerais - Pregão Eletrônico 40/2023
1.1.13. Procuradoria Geral de Justiça do Estado da Bahia - Pregão Eletrônico 41/2023
1.1.14. Conselho Federal de Engenharia e Agronomia - Pregão Eletrônico 18/2023
1.1.15. Tribunal Regional Eleitoral do Amapá - Contrato 21/2023
1.1.16. Conselho Regional de Educação Física da Primeira Região - Pregão Eletrônico 7/2023
1.1.17. Prefeitura Municipal de São José dos Pinhais - SRP 129/2023
1.1.18. Universidade Estadual do Pará - SRP 42/2023
1.1.19. Universidade Federal de Viçosa - SRP 134/2023
1.1.20. Ministério Público do Estado de Pernambuco - SRP 39/2023
1.1.21. Ministério de Minas e Energia - Empresa de Pesquisa Energética - PE 12/2023

1.2. COTAÇÃO DIRETA

1.2.1. Fortam encaminhados e-mails para os seguintes fornecedores (0842005):
1.2.1.1. Techlead IT
1.2.1.2. Vector IT
1.2.1.3. Integratto

1.2.1.4. PPN Tecnologia
1.2.1.5. Team TI
1.2.1.6. Click TI
1.2.1.7. Security Data
1.2.1.8. WPI Soluções
1.2.1.9. Solus IT

1.2.2. Foram enviadas as cotações solicitadas pelos seguintes fornecedores (0842006):
1.2.2.1. Solus IT
1.2.2.2. Techlead IT Solutions
1.2.2.3. Vector IT
1.2.2.4. WPI Soluções em TI

2. SÉRIE DE PREÇOS COLETADOS (Art. 3º, IV)
2.1. Os preços coletados foram consolidados na tabela abaixo:

ITEM	DESCRIÇÃO	FONTE DE PREÇOS	PREÇO 1	PREÇO 2	PREÇO 3	PREÇO ESTIMADO
1	Solução de Gerenciamento Centralizado de Configuração	SOLUS IT WPI SOLUÇÕES VECTOR IT	R$ 24.591,06	R$ 25.900,00	R$ 26.100,10	R$ 24.591,06
2	Solução de Logs e Relatoria	SEDUC-SE EPE MPPE	R$ 86.219,00	R$ 100.000,00	R$ 136.200,00	R$ 107.473,00
3	Solução de Controle de Acesso à Rede	SOLUS VECTOR IT TECHLEAD	R$ 75.450,19	R$ 75.151,85	R$ 63.744,68	R$ 63.744,68
4	Switch Core	PSJP UEPA UFV	R$ 109.780,00	R$ 142.464,78	R$ 108.790,00	R$ 120.344,93
5	Switch de Distribuição	PSJP UEPA UFV	R$ 99.800,00	R$ 129.513,44	R$ 98.900,00	R$ 109.404,48
6	Switch de Acesso - Tipo 1 (48 Portas)	SEDUC-SE WPI SOLUÇÕES EM TI SOLUS IT	R$ 17.155,00	R$ 23.800,00	R$ 23.938,78	R$ 21.631,26
7	Switch de Acesso - Tipo 2 (24 Portas)	SEDUC-SE UTFPR BANESE	R$ 11.453,00	R$ 15.768,16	R$ 15.182,63	R$ 14.134,60
8	Access Point	SOLUS IT WPI SOLUÇÕES VECTOR IT	R$ 4.647,01	R$ 5.350,00	R$ 5.507,80	R$ 4.647,01
9	Firewall de Nova Geração (NGFW)	SEDUC-SE SOLUS IT VECTOR IT	R$ 16.147,00	R$ 21.209,25	R$ 21.209,25	R$ 19.521,83
10	Transceiver SFP+ 10GBase-SR	SEDUC-SE SOLUS IT TECHLEAD	R$ 756,00	R$ 1.025,62	R$ 1.178,91	R$ 986,84
11	Transceiver SFP+ 10GBase-LR	SEDUC-SE WPI SOLUÇÕES VECTOR IT	R$ 1.399,00	R$ 1.850,00	R$ 1.853,75	R$ 1.700,92
12	Transceiver SFP 1000Base-LX	IFPE UTFPR SOLUS IT	R$ 1.100,00	R$ 1.092,12	R$ 1.286,76	R$ 1.159,63
13	Transceiver SFP 1000Base-SX	VECTOR IT UTFPR WPI SOLUÇÕES	R$ 624,50	R$ 525,96	R$ 620,00	R$ 590,15
14	Solução de ZTNA (Pacote de 25 dispositivos)	SOLUS IT WPI SOLUÇÕES VECTOR IT	R$ 22.217,65	R$ 28.200,00	R$ 23.950,00	R$ 22.217,65
15	Banco de Horas Técnica	BANESE PGE-BA SOLUS IT	R$ 703,44	R$ 636,88	R$ 900,00	R$ 746,77
16	Solução de Orquestração, Automação e Resposta de Segurança (SOAR)	SOLUS IT WPI SOLUÇÕES VECTOR IT	R$ 2.888.558,66	R$ 2.900.000,00	R$ 2.920.520,25	R$ 2.888.558,66
17	Treinamento Oficial - Switches	TECHLEAD WPI SOLUÇÕES VECTOR IT	R$ 28.912,54	R$ 36.500,00	R$ 35.025,90	R$ 28.912,54
18	Treinamento Oficial - Access Points	TECHLEAD WPI SOLUÇÕES VECTOR IT	R$ 18.942,72	R$ 24.500,00	R$ 23.838,58	R$ 18.942,72
19	Treinamento Oficial - Controle de Acesso à Rede	TECHLEAD SOLUS IT VECTOR IT	R$ 28.912,54	R$ 36.385,19	R$ 35.023,10	R$ 28.912,54
20	Treinamento Oficial - Infraestrutura e Segurança	VECTOR IT	R$ 45.011,10	R$ 25.974,90	R$ 36.500,00	R$ 25.974,90

		SOLUS IT WPI SOLUÇÕES				
21	Treinamento Oficial - Gerenciamento e Relatoria	VECTOR IT SOLUS IT WPI SOLUÇÕES	R$ 25.009,95	R$ 14.061,60	R$ 24.500,00	R$ 14.061,60
22	Treinamento Oficial - Solução de Orquestração, Automação e Resposta de Segurança (SOAR)	TECHLEAD SOLUS IT WPI SOLUÇÕES	R$ 18.942,72	R$ 20.493,18	R$ 24.500,00	R$ 18.942,72
23	Implantação com Hands On - UST	SEDUC-SE IFPE TECHLEAD	R$ 1.157,00	R$ 1.392,00	R$ 800,00	R$ 1.116,33

Tabela 1 - Análise de custos médios para contratação de cada item

3. MÉTODO MATEMÁTICO APLICADO PARA DEFINIÇÃO DO VALOR ESTIMADO (Art. 3º, V)

3.1. Para os itens onde foram utilizados exclusivamente preços obtidos através de pesquisas por contratações semelhantes, bem como mescla de preços obtidos por contratações semelhantes e cotação direta com fornecedores:

3.1.1. Foi utilizada a média aritmética simples, chegando-se ao valor através da soma de todos os elementos, dividida pela quantidade.

3.2. Para os itens onde foram utilizados exclusivamente preços obtidos através de cotação direta:

3.2.1. Foi utilizado o menor preço dentre três propostas obtidas.

3.3. Excepcionalmente, para o Item 4 - Switch Core, foram utilizados os preços base do Item 5 - Switch de Distribuição, acrescidos de 10%;

3.3.1. Esse método foi utilizado em virtude de ambos os itens possuírem quase que integralmente as mesmas características, diferenciando-se somente em relação às funcionalidades de Switch Core, que estão presentes no Item 4 e não no Item 5;

3.3.2. O acréscimo de custo estimado pelas referidas funcionalidades é de 10% do valor obtido na pesquisa do Item 5;

3.3.3. Dessa forma, o preço médio obtido para o Item 4 é o mesmo preço do Item 5, acrescido de 10%;

3.4. Os preços obtidos, para cada item, foram selecionados conciliando critérios de similaridade com a presente contratação e custos.

4. JUSTIFICATIVAS PARA A METODOLOGIA UTILIZADA (Art. 3º, VI)

4.1. As buscas por contratações semelhantes se mostram uma forma eficaz de avaliação do preço praticado pelos fornecedores, no mercado. Porém, diversas variáveis podem alterar a composição dos preços das diversas soluções que compõem os itens da presente contratação. Dessa forma, a Equipe de Planejamento da Contratação entendeu ser mais preciso utilizar a média dos preços obtidos, quando, entre os preços utilizados pela pesquisa, constarem um ou mais preços oriundos de contratações semelhantes, realizadas pela Administração Pública, em até 1 (um) ano;

4.2. Por outro lado, quando os preços utilizados forem obtidos exclusivamente por cotação direta, há uma garantia de entrega do item nos valores ofertados, de forma que utilizar a média dos preços já não se mostra a melhor forma de estimativa. Por esse motivo, quando os 3 (três) preços que compõem a pesquisa forem exclusivamente obtidos por cotação direta, deverá ser utilizado o menor preço entre eles.

5. MEMÓRIA DE CÁLCULO DO VALOR ESTIMADO (Art. 3º, VII)

5.1. ITEM 1 - SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO

5.1.1. Composição de Preços

5.1.1.1. SOLUS IT

5.1.1.1.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa SOLUS IT;

5.1.1.1.2. O valor unitário indicado na proposta do Item 1 - SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO é de **R$ 24.591,06**.

5.1.1.2. WPI SOLUÇÕES EM TI

5.1.1.2.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa WPI SOLUÇÕES EM TI;

5.1.1.2.2. O valor unitário indicado na proposta do Item 1 - SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO é de **R$ 25.900,00**.

5.1.1.3. VECTOR IT

5.1.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa VECTOR IT;

5.1.1.3.2. O valor unitário indicado na proposta do Item 1 - SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO é de **R$ 26.100,10**.

5.1.2. Visto que a estimativa utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.2, do presente Anexo, o preço estimado para o ITEM 1 - SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO é **R$ 24.591,06**.

5.2. ITEM 2 - SOLUÇÃO DE LOGS E RELATORIA

5.2.1. Composição de Preços

5.2.1.1. Secretaria da Educação de Sergipe - Pregão 228/2023 - Item 11

5.2.1.1.1. Na contratação utilizada como base, foi registrado preço para o **FortiAnalyzer-VM, com capacidade de retenção de logs de 25GB por dia de logs**, no valor de **R$ 86.219,00**;

5.2.1.1.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;

5.2.1.1.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 86.219,00**.

5.2.1.2. Ministério de Minas e Energia - Empresa de Pesquisa Energética - PE 12/2023 - Item 1

5.2.1.2.1. Na contratação utilizada como base, foi registrado preço para **Licença para ampliação da capacidade de coleta diária de dados - FAZ-VM-GB25 (de 25 GB/dia)**, no valor de **R$ 100.000,00**;

5.2.1.2.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;

5.2.1.2.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 100.000,00**.

5.2.1.3. Ministério Público do Estado de Pernambuco - SRP 39/2023 - Item 1.4

5.2.1.3.1. Na contratação utilizada como base, foi registrado preço para o **Solução de Análise de Logs e Relatórios**, no valor de **R$ 136.200,00**;

5.2.1.3.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;

5.2.1.3.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 136.200,00**.

5.2.2. Visto que a estimativa não utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.1, do presente Anexo, o preço estimado para o ITEM 2 - SOLUÇÃO DE LOGS E RELATORIA será a média dos valores obtidos, qual seja, **R$ 107.473,00**.

5.3. ITEM 3 - SOLUÇÃO DE CONTROLE DE ACESSO À REDE

5.3.1. Composição de Preços

5.3.1.1. SOLUS IT

5.3.1.1.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa SOLUS IT;

5.3.1.1.2. O valor unitário indicado na proposta do Item 3 - SOLUÇÃO DE CONTROLE DE ACESSO À REDE é de **R$ 75.450,19**.

5.3.1.2. VECTOR IT

5.3.1.2.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa VECTOR IT;

5.3.1.2.2. O valor unitário indicado na proposta do Item 3 - SOLUÇÃO DE CONTROLE DE ACESSO À REDE é de **R$ 75.151,85**.

5.3.1.3. TECHLEAD

5.3.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa TECHLEAD;
5.3.1.3.2. O valor unitário indicado na proposta do Item 3 - SOLUÇÃO DE CONTROLE DE ACESSO À REDE é de **R$ 63.744,68**.

5.3.2. Visto que a estimativa utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.2, do presente Anexo, o preço estimado para o ITEM 3 - SOLUÇÃO DE CONTROLE DE ACESSO À REDE é **R$ 63.744,68**.

5.4. ITEM 4 - SWITCH CORE

5.4.1. Conforme indicado no item 3.3, o preço estimado para o Item 4 - Switch Core, será o mesmo utilizado para o Item 5 - Switch de Distribuição, acrescido de 10%;
5.4.2. Os preços obtidos para o Item 5 - Switch de Distribuição foram:
5.4.2.1. R$ 99.800,00;
5.4.2.2. R$ 129.513,44;
5.4.2.3. R$ 108.790,00.
5.4.3. Os valores considerados para o Item 4 - Switch Core, serão os supramencionados acrescidos de 10%:
5.4.3.1. R$ 109.780,00;
5.4.3.2. R$ 142.464,78;
5.4.3.3. R$ 108.790,00.
5.4.4. Dessa forma, o preço estimado para o ITEM 4 - SWITCH CORE, é a média dos preços indicados no item 6.4.3, qual seja, **R$ 120.344,93**.

5.5. ITEM 5 - SWITCH DE DISTRIBUIÇÃO

5.5.1. Composição de Preços
5.5.1.1. Prefeitura Municipal de São José dos Pinhais - SRP 129/2023 - Item 1 / Grupo 1
5.5.1.1.1. Na contratação utilizada como base, foi registrado preço para o **Switch Quantidade Portas: 24 UN, Tipo Portas: Gigabit Ethernet , Velocidade Porta: 10 Gbps**, no valor de **R$ 99.800,00**;
5.5.1.1.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;
5.5.1.1.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 99.800,00**.
5.5.1.2. Universidade Estadual do Pará - SRP 42/2023 - Item 2
5.5.1.2.1. Na contratação utilizada como base, foi registrado preço para **Switch HUAWEI S6730-H 24 portas 10G SFP+. 6 portas 40G/100G QSFP28**, no valor de **R$ 129.513,44**;
5.5.1.2.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;
5.5.1.2.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 129.513,44**.
5.5.1.3. Universidade Federal de Viçosa - SRP 134/2023 - Item 3 / Grupo 1
5.5.1.3.1. Na contratação utilizada como base, foi registrado preço para o **RUCKUS ICX7550-24F**, no valor de **R$ 98.900,00**;
5.5.1.3.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;
5.5.1.3.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 98.900,00**.
5.5.2. Visto que a estimativa não utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.1, do presente Anexo, o preço estimado para o ITEM 5 - SWITCH DE DISTRIBUIÇÃO será a média dos valores obtidos, qual seja, **R$ 109.404,48**.

5.6. ITEM 6 - SWITCH DE ACESSO TIPO 1 – 48 PORTAS GIGABIT

5.6.1. Composição de Preços
5.6.1.1. Secretaria da Educação de Sergipe - Pregão 228/2023 - Item 6
5.6.1.1.1. Na contratação utilizada como base, foi registrado preço para o **FortSwitch FS 148F-POE**, no valor de **R$ 17.155,00**;
5.6.1.1.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;
5.6.1.1.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 17.155,00**.
5.6.1.2. WPI SOLUÇÕES EM TI
5.6.1.2.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa WPI SOLUÇÕES EM TI;
5.6.1.2.2. O valor unitário indicado na proposta do Item 6 - Switch de Acesso - Tipo 1 é de **R$ 23.800,00**.
5.6.1.3. SOLUS IT
5.6.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa SOLUS IT;
5.6.1.3.2. O valor unitário indicado na proposta do Item 6 - Switch de Acesso - Tipo 1 é de **R$ 23.938,78**.
5.6.2. Visto que a estimativa não utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.1, do presente Anexo, o preço estimado para o ITEM 6 - SWITCH DE ACESSO TIPO 1 será a média dos valores obtidos, qual seja, **R$ 21.631,26**.

5.7. ITEM 7 - SWITCH DE ACESSO TIPO 2 – 24 PORTAS GIGABIT

5.7.1. Composição de Preços
5.7.1.1. Secretaria da Educação de Sergipe - Pregão 228/2023 - Item 5
5.7.1.1.1. Na contratação utilizada como base, foi registrado preço para o **FortSwitch FS 124F-POE**, no valor de **R$ 11.453,00**;
5.7.1.1.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;
5.7.1.1.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 11.453,00**.
5.7.1.2. Universidade Tecnológica Federal do Paraná - Grupo 1
5.7.1.2.1. Na contratação utilizada como base, foi registrado preço para o **FortSwitch FS 124F-POE**, no valor de **R$ 15.768,16**;
5.7.1.2.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;
5.7.1.2.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 15.768,16**.
5.7.1.3. Banco do Estado de Sergipe - ARP 25/2023 - Item 4
5.7.1.3.1. Na contratação utilizada como base, foi registrado preço para o **FortSwitch FS 124F-POE**, no valor de **R$ 15.182,63**;
5.7.1.3.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;
5.7.1.3.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 15.182,63**.
5.7.2. Visto que a estimativa não utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.1, do presente Anexo, o preço estimado para o ITEM 7 - SWITCH DE ACESSO TIPO 2 será a média dos valores obtidos, qual seja, **R$ 14.134,60**.

5.8. ITEM 8 - ACCESS POINT

5.8.1. Composição de Preços
5.8.1.1. SOLUS IT
5.8.1.1.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa SOLUS IT;
5.8.1.1.2. O valor unitário indicado na proposta do Item 8 - Access Point é de **R$ 4.647,01**.
5.8.1.2. WPI SOLUÇÕES EM TI
5.8.1.2.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa WPI SOLUÇÕES EM TI;
5.8.1.2.2. O valor unitário indicado na proposta do Item 8 - Access Point é de **R$ 5.350,00**.
5.8.1.3. VECTOR IT
5.8.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa VECTOR IT;
5.8.1.3.2. O valor unitário indicado na proposta do Item 8 - Access Point é de **R$ 5.507,80**.

5.8.2. Visto que a estimativa utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.2, do presente Anexo, o preço estimado para o ITEM 8 - ACCESS POINT é **R$ 4.647,01**.

5.9. ITEM 9 - FIREWALL DE NOVA GERAÇÃO (NGFW)

5.9.1. Composição de Preços

5.9.1.1. Secretaria de Estado da Educação e da Cultura de Sergipe - ARP 228/2023 - Item 2

5.9.1.1.1. Na contratação utilizada como base, foi registrado preço para o **FortiGate FG60F**, no valor de **R$ 16.147,00**;

5.9.1.1.2. A necessidade da presente contratação é compatível com o item registrado na contratação utilizada como base;

5.9.1.1.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 16.147,00**.

5.9.1.2. SOLUS IT

5.9.1.2.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa SOLUS IT;

5.9.1.2.2. O valor unitário indicado na proposta do ITEM 9 - FIREWALL DE NOVA GERAÇÃO (NGFW) é de **21.209,25**.

5.9.1.3. WPI SOLUÇÕES EM TI

5.9.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa WPI SOLUÇÕES EM TI;

5.9.1.3.2. O valor unitário indicado na proposta do ITEM 9 - FIREWALL DE NOVA GERAÇÃO (NGFW) é de **21.209,25**.

5.9.2. Visto que a estimativa não utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.1, do presente Anexo, o preço estimado para o ITEM 9 - FIREWALL DE NOVA GERAÇÃO (NGFW) será a média dos valores obtidos, qual seja, **R$ 19.521,83**.

5.10. ITEM 10 - TRANSCEIVER SFP+ 10GBase-SR

5.10.1. Composição de Preços

5.10.1.1. Secretaria da Educação de Sergipe - Pregão 228/2023 - Item 20

5.10.1.1.1. Na contratação utilizada como base, foi registrado preço para o **FN-TRAN-SFP+SR**, no valor de **R$ 756,00**;

5.10.1.1.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;

5.10.1.1.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 756,00**.

5.10.1.2. SOLUS IT

5.10.1.2.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa SOLUS IT;

5.10.1.2.2. O valor unitário indicado na proposta do ITEM 10 - TRANSCEIVER SFP+ 10GBase-SR é de **R$ 1.025,62**.

5.10.1.3. TECHLEAD

5.10.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa TECHLEAD;

5.10.1.3.2. O valor unitário indicado na proposta do ITEM 10 - TRANSCEIVER SFP+ 10GBase-SR é de **R$ 1.178,91**.

5.10.2. Visto que a estimativa não utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.1, do presente Anexo, o preço estimado para o ITEM 10 - TRANSCEIVER SFP+ 10GBase-SR será a média dos valores obtidos, qual seja, **R$ 986,84**.

5.11. ITEM 11 - TRANSCEIVER SFP+ 10GBase-LR

5.11.1. Composição de Preços

5.11.1.1. Secretaria da Educação de Sergipe - Pregão 228/2023 - Item 21

5.11.1.1.1. Na contratação utilizada como base, foi registrado preço para o **FN-TRAN-SFP+LR**, no valor de **R$ 1.399,00**;

5.11.1.1.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;

5.11.1.1.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 1.399,00**.

5.11.1.2. WPI SOLUÇÕES EM TI

5.11.1.2.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa WPI SOLUÇÕES EM TI;

5.11.1.2.2. O valor unitário indicado na proposta do ITEM 11 - TRANSCEIVER SFP+ 10GBase-LR é de **R$ 1.850,00**.

5.11.1.3. VECTOR IT

5.11.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa VECTOR IT;

5.11.1.3.2. O valor unitário indicado na proposta do ITEM 11 - TRANSCEIVER SFP+ 10GBase-LR é de **R$ 1.853,75**.

5.11.2. Visto que a estimativa não utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.1, do presente Anexo, o preço estimado para o ITEM 11 - TRANSCEIVER SFP+ 10GBase-LR será a média dos valores obtidos, qual seja, **R$ 1.700,92**.

5.12. ITEM 12 - TRANSCEIVER SFP 1000Base-LX

5.12.1. Composição de Preços

5.12.1.1. Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco - ARP 01/2023 - Item 5

5.12.1.1.1. Na contratação utilizada como base, foi registrado preço para o **TRANSCEIVER 1000BASE-LX**, no valor de **R$ 1.100,00**;

5.12.1.1.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;

5.12.1.1.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 1.100,00**.

5.12.1.2. Universidade Tecnológica Federal do Paraná - Item 24

5.12.1.2.1. Na contratação utilizada como base, foi registrado preço para o **FR-TRAN-LX**, no valor de **R$ 1.092,12**;

5.12.1.2.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;

5.12.1.2.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 1.092,12**.

5.12.1.3. SOLUS IT

5.12.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa SOLUS IT;

5.12.1.3.2. O valor unitário indicado na proposta do ITEM 12 - TRANSCEIVER SFP 1000Base-LX é de **R$ 1.286,76**.

5.12.2. Visto que a estimativa não utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.1, do presente Anexo, o preço estimado para o ITEM 12 - TRANSCEIVER SFP 1000Base-LX será a média dos valores obtidos, qual seja, **R$ 1.159,63**.

5.13. ITEM 13 - TRANSCEIVER SFP 1000Base-SX

5.13.1. Composição de Preços

5.13.1.1. VECTOR IT

5.13.1.1.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa VECTOR IT;

5.13.1.1.2. O valor unitário indicado na proposta do ITEM 13 - TRANSCEIVER SFP 1000Base-SX é de **R$ 624,50**.

5.13.1.2. Universidade Tecnológica Federal do Paraná - Item 23

5.13.1.2.1. Na contratação utilizada como base, foi registrado preço para o **FR-TRAN-SX**, no valor de **R$ 525,96**;

5.13.1.2.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;

5.13.1.2.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 525,96**.

5.13.1.3. WPI SOLUÇÕES EM TI

5.13.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa SOLUS IT;

5.13.1.3.2. O valor unitário indicado na proposta do ITEM 13 - TRANSCEIVER SFP 1000Base-SX é de **R$ 620,00**.

5.13.2. Visto que a estimativa não utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.1, do presente Anexo, o preço estimado para o ITEM 13 - TRANSCEIVER SFP 1000Base-SX será a média dos valores obtidos, qual seja, **R$ 590,15**.

5.14. ITEM 14 - SOLUÇÃO DE ZTNA (PACOTE DE 25 DISPOSITIVOS)

5.14.1. Composição de Preços

5.14.1.1. SOLUS IT

5.14.1.1.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa SOLUS IT;

5.14.1.1.2. O valor unitário indicado na proposta do ITEM 14 - SOLUÇÃO DE ZTNA é de **R$ 22.217,65**.

5.14.1.2. WPI SOLUÇÕES EM TI

5.14.1.2.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa WPI SOLUÇÕES EM TI;

5.14.1.2.2. O valor unitário indicado na proposta do ITEM 14 - SOLUÇÃO DE ZTNA é de **R$ 28.200,00**.

5.14.1.3. VECTOR IT

5.14.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa VECTOR IT;

5.14.1.3.2. O valor unitário indicado na proposta do ITEM 14 - SOLUÇÃO DE ZTNA é de **R$ 23.950,00**.

5.14.2. Visto que a estimativa utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.2, do presente Anexo, o preço estimado para o ITEM 14 - SOLUÇÃO DE ZTNA é **R$ 22.217,65**.

5.15. ITEM 15 - BANCO DE HORAS TÉCNICA

5.15.1. Composição de Preços

5.15.1.1. Banco do Estado de Sergipe - ARP 25/2023 - Item 7

5.15.1.1.1. Na contratação utilizada como base, foi registrado preço para **NIDADE DE SERVIÇOS TÉCNICO**, no valor de **R$ 703,44**;

5.15.1.1.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;

5.15.1.1.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 703,44**.

5.15.1.2. Procuradoria Geral de Justiça do Estado da Bahia - Pregão Eletrônico 41/2023 - Item 3 / Grupo 1

5.15.1.2.1. Na contratação utilizada como base, foi registrado preço para **Serviços Profissionais - Unidade De Serviços Técnicos**, no valor de **R$ 636,88**;

5.15.1.2.2. A necessidade da presente contratação é equivalente ao item registrado na contratação utilizada como base;

5.15.1.2.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 636,88**.

5.15.1.3. SOLUS IT

5.15.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa SOLUS IT;

5.15.1.3.2. O valor unitário indicado na proposta do ITEM 15 - BANCO DE HORAS TÉCNICA é de **R$ 900,00**.

5.15.2. Visto que a estimativa não utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.1, do presente Anexo, o preço estimado para o ITEM 15 - BANCO DE HORAS TÉCNICA será a média dos valores obtidos, qual seja, **R$ 746,77**.

5.16. ITEM 16 - SOLUÇÃO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA DE SEGURANÇA (SOAR)

5.16.1. Composição de Preços

5.16.1.1. SOLUS IT

5.16.1.1.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa SOLUS IT;

5.16.1.1.2. O valor unitário indicado na proposta do ITEM 16 - SOLUÇÃO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA DE SEGURANÇA (SOAR) é de **R$ 2.888.558,66**.

5.16.1.2. WPI SOLUÇÕES EM TI

5.16.1.2.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa WPI SOLUÇÕES EM TI;

5.16.1.2.2. O valor unitário indicado na proposta do ITEM 16 - SOLUÇÃO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA DE SEGURANÇA (SOAR) é de **R$ 2.900.000,00**.

5.16.1.3. VECTOR IT

5.16.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa VECTOR IT;

5.16.1.3.2. O valor unitário indicado na proposta do ITEM 16 - SOLUÇÃO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA DE SEGURANÇA (SOAR) é de **R$ 2.920.520,25**.

5.16.2. Visto que a estimativa utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.2, do presente Anexo, o preço estimado para o ITEM 16 - SOLUÇÃO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA DE SEGURANÇA (SOAR) é **R$ 2.888.558,66**.

5.17. ITEM 17 - TREINAMENTO OFICIAL - SWITCHES

5.17.1. Composição de Preços

5.17.1.1. TECHLEAD

5.17.1.1.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa TECHLEAD;

5.17.1.1.2. O valor unitário indicado na proposta do ITEM 17 - TREINAMENTO OFICIAL - SWITCHES é de **R$ 28.912,54**.

5.17.1.2. WPI SOLUÇÕES EM TI

5.17.1.2.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa WPI SOLUÇÕES EM TI;

5.17.1.2.2. O valor unitário indicado na proposta do ITEM 17 - TREINAMENTO OFICIAL - SWITCHES é de **R$ 36.500,00**.

5.17.1.3. VECTOR IT

5.17.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa VECTOR IT;

5.17.1.3.2. O valor unitário indicado na proposta do ITEM 17 - TREINAMENTO OFICIAL - SWITCHES é de **R$ 35.025,90**.

5.17.2. Visto que a estimativa utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.2, do presente Anexo, o preço estimado para o ITEM 17 - TREINAMENTO OFICIAL - SWITCHES é **R$ 28.912,54**.

5.18. ITEM 18 - TREINAMENTO OFICIAL - ACCESS POINTS

5.18.1. Composição de Preços

5.18.1.1. TECHLEAD

5.18.1.1.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa TECHLEAD;

5.18.1.1.2. O valor unitário indicado na proposta do ITEM 18 - TREINAMENTO OFICIAL - ACCESS POINTS é de **R$ 18.942,72**.

5.18.1.2. WPI SOLUÇÕES EM TI

5.18.1.2.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa WPI SOLUÇÕES EM TI;

5.18.1.2.2. O valor unitário indicado na proposta do ITEM 18 - TREINAMENTO OFICIAL - ACCESS POINTS é de **R$ 24.500,00**.

5.18.1.3. VECTOR IT

5.18.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa VECTOR IT;
5.18.1.3.2. O valor unitário indicado na proposta do ITEM 19 - TREINAMENTO OFICIAL - ACCESS POINTS é de **R$ 23.838,58**.

5.18.2. Visto que a estimativa utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.2, do presente Anexo, o preço estimado para o ITEM 18 - TREINAMENTO OFICIAL - ACCESS POINTS é **R$ 18.942,72**.

5.19. ITEM 19 - TREINAMENTO OFICIAL - CONTROLE DE ACESSO À REDE

5.19.1. Composição de Preços
5.19.1.1. TECHLEAD
5.19.1.1.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa TECHLEAD;
5.19.1.1.2. O valor unitário indicado na proposta do ITEM 19 - TREINAMENTO OFICIAL - CONTROLE DE ACESSO À REDE é de **R$ 28.912,54**.
5.19.1.2. SOLUS IT
5.19.1.2.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa SOLUS IT;
5.19.1.2.2. O valor unitário indicado na proposta do ITEM 19 - TREINAMENTO OFICIAL - CONTROLE DE ACESSO À REDE é de **R$ 36.385,19**.
5.19.1.3. VECTOR IT
5.19.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa VECTOR IT;
5.19.1.3.2. O valor unitário indicado na proposta do ITEM 19 - TREINAMENTO OFICIAL - CONTROLE DE ACESSO À REDE é de **R$ 35.023,10**.

5.19.2. Visto que a estimativa utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.2, do presente Anexo, o preço estimado para o ITEM 20 - TREINAMENTO OFICIAL - CONTROLE DE ACESSO À REDE é **R$ 28.912,54**.

5.20. ITEM 20 - TREINAMENTO OFICIAL - INFRAESTRUTURA E SEGURANÇA

5.20.1. Composição de Preços
5.20.1.1. VECTOR IT
5.20.1.1.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa VECTOR IT;
5.20.1.1.2. O valor unitário indicado na proposta do ITEM 20 - TREINAMENTO OFICIAL - INFRAESTRUTURA E SEGURANÇA é de **R$ 45.011,10**.
5.20.1.2. SOLUS IT
5.20.1.2.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa SOLUS IT;
5.20.1.2.2. O valor unitário indicado na proposta do ITEM 20 - TREINAMENTO OFICIAL - INFRAESTRUTURA E SEGURANÇA é de **R$ 25.974,90**.
5.20.1.3. WPI SOLUÇÕES EM TI
5.20.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa WPI SOLUÇÕES EM TI;
5.20.1.3.2. O valor unitário indicado na proposta do ITEM 20 - TREINAMENTO OFICIAL - INFRAESTRUTURA E SEGURANÇA é de **R$ 36.500,00**.

5.20.2. Visto que a estimativa utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.2, do presente Anexo, o preço estimado para o ITEM 20 - TREINAMENTO OFICIAL - INFRAESTRUTURA E SEGURANÇA é **R$ 25.974,90**.

5.21. ITEM 21 - TREINAMENTO OFICIAL - GERENCIAMENTO E RELATORIA

5.21.1. Composição de Preços
5.21.1.1. VECTOR IT
5.21.1.1.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa VECTOR IT;
5.21.1.1.2. O valor unitário indicado na proposta do ITEM 21 - TREINAMENTO OFICIAL - GERENCIAMENTO E RELATORIA é de **R$ 25.009,95**.
5.21.1.2. SOLUS IT
5.21.1.2.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa SOLUS IT;
5.21.1.2.2. O valor unitário indicado na proposta do ITEM 21 - TREINAMENTO OFICIAL - GERENCIAMENTO E RELATORIA é de **R$ 14.061,60**.
5.21.1.3. WPI SOLUÇÕES EM TI
5.21.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa WPI SOLUÇÕES EM TI;
5.21.1.3.2. O valor unitário indicado na proposta do ITEM 21 - TREINAMENTO OFICIAL - GERENCIAMENTO E RELATORIA é de **R$ 24.500,00**.

5.21.2. Visto que a estimativa utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.2, do presente Anexo, o preço estimado para o ITEM 21 - TREINAMENTO OFICIAL - GERENCIAMENTO E RELATORIA é **R$ 14.061,60**.

5.22. ITEM 22 - TREINAMENTO OFICIAL - SOLUÇÃO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA DE SEGURANÇA (SOAR)

5.22.1. Composição de Preços
5.22.1.1. TECHLEAD
5.22.1.1.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa TECHLEAD;
5.22.1.1.2. O valor unitário indicado na proposta do ITEM 22 - TREINAMENTO OFICIAL - SOLUÇÃO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA DE SEGURANÇA (SOAR) é de **R$ 18.942,72**.
5.22.1.2. SOLUS IT
5.22.1.2.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa SOLUS IT;
5.22.1.2.2. O valor unitário indicado na proposta do ITEM 22 - TREINAMENTO OFICIAL - SOLUÇÃO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA DE SEGURANÇA (SOAR) é de **R$ 20.493,18**.
5.22.1.3. WPI SOLUÇÕES EM TI
5.22.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa WPI SOLUÇÕES EM TI;
5.22.1.3.2. O valor unitário indicado na proposta do ITEM 22 - TREINAMENTO OFICIAL - SOLUÇÃO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA DE SEGURANÇA (SOAR) é de **R$ 24.500,00**.

5.22.2. Visto que a estimativa utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.2, do presente Anexo, o preço estimado para o ITEM 22 - TREINAMENTO OFICIAL - SOLUÇÃO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA DE SEGURANÇA (SOAR) é **R$ 18.942,72**.

5.23. ITEM 23 - IMPLANTAÇÃO COM HANDS ON – UST

5.23.1. Composição de Preços
5.23.1.1. Secretaria da Educação de Sergipe - Pregão 228/2023 - Item 26
5.23.1.1.1. Na contratação utilizada como base, foi registrado preço para o **Unidades de Serviços Técnicos para Implantação de Ativos de Rede Wired**, no valor de **R$ 1.157,00**;
5.23.1.1.2. A necessidade da presente contratação é compatível com o item registrado na contratação utilizada como base;
5.23.1.1.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 1.157,00**.
5.23.1.2. Instituto Federal de Educação, Ciência e Tecnologia de Pernambuco - ARP 01/2023

5.23.1.2.1. Na contratação utilizada como base, foi registrado preço para o **Serviço de Configuração da Solução de Redes e Segurança**, no valor de **R$ 1.392,00**;
5.23.1.2.2. A necessidade da presente contratação é compatível com o item registrado na contratação utilizada como base;
5.23.1.2.3. Dessa forma, o preço utilizado, para fins de estimativa é o valor registrado na contratação utilizada como base, qual seja, **R$ 1.392,00**.

5.23.1.3. TECHLEAD

5.23.1.3.1. Pela vantajosidade apresentada na proposta enviada, por solicitação de cotação direta, em relação às demais contratações utilizadas como base de pesquisa, foi utilizado o preço da proposta da empresa TECHLEAD;
5.23.1.3.2. O valor unitário indicado na proposta do TREINAMENTO OFICIAL - SOLUÇÃO DE ORQUESTRAÇÃO, AUTOMAÇÃO E RESPOSTA DE SEGURANÇA (SOAR) é de **R$ 800,00**.

5.23.2. Visto que a estimativa não utilizou somente preços obtidos através da cotação direta, conforme critério indicado no item 3.1, do presente Anexo, o preço estimado para o ITEM 25 - IMPLANTAÇÃO COM HANDS ON – UST será a média dos valores obtidos, qual seja, **R$ 1.116,33**.

Concluídos os procedimentos acima, encaminho a Informação Conclusiva sobre o Valor Estimado da Contratação acompanhada dos comprovantes de Cotação de Preços, Pesquisa de Mercado e demais fontes de consultas de composição do valor estimado, nos termos registrados neste formulário, bem como o ETP e TR/PB para apreciação e aprovação pela autoridade competente.

ANEXO V DO TERMO DE REFERÊNCIA
Análise de Riscos
MAPEAMENTO DE RISCOS

1. INTRODUÇÃO

O gerenciamento de riscos permite ações contínuas de planejamento, organização e controle dos recursos relacionados aos riscos que possam comprometer o sucesso da contratação, da execução do objeto e da gestão contratual.

O Mapa de Gerenciamento de Riscos deve conter a identificação e a análise dos principais riscos, consistindo na compreensão da natureza e determinação do nível de risco, que corresponde à combinação do impacto e de suas probabilidades que possam comprometer a efetividade da contratação, bem como o alcance dos resultados pretendidos com a solução de TIC.

Para cada risco identificado, define-se: a probabilidade de ocorrência dos eventos, os possíveis danos e impactos caso o risco ocorra, possíveis ações preventivas e de contingência (respostas aos riscos), a identificação de responsáveis pelas ações, bem como o registro e o acompanhamento das ações de tratamento dos riscos.

Os riscos identificados no projeto devem ser registrados, avaliados e tratados:

a) Durante a fase de planejamento, a equipe de Planejamento da Contratação deve proceder às ações de gerenciamento de riscos e produzir o Mapa de Gerenciamento de Riscos;
b) Durante a fase de Seleção do Fornecedor, o Integrante Administrativo, com apoio dos Integrantes Técnico e Requisitante, deve proceder às ações de gerenciamento dos riscos e atualizar o Mapa de Gerenciamento de Riscos;
c) Durante a fase de Gestão do Contrato, a Equipe de Fiscalização do Contrato, sob coordenação do Gestor do Contrato, deverá proceder à atualização contínua do Mapa de Gerenciamento de Riscos, procedendo à reavaliação dos riscos identificados nas fases anteriores com a atualização de suas respectivas ações de tratamento, e proceder também com a identificação, análise, avaliação e tratamento de novos riscos.

Como **exemplo**, parâmetros escalares podem ser utilizados para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis de risco, que direcionarão as ações relacionadas aos riscos durante as fases de contratação (planejamento, seleção de fornecedor e gestão do contrato).

Classificação	Valor
Baixo	5
Médio	10
Alto	15

Tabela 1 - Escala de Classificação de Probabilidade e Impacto

A tabela a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco:

Probabilidade (P)	15	**75**	**150**	**225**
	10	**50**	**100**	**150**
	5	**25**	**50**	**75**
		5	10	15
		Impacto (I)		

Tabela 2 - Matriz de Probabilidade x Impacto

O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz probabilidade x impacto. Caso o risco enquadre-se na região verde, seu nível de risco é entendido como baixo, logo admite-se a aceitação ou adoção das medidas preventivas. Se estiver na região amarela, entende-se como médio; e se estiver na região vermelha, entende-se como nível de risco alto. Nos casos de riscos classificados como médio e alto, deve-se adotar obrigatoriamente as medidas preventivas previstas.

2. IDENTIFICAÇÃO E ANÁLISE DOS PRINCIPAIS RISCOS

A tabela a seguir apresenta uma síntese dos riscos identificados e classificados neste documento:

ID	RISCO	RELACIONADO	P	I	NÍVEL DE RISCO (P X I)
R1	Alteração do escopo dos serviços a serem contratados	Planejamento da Contratação	5	10	**50**
R2	Atraso no processo administrativo de contratação	Planejamento da Contratação	5	10	**50**
R3	Atraso ou suspensão no processo licitatório em face de impugnações	Seleção do Fornecedor	10	10	**100**
R4	Valores licitados superiores aos estimados para a contratação dos serviços	Seleção do Fornecedor	10	10	**100**
R5	Contratação de fornecedor com baixa qualificação técnica	Seleção do Fornecedor	5	15	**75**
R6	Descumprimento dos níveis de serviço previstos no Planejamento da Contratação	Gestão Contratual	5	15	**75**

Tabela 3 - Identificação dos Riscos

3. AVALIAÇÃO E TRATAMENTO DOS RISCOS IDENTIFICADOS

Para o tratamento de riscos, as seguintes opções podem ser selecionadas: evitar, reduzir ou mitigar, transferir ou compartilhar, e aceitar ou tolerar o risco.

Os riscos de identificação R01 e R02 serão aceitos/tolerados, de forma que não haverá tratamento. Os demais riscos serão tratados de acordo com as tabelas abaixo:

RISCO R3	
Risco	Atraso ou suspensão no processo licitatório em face de impugnações
Probabilidade	Média
Impacto	Médio
Dano 1	Atraso na contratação e consequente atraso nas melhorias na operação e gerenciamento da rede interna de todo o TRE-AP

Tratamento	Mitigar	
ID	**AÇÃO PREVENTIVA**	**RESPONSÁVEL**
1	Elaboração do planejamento da contratação consultando soluções similares em outros órgãos	Equipe de Planejamento da Contratação
2	Definição dos critérios de seleção de fornecedores com respaldo na jurisprudência dos órgãos de controle	Equipe de Planejamento da Contratação
3	Verificação do teor de impugnações e recursos em contrações similares.	Equipe de Planejamento da Contratação
4	Estrita observância às recomendações da área jurídica do órgão/entidade.	Equipe de Planejamento da Contratação
ID	**AÇÃO DE CONTINGÊNCIA**	**RESPONSÁVEL**
1	Alocação integral da Equipe de Planejamento da Contratação na resposta e mitigação das causas que originaram a suspensão do processo licitatório.	Equipe de Planejamento da Contratação
2	Mitigação e eliminação das causas que obstruem o processo licitatório.	Equipe de Planejamento da Contratação

Tabela 4 - Tratamento do Risco R3

RISCO R4		
Risco	Valores licitados superiores aos estimados para a contratação dos serviços	
Probabilidade	Média	
Impacto	Médio	
Dano 1	Impossibilidade de adquirir os ativos de rede e segurança, caso o valor máximo para a contratação seja equivalente ao valor estimado e consequente atraso na implantação da solução.	
Dano 2	Atraso na contratação	
Tratamento	Mitigar	
ID	**AÇÃO PREVENTIVA**	**RESPONSÁVEL**
1	Concentrar mais esforços na pesquisa de preços	Equipe de Planejamento da Contratação
2	Contatar fornecedores	Equipe de Planejamento da Contratação
3	Comunicar maior quantidade de fornecedores possível, visando aumentar o nível de competição	Equipe de Planejamento da Contratação
ID	**AÇÃO DE CONTINGÊNCIA**	**RESPONSÁVEL**
1	Utilizar o que for possível dos preços registrados com valores adequados e permanecer utilizando a infraestrutura de rede atual, na medida do possível	SGIRC
2	Concentrar esforços para realização de nova contratação	Secretário de TI

Tabela 5 - Tratamento do Risco R4

RISCO R5		
Risco	Contratação de fornecedor com baixa qualificação técnica	
Probabilidade	Baixa	
Impacto	Médio	
Dano 1	Dificuldade para implantar a solução, bem como para buscar auxílio para reparos e gerenciamento, quando necessário	
Dano 2	Dificuldade de contato	
Dano 3	Atraso na entrega da solução	
Dano 4	Aumento das chances de baixa qualidade na prestação do serviço	
Tratamento	Mitigar	
ID	**AÇÃO PREVENTIVA**	**RESPONSÁVEL**
1	Inclusão de requisitos relativos à capacidade técnica do fornecedor nos Estudos Técnicos Preliminares	Equipe de Planejamento da Contratação
2	Verificar capacidade técnica da contratada junto a outros órgãos, se possível	Fiscal Técnico
3	Redobrar atenção no cumprimento de requisitos da contratação, pelo fornecedor	Fiscal Técnico
ID	**AÇÃO DE CONTINGÊNCIA**	**RESPONSÁVEL**
1	Reforçar monitoramento de SLAs, a fim de penalizar a empresa em caso de descumprimento	Fiscal Técnico
2	Recomendar aplicação de penalidades à empresa para regularização do serviço	Gestor do Contrato
3	Elaborar estudos visando uma nova contratação	

Tabela 6 - Tratamento do Risco R5

RISCO R6	
Risco	Descumprimento dos níveis de serviço previstos no Planejamento da Contratação
Probabilidade	Média
Impacto	Médio
Dano 1	Dificuldade de solucionar problemas e implantar novas funcionalidades, com apoio da CONTRATADA

Tratamento	Mitigar	
ID	**AÇÃO PREVENTIVA**	**RESPONSÁVEL**
1	Fiscalizar de forma efetiva a execução do contrato, a fim de não normalizar o descumprimento dos níveis de serviço	Fiscal Técnico
2	Aplicar glosas de acordo com o descumprimento dos níveis de serviço	Gestor do Contrato
3	Manter contato com a CONTRATADA e o Fabricante, a fim de manter o alinhamento na prestação de serviços relacionado aos equipamentos	Gestor do Contrato
4	Manter a equipe em constante aperfeiçoamento, para reduzir as hipóteses de necessidade de apoio da CONTRATADA	
ID	**AÇÃO PREVENTIVA**	**RESPONSÁVEL**
1	Adiar a implantação de melhorias, quando for o caso	SGIRC
2	Buscar soluções de rápida implantação, capazes de mitigar problemas, quando for o caso	Fiscal Técnico

Tabela 7 - Tratamento do Risco R6

ANEXO II DO EDITAL
ATA DE REGISTRO DE PREÇOS - ARP
TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ

ATA DE REGISTRO DE PREÇOS Nº ...../2024

O **TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ**, com sede Av. Mendonça Junior, 1.502, Centro, Macapá, Estado do Amapá, neste ato representado pelo senhor **FRANCISCO VALENTIM MAIA**, CPF nº xxx.651.522-xx, considerando o julgamento da licitação na modalidade de pregão, na forma eletrônica, para **REGISTRO DE PREÇOS nº ...../202..., publicada no ..... de ...../...../202.....,** processo administrativo SEI nº **0001999-17.2024.6.03.8000**, **RESOLVE** registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s), atendendo as condições previstas no Edital de licitação, sujeitando-se as partes às normas constantes na Lei nº 14.133, de 1º de abril de 2021, no Decreto n.º 11.462, de 31 de março de 2023, e em conformidade com as disposições a seguir:

1. DO OBJETO
1.1 A presente Ata tem por objeto o registro de preços para a eventual **aquisição de Rede e Segurança da Informação, incluindo Switches, Access Points, Firewalls, Soluções de Gerenciamento, Controle de Acesso e acessórios necessários, com garantia de pelo menos 60 (sessenta) meses, instalação, configuração da solução e treinamento**, especificado **no item 1** do Termo de Referência, anexo I **do edital de Licitação nº ...../2024**, que é parte integrante desta Ata, assim como as propostas cujos preços tenham sido registrados, independentemente de transcrição.

2 DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS
2.1 O preço registrado, as especificações do objeto, as quantidades mínimas e máximas de cada item, fornecedor(es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

Item do TR	Fornecedor (razão social, CNPJ/MF, endereço, contatos, representante)				
X	Especificação	Unidade	Quantidade	Valor Unit.	Prazo garantia ou validade

2.2 A listagem do cadastro de reserva referente ao presente registro de preços consta como anexo a esta Ata.

3.ÓRGÃO(S) GERENCIADOR E PARTICIPANTE(S)
3.1 O órgão gerenciador será o .....(nome do órgão)....
3.2{Além do gerenciador, não há [ou] São} órgãos e entidades públicas participantes do registro de preços:

Item nº	Órgãos Participantes	Unidade	Quantidade

4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS
4.1 Durante a vigência da ata, os órgãos e as entidades da Administração Pública federal, estadual, distrital e municipal que não participaram do procedimento de IRP poderão aderir à ata de registro de preços na condição de não participantes, observados os seguintes requisitos:
4.1.1 apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;
4.1.2 demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado na forma do art. 23 da Lei nº 14.133, de 2021; e
4.1.3 consulta e aceitação prévias do órgão ou da entidade gerenciadora e do fornecedor.
4.2 A autorização do órgão ou entidade gerenciadora apenas será realizada após a aceitação da adesão pelo fornecedor.
4.2.1 O órgão ou entidade gerenciadora poderá rejeitar adesões caso elas possam acarretar prejuízo à execução de seus próprios contratos ou à sua capacidade de gerenciamento.