PREGÃO ELETRÔNICO SRP Nº 90010/2024 - DPE
PARA AMPLA CONCORRÊNCIA

OBJETO: Registro de Preços para futura e eventual contratação de solução de cibersegurança e gestão de rede com fornecimento de equipamentos, licenças de softwares e serviços, , para solução de proteção e gerenciamento seguro da rede LAN/WLAN/WAN da Defensoria Pública do Estado do Pará – DPE/PA, para garantir a segurança da informação fim a fim e que possibilite a visibilidade e controle de tráfego e aplicações, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, conforme condições e exigências constantes neste Edital e seus anexos.

CRITÉRIO DE JULGAMENTO: MENOR PREÇO GLOBAL
MODO DE DISPUTA: ABERTO
VALOR ESTIMADO DA CONTRATAÇÃO POR PARTE DA DO GERENCIADOR: R$ 15.815.993,77
VALOR ESTIMADO DA CONTRATAÇÃO POR PARTE DA DOS PARTICIPES: R$ 43.006.467,67
DATA DA ABERTURA: 08 de outubro de 2024.

HORÁRIO: 10 h (dez) horas (horário de Brasília)

LOCAL: www.gov.br/compras

UASG CONTRATANTE: 925989

LOCAL, DIAS E HORÁRIOS PARA LEITURA OU OBTENÇÃO DESTE EDITAL:

LOCAL: nos sites www.gov.br/compras ou www.compraspara.pa.gov.br ou na Defensoria Pública do Estado do Pará, sito a Rua Padre Prudêncio, nº. 154, 2º andar – CLCC, Campina, Belém/Pará, sem custos, por meio de mídia digital.

ANEXOS:
- Termo de Referência;
- Estudo Técnico Preliminar;
- Modelo de Proposta;
- Minuta da Ata de Registro de Preços;
- Minuta de Contrato.

DEFENSORIA PÚBLICA DO ESTADO DO PARÁ
PREGÃO ELETRÔNICO Nº. 90010/2024-DPE
PROCESSO/PROTOCOLO Nº. 2024/2096228

A DEFENSORIA PÚBLICA DO ESTADO DO PARÁ torna público que realizará **licitação, na modalidade PREGÃO ELETRÔNICO SRP**, no tipo **MENOR PREÇO GLOBAL**, processada e julgada consoante a nos termos da Lei nº 14.133, de 1º de abril de 2021, do Decreto nº 11.462, de 31 de março de 2023, regulamentada pelo o Decreto Estadual no 2.939, de 10 de março de 2023, Decreto Estadual no 2.940, de 10 de março de 2023, Decreto estadual Nº 3.371, de 29 de setembro de 2023, e suas posteriores alterações, bem como pelas condições, exigências e recomendações contidas neste Ato Convocatório.

1. DO OBJETO:

1.1. O objeto da presente licitação é o Registro de Preços para futura e eventual Contratação de solução de cibersegurança e gestão de rede com fornecimento de equipamentos, licenças de softwares e serviços, para solução de proteção e gerenciamento seguro da rede LAN/WLAN/WAN da Defensoria Pública do Estado do Pará – DPE/PA, para garantir a segurança da informação fim a fim e que possibilite a visibilidade e controle de tráfego e aplicações, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede**,** conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.
1.2. A licitação será realizada em grupo único, formados por 06 itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

2. DO REGISTRO DE PREÇOS:

2.1. As regras referentes aos órgãos gerenciador e participantes, bem como a eventuais adesões são as que constam da minuta de Ata de Registro de Preços.

3. DA PARTICIPAÇÃO NA LICITAÇÃO:

3.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).
3.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicaf até o terceiro dia útil anterior à data prevista para recebimento das propostas.
3.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.
3.3. É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.
3.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

3.5. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015, bem como para bens e serviços produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010.
3.6. Não poderão disputar esta licitação:
3.6.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);
3.6.2. autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a licitação versar sobre serviços ou fornecimento de bens a ele relacionados;
3.6.3. empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a licitação versar sobre serviços ou fornecimento de bens a ela necessários;
3.6.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;
3.6.5. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;
3.6.6. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;
3.6.7. pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista;
3.6.8. agente público do órgão ou entidade licitante;
3.6.9. pessoas jurídicas reunidas em consórcio;
3.6.10. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;
3.6.11. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.
3.7. O impedimento de que trata o item 0 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.
3.8. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 0 e 0 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.
3.9. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

3.10. O disposto nos itens 0 e 0 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.
3.11. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133/2021.
3.12. A vedação de que trata o item 0 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

4. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO:
4.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.
4.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.
4.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 8.1.1 e 8.12.1 deste Edital.
4.4. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:
4.4.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório; não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;
4.4.2. não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;
4.4.3. cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.
4.5. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.
4.6. O fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.
4.6.1. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao

tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

4.7. A falsidade da declaração de que trata os itens 0 ou 0 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

4.8. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.

4.9. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.

Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.

4.10. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:

4.10.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e

4.10.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.

4.11. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:

4.11.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e

4.11.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.

4.12. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 0 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.

4.13. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

4.14. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

5. DO PREENCHIMENTO DA PROPOSTA:

5.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

5.1.1. *valor do item;*

5.1.2. Marca;

5.1.3. Fabricante;

5.1.4. Quantidade cotada.

5.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.

5.2.1. O licitante não poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.
5.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.
5.4. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.
5.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.
5.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.
5.7. Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional.
5.8. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.
5.9. O prazo de validade da proposta não será inferior a **90 (noventa)** dias**,** a contar da data de sua apresentação.
5.10. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;
5.10.1. Caso o critério de julgamento seja o de maior desconto, o preço já decorrente da aplicação do desconto ofertado deverá respeitar os preços máximos previstos no item 4.9.
5.11. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

6. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES:

6.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.
6.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.
6.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.
6.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.
6.5. O lance deverá ser ofertado pelo valor unitário do item.

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

6.7. O licitante somente poderá oferecer lance *de valor inferior* ao último por ele ofertado e registrado pelo sistema.

6.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de R$ 0,01 (um centavo).

6.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.

6.10. O procedimento seguirá de acordo com o modo de disputa adotado.

6.11. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto”, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

6.11.1. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

6.11.2. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

6.11.3. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

6.11.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

6.11.5. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

6.12. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

6.12.1. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.

6.12.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

6.12.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.

6.12.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.

6.12.5. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

6.13. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa "fechado e aberto", poderão participar da etapa aberta somente os licitantes que apresentarem a proposta de menor preço/ maior percentual de desconto e os das propostas até 10% (dez por cento) superiores/inferiores àquela, em que os licitantes apresentarão lances públicos e sucessivos, até o encerramento da sessão e eventuais prorrogações.

6.13.1. Não havendo pelo menos 3 (três) propostas nas condições definidas no item 6.13, poderão os licitantes que apresentaram as três melhores propostas, consideradas as empatadas, oferecer novos lances sucessivos.

6.13.2. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.

6.13.3. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

6.13.4. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação.

6.13.5. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

6.13.6. Após o reinício previsto no subitem supra, os licitantes serão convocados para apresentar lances intermediários.

6.14. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.

6.15. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.

6.16. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.

6.17. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

6.18. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.

6.19. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

6.20. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos arts. 44 e 45 da Lei Complementar nº 123, de 2006, regulamentada pelo Decreto nº 8.538, de 2015.

6.20.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.

6.20.2. A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.

6.20.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.

6.20.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.

6.21. Será assegurado o direito de preferência previsto no artigo 3º da Lei nº 8.248, de 1991, conforme procedimento estabelecido nos artigos 5° e 8° do Decreto n° 7.174, de 2010, nos seguintes termos:

6.21.1. Após a aplicação das regras de preferência para microempresas e empresas de pequeno porte, caberá a aplicação das regras de preferência, sucessivamente, para:

6.21.1.1. bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

6.21.1.2. bens e serviços com tecnologia desenvolvida no País; e

6.21.1.3. bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal, nos termos do art. 5º e 8º do Decreto 7.174, de 2010 e art. 3º da Lei nº 8.248, de 1991.

6.21.2. Os licitantes classificados que estejam enquadrados no item 6.21.1.1, na ordem de classificação, serão convocados para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarado vencedor do certame.

6.21.3. Caso a preferência não seja exercida na forma do item 6.21.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 6.21.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 6.21.1.3 caso esse direito não seja exercido.

6.21.4. As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.

6.22. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.

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

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

6.22.1.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

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

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

6.22.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

6.22.2.1. empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

6.22.2.2. empresas brasileiras;

6.22.2.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

6.22.2.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

6.23. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

6.23.1. A negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração.

6.23.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

6.23.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

6.23.4. O pregoeiro solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

6.23.5. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

6.24. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

7. DA FASE DE JULGAMENTO:

7.1. Encerrada a etapa de negociação, o pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 0 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

7.1.1. SICAF;

7.1.2. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

7.1.3. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

7.2. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

7.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. (IN nº 3/2018, art. 29, *caput*)

7.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. (IN nº 3/2018, art. 29, §1º).

7.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. (IN nº 3/2018, art. 29, §2º).

7.3.3. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

7.4. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

7.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com os itens **Erro! Fonte de referência não encontrada.** e 0 deste edital.

7.6. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos, observado o disposto no artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022.

7.7. Será desclassificada a proposta vencedora que:

7.7.1. contiver vícios insanáveis;

7.7.2. não obedecer às especificações técnicas contidas no Termo de Referência;

7.7.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

7.7.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

7.7.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

7.8. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

7.9. Caso o custo global estimado do objeto licitado tenha sido decomposto em seus respectivos custos unitários por meio de Planilha de Custos e Formação de Preços elaborada pela Administração, o licitante classificado em primeiro lugar será convocado para apresentar Planilha por ele elaborada, com os respectivos valores adequados ao valor final da sua proposta, sob pena de não aceitação da proposta.

7.9.1. Em se tratando de serviços com fornecimento de mão de obra em regime de dedicação exclusiva cuja produtividade seja mensurável e indicada pela Administração, o licitante deverá indicar a produtividade adotada e a quantidade de pessoal que será alocado na execução contratual.

7.9.2. Caso a produtividade for diferente daquela utilizada pela Administração como referência, ou não estiver contida na faixa referencial de produtividade, mas admitida pelo ato convocatório, o licitante deverá apresentar a respectiva comprovação de exequibilidade;

7.9.3. Os licitantes poderão apresentar produtividades diferenciadas daquela estabelecida pela Administração como referência, desde que não alterem o objeto da contratação, não contrariem dispositivos legais vigentes e, caso não estejam contidas nas faixas referenciais de produtividade, comprovem a exequibilidade da proposta.

7.9.4. Para efeito do subitem anterior, admite-se a adequação técnica da metodologia empregada pela contratada, visando assegurar a execução do objeto, desde que mantidas as condições para a justa remuneração do serviço.

7.10. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço e que se comprove que este é o bastante para arcar com todos os custos da contratação;

7.11. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

7.12. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

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

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

7.15. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a avaliação das amostras, cuja presença será facultada a todos os interessados, incluindo os demais licitantes.

7.16. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

7.17. No caso de não haver entrega da amostra ou ocorrer atraso na entrega, sem justificativa aceita pelo Pregoeiro, ou havendo entrega de amostra fora das especificações previstas neste Edital, a proposta do licitante será recusada.

7.18. Se a(s) amostra(s) apresentada(s) pelo primeiro classificado não for(em) aceita(s), o Pregoeiro analisará a aceitabilidade da proposta ou lance ofertado pelo segundo classificado. Seguir-se-á com a verificação da(s) amostra(s) e, assim, sucessivamente, até a verificação de uma que atenda às especificações constantes no Termo de Referência.

7.19. Caso o Termo de Referência exija prova de conceito, o licitante classificado em primeiro lugar será convocado pelo pregoeiro, com antecedência mínima de 01 (um) dia útil da data estabelecia para sua realização, para executá-la, visando aferir o atendimento dos requisitos e funcionalidades mínimas da solução de tecnologia da informação e comunicação, conforme disciplinado no Termo de Referência.

7.20. Por meio de mensagem no sistema, será divulgado o local e horário de realização do procedimento para a realização da prova de conceito.

7.21. A prova de conceito será realizada por equipe técnica designada, responsável pela aferição do atendimento dos itens estabelecidos, e poderá ser acompanhada pelos demais licitantes, mediante registro formal junto ao pregoeiro.

7.22. Todas as despesas decorrentes de participação ou acompanhamento da prova de conceito são de responsabilidade de cada um dos licitantes.

7.23. A equipe técnica elaborará relatório com o resultado da prova de conceito, informando se a solução apresentada pelo licitante provisoriamente classificado em primeiro lugar está ou não de acordo com os requisitos e funcionalidades estabelecidas.

7.24. Caso o relatório indique que a solução tecnológica está em conformidade com as especificações exigidas, o licitante será declarado vencedor do processo licitatório e, caso indique a não conformidade, o licitante será desclassificado do processo licitatório.

7.25. Caso o relatório indique que a solução foi aprovada com ressalvas, as não conformidades serão listadas e o licitante terá prazo de 3 (três) dias úteis, não prorrogáveis, a contar da data de ciência do respectivo relatório, para proceder aos ajustes necessários na solução e disponibilizá-la, para a realização de testes complementares, para aferição da correção ou não das inconformidades indicada.

7.26. Poderá ser considerada aprovada com ressalva a solução que, embora possua todas as funcionalidades previstas na Prova de Conceito (POC), venha a apresentar falha durante o teste.

7.27. Caso o novo relatório indique a não conformidade da solução ajustada às especificações técnicas exigidas, a licitante será desclassificada do processo licitatório.

7.28. Não será aceita a proposta da licitante que tiver a prova de conceito rejeitada, que não a realizar ou que não a realizar nas condições estabelecidas no Termo de Referência.

7.29. No caso de desclassificação do licitante, o pregoeiro convocará o próximo licitante, obedecida a ordem de classificação, sucessivamente, até que um licitante cumpra os requisitos e funcionalidades previstas na POC.

7.30. Os resultados das avaliações serão divulgados por meio de mensagem no sistema.

8. DA FASE DE HABILITAÇÃO:

8.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos arts. 62 a 70 da Lei nº 14.133, de 2021.

8.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

8.2. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

8.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

8.4. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, por cópia enviada por meio eletrônico.

8.5. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.

8.6. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021).

8.7. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

8.8. O licitante deverá apresentar, sob pena de desclassificação, declaração de que suas propostas econômicas compreendem a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

8.9. Visando subsidiar a adequada elaboração das propostas das LICITANTES, é optativa a realização da vistoria no local de implantação da solução. Se considerada necessária, deverá ser feita por responsável técnico da empresa. A vistoria deverá ser agendada e realizada até 02 (dois) dias úteis antes da abertura do certame licitatório.

8.9.1. O agendamento deve ser realizado no Prédio SEDE - Rua Padre Prudêncio, nº 154, Belém - Pará - Brasil. CEP: 66019-080 - Fone: (91) 3201-2684, pelo telefone (91) 3201-2684 ou e-mail cetic@defensoria.pa.def.br, no horário de 09h às 12h e/ou 14h às 17h. até 02 (dois) dias úteis antes da abertura do certame licitatório.

8.9.2. A LICITANTE deverá apresentar Declaração de Vistoria, caso a realize.

8.9.3. Caso a LICITANTE não realize a vistoria, estará ciente que deverá OPTOU PELA NÃO REALIZAÇÃO DA VISTORIA TÉCNICA NAS INSTALAÇÕES FÍSICAS DA DEFENSORIA PÚBLICA, tendo pleno conhecimento das informações para o cumprimento das obrigações, objeto da licitação, e não poderá alegar em qualquer fase da licitação ou vigência da relação contratual que não realizará os serviços em conformidade com a qualidade e requisitos exigidos.

8.10. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.

8.10.1. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

8.11. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados. (IN nº 3/2018, art. 7º, *caput*).

8.11.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. (IN nº 3/2018, art. 7º, parágrafo único).

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

8.12.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de 02 (duas) horas, prorrogável por igual período, contado da solicitação do pregoeiro.

8.12.2. Na hipótese de a fase de habilitação anteceder a fase de apresentação de propostas e lances, os licitantes encaminharão, por meio do sistema, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto no § 1º do art. 36 e no § 1º do art. 39 da *Instrução Normativa SEGES nº 73, de 30 de setembro de 2022*.

8.13. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

8.13.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.

8.13.2. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.

8.14. Após a entrega dos documentos para habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º):

8.14.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e

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

8.15. Na análise dos documentos de habilitação, a comissão de contratação poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

8.16. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 8.12.1.

8.17. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

8.18. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação (art. 4º do Decreto nº 8.538/2015).

8.19. Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

9. DA ATA DE REGISTRO DE PREÇOS:

9.1. Homologado o resultado da licitação, o licitante mais bem classificado terá o prazo de 10 (dez) dias, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decadência do direito à contratação, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

9.2. O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação do licitante mais bem classificado ou do fornecedor convocado, desde que:

9.2.1. a solicitação seja devidamente justificada e apresentada dentro do prazo; e

9.2.2. a justificativa apresentada seja aceita pela Administração.

9.3. A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no sistema de registro de preços.

9.4. Serão formalizadas tantas Atas de Registro de Preços quantas forem necessárias para o registro de todos os itens constantes no Termo de Referência, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.

9.5. O preço registrado, com a indicação dos fornecedores, será divulgado no PNCP e disponibilizado durante a vigência da ata de registro de preços.

9.6. O preço registrado poderá ser reajustado ou suprimido, nos termos da Lei Federal nº 14.133/2021 e Decreto estadual Nº 3.371, de 29 de setembro de 2023.

9.7. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.

9.8. Na hipótese de o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidas, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

10. DA FORMAÇÃO DO CADASTRO DE RESERVA:

10.1. Após a homologação da licitação, será incluído na ata, na forma de anexo, o registro:

10.1.1. dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário, observada a classificação na licitação; e

10.1.2. dos licitantes que mantiverem sua proposta original.

10.2. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou fornecedores registrados na ata.

10.2.1. A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante mais bem classificado.

10.2.2. Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem cotar o objeto com preço igual ao do adjudicatário antecederão aqueles que mantiverem sua proposta original.

10.3. A habilitação dos licitantes que comporão o cadastro de reserva será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

10.3.1. quando o licitante vencedor não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital; ou

10.3.2. quando houver o cancelamento do registro do fornecedor ou do registro de preços, nas hipóteses previstas nos art. 28 e art. 29 do Decreto nº 11.462/23.

10.4. Na hipótese de nenhum dos licitantes que aceitaram cotar o objeto com preço igual ao do adjudicatário concordar com a contratação nos termos em igual prazo e nas condições propostas pelo primeiro classificado, a Administração, observados o valor estimado e a sua eventual atualização na forma prevista no edital, poderá:

10.4.1. convocar os licitantes que mantiveram sua proposta original para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

10.4.2. adjudicar e firmar o contrato nas condições ofertadas pelos licitantes remanescentes, observada a ordem de classificação, quando frustrada a negociação de melhor condição.

11. DOS RECURSOS:

11.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

11.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.

11.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

11.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;

11.3.1.1. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.

11.3.2. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;

11.3.3. na hipótese de adoção da inversão de fases prevista no § 1º do art. 17 da Lei nº 14.133, de 2021, o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.

11.4. Os recursos deverão ser encaminhados em campo próprio do sistema.

11.5. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.

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

11.7. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.

11.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

11.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.

11.10. Os autos do processo permanecerão acessíveis aos interessados por meio do Portal ComprasPará.

12. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES:

12.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

12.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;

12.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:

12.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;

12.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;

12.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou

12.1.2.4. deixar de apresentar amostra;

12.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

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

12.1.3.1. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;

12.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;

12.1.5. fraudar a licitação;

12.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

12.1.6.1. agir em conluio ou em desconformidade com a lei;

12.1.6.2. induzir deliberadamente a erro no julgamento;

12.1.6.3. apresentar amostra falsificada ou deteriorada;

12.1.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação

12.1.8. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

12.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

12.2.1. advertência;

12.2.2. multa;

12.2.3. impedimento de licitar e contratar e

12.2.4. declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

12.3. Na aplicação das sanções serão considerados:

12.3.1. a natureza e a gravidade da infração cometida.

12.3.2. as peculiaridades do caso concreto

12.3.3. as circunstâncias agravantes ou atenuantes

12.3.4. os danos que dela provierem para a Administração Pública

12.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de **10 (dez) dias** úteis, a contar da comunicação oficial.

12.4.1. Para as infrações previstas nos itens 12.1.1, 12.1.2 e 12.1.3, a multa será de 0,5% a 15% do valor do contrato licitado.

12.4.2. Para as infrações previstas nos itens 12.1.4, 12.1.5, 12.1.6, 12.1.7 e 12.1.8, a multa será de 15% a 30% do valor do contrato licitado.

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

12.6. Na aplicação da sanção de multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

12.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 12.1.1, 12.1.2 e 12.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

12.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 12.1.4, 12.1.5, 12.1.6, 12.1.7 e 12.1.8, bem como pelas infrações administrativas previstas nos itens 12.1.1, 12.1.2 e 12.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

12.9. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 12.1.3, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

12.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as provas que pretenda produzir.
12.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.
12.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.
12.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.
12.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

13. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO:

13.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.
13.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.
13.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, pelo e-mail: *licitacao@defensoria.pa.def.br*.
13.4. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.
13.4.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.
13.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

14. DAS DISPOSIÇÕES GERAIS:

14.1. Será divulgada ata da sessão pública no sistema eletrônico.
14.2. 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.
14.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.
14.4. A homologação do resultado desta licitação não implicará direito à contratação.

14.5. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.
14.6. Os licitantes assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo licitatório.
14.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.
14.8. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.
14.9. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.
14.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico www.compraspara.pa.gov.br.
14.11. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

14.1.1. ANEXO I - Termo de Referência
14.1.1.1. Apêndice do Anexo I – Estudo Técnico Preliminar
14.1.2. ANEXO II – *Modelo de Proposta*
14.1.3. ANEXO III – Minuta de Ata de Registro de Preços
14.1.4. ANEXO IV –Minuta de Termo de Contrato

15. DO FORO:
15.1. Fica eleito o Foro da cidade de Belém/PA, como competente para dirimir quaisquer questões oriundas do presente Edital, que não puderem ser resolvidas pela via administrativa, com renúncia de qualquer outro, por mais privilegiado que seja.

Belém, 20 de setembro de 2024.

MÔNICA PALHETA FURTADO BELÉM
Defensora Pública Geral do Estado do Pará

ANEXO I

PREGÃO ELETRÔNICO Nº. 90010/2024-DPE
PROCESSO/PROTOCOLO Nº. 2024/2096228
TERMO DE REFERÊNCIA

DO OBJETO

Registro de Preços para futura e eventual contratação de solução de cibersegurança e gestão de rede com fornecimento de equipamentos, licenças de softwares e serviços, conforme quantidades e exigências estabelecidas neste Termo de Referência, para solução de proteção e gerenciamento seguro da rede LAN/WLAN/WAN da Defensoria Pública do Estado do Pará – DPE/PA, para garantir a segurança da informação fim a fim e que possibilite a visibilidade e controle de tráfego e aplicações, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, de acordo com as especificações e quantitativos previstos neste Termo.

Este objeto será realizado através de licitação na modalidade PREGÃO, na forma ELETRÔNICA, do tipo MENOR PREÇO, com a forma de fornecimento por demanda.

DA JUSTIFICATIVA

A Defensoria Pública do Estado do Pará – DPE/PA tem como meta estratégica na Tecnologia da Informação e Comunicação - TIC a disponibilização de ferramentas tecnológicas que garantam o adequado funcionamento do ambiente tecnológico e que colaborem com a melhoria da produtividade dos seus usuários. Portanto, assim como os outros poderes que compõem a estrutura de Estado, a DPE/PA necessita de proteção e segurança sobre o conteúdo armazenado e manipulado internamente nos respectivos ambientes para que sejam mantidas a confidencialidade, a integridade e a disponibilidade das informações existentes.

Os seguintes fatores motivaram essa contratação:

- Reforço da segurança cibernética das unidades da Defensoria Pública do Pará;
- Aumento da quantidade de ataques maliciosos às aplicações oferecidas pela DPE;
- Aumento nos sistemas informatizados;

Os seguintes resultados são esperados:

- Disponibilidade de sistemas e aplicações da DPE (Solar, Intranet, Sistema de Diária, etc);
- Reforço da estrutura de Segurança da Informação, principalmente em virtude do aumento massivo de ataques cibernéticos a órgãos governamentais.
- Minimizar o risco de continuidade do negócio por ataques à infraestrutura de TI.
- Melhorar o nível de segurança de dados da Defensoria Pública do Estado do Pará;
- Controlar os usuários que entram na rede corporativa;
- Controlar o acesso aos aplicativos e recursos que os usuários pretendem acessar;
- Permitir que contratados, parceiros e convidados entrem na rede conforme necessário, mas restrinja seu acesso;
- Segmentar funcionários em grupos com base em sua função de trabalho e crie políticas de acesso baseadas em função;

- Proteger contra ataques cibernéticos implementando sistemas e controles que detectam atividades incomuns ou suspeitas;
- Automatizar a resposta a incidentes;
- Gerar relatórios e insights sobre tentativas de acesso em toda a instituição;
- Reduzir a proliferação de dispositivos nas unidades de todo estado combinando firewalls, switches e pontos de acesso wi-fi em uma única solução, permitindo o gerenciamento integrado de serviços de rede.
- Consolidar a identificação, autenticação, autorização, detecção e resposta dos incidentes de segurança.

Diversos fatores impulsionaram essa consolidação, como a busca por redução de custos, aumento da produtividade, melhora da mobilidade, flexibilidade e escalabilidade. Os benefícios da integração são numerosos, incluindo eficiência na gestão da infraestrutura e dos processos, agilidade na comunicação entre colaboradores, flexibilidade para se adaptar às necessidades da instituição!ão e segurança contra ataques cibernéticos. Apesar dos desafios, as tendências para o futuro da gestão de redes são promissoras, com a integração da inteligência artificial, migração para a nuvem e integração de dispositivos da Internet das Coisas (IoT) à plataforma de comunicação. Exemplos de soluções convergentes que já estão disponíveis no mercado e que hoje utilizamos na Defensoria, como o Google Workspace, para atender às nossas necessidades.

No cenário atual, caracterizado por ameaças cibernéticas em constante evolução e pela necessidade de uma infraestrutura de TI ágil e eficiente, a consolidação das tecnologias de conectividade de rede corporativa emerge como uma necessidade imperativa. Esta iniciativa visa integrar redes wireless, controle de admissão à rede e soluções robustas de segurança cibernética em uma única plataforma. Para a DPE-PA, tal consolidação é estratégica, garantindo não apenas a eficiência operacional, mas também a segurança e a confiabilidade de sua infraestrutura de rede.

A base para esta justificativa reside em três premissas fundamentais: a necessidade de uma conectividade de rede ininterrupta, a demanda por uma infraestrutura robusta e flexível e a importância primordial da segurança cibernética. No contexto da DPE-PA, uma organização que depende criticamente de seus sistemas de TI para a prestação de serviços jurídicos essenciais, estas premissas são inegociáveis.

A consolidação visa abordar várias necessidades cruciais. Primeiramente, reduzir a complexidade e o custo de gerenciamento de múltiplas redes, uma vez que a diversidade de soluções fragmentadas pode aumentar os riscos operacionais e os custos. Além disso, busca-se melhorar a performance da rede, aumentando a velocidade, confiabilidade e disponibilidade - fatores que são diretamente proporcionais à capacidade da DPE-PA de responder de maneira eficiente às necessidades de seus usuários. A segurança aprimorada, através de medidas robustas de proteção e controle de acesso granular, é outra necessidade vital, permitindo o acesso seguro à rede e alinhando-se às melhores práticas de segurança da informação.

Os benefícios de tal consolidação são abrangentes. Primeiramente, observa-se uma redução significativa de custos relacionados à aquisição, manutenção e gerenciamento da infraestrutura de rede. A melhoria na performance da rede não só aumenta a produtividade como também garante maior agilidade nos processos operacionais. A segurança da rede é consideravelmente reforçada, protegendo a organização contra-ataques cibernéticos e acesso não autorizado. Além disso, a maior flexibilidade permite uma fácil expansão e adaptação da rede às necessidades em constante mudança da organização, enquanto o gerenciamento simplificado facilita a administração e o controle centralizado.

Propõe-se a consolidação das tecnologias de conectividade de rede corporativa em uma única plataforma, que abranja tanto a rede cabeada quanto a rede sem fio, o controle de admissão à rede, e soluções robustas de segurança cibernética. Esta plataforma escalável, adaptando-se ao crescimento da organização e às novas demandas de conectividade. A segurança avançada e a conformidade com os padrões de segurança da informação são imperativos, assim como a gestão centralizada, que simplifica a administração e o controle da rede.

A consolidação das tecnologias de conectividade de rede corporativa representa um investimento estratégico crucial para a DPE-PA. Essa iniciativa não só garante a eficiência, segurança e confiabilidade da infraestrutura de rede, mas também traz benefícios tangíveis como a redução de custos, aumento da produtividade, segurança reforçada e maior flexibilidade. A implementação de uma plataforma consolidada posiciona a DPE-PA como uma organização ágil e resiliente, pronta para enfrentar os desafios tecnológicos atuais e futuros ao considerar a justificativa para a consolidação de tecnologias de conectividade de rede corporativa na Defensoria Pública do Estado do Pará (DPE-PA).

A argumentação abordada anteriormente é fortalecida e ampliada pela integração e simplificação de gestão, pela segurança aprimorada, pela resiliência e confiabilidade, pela eficiência operacional e redução de custos, e pela adaptação às evoluções das necessidades de negócios. Além disso, aspectos como compatibilidade e interoperabilidade, atualizações e manutenção simplificadas, redução de silos operacionais, análise de dados aprimorada, resposta a incidentes acelerada, conformidade regulatória facilitada, e a melhoria na experiência do usuário ressaltam a importância estratégica desta consolidação.

No âmbito técnico, a consolidação permite abordar desafios como desempenho e escalabilidade, essenciais para atender às demandas atuais e futuras da DPE-PA. Garantir a confiabilidade e a segurança em um cenário de ameaças cibernéticas em evolução é crucial para proteger os dados sensíveis e as operações da instituição. Além disso, o gerenciamento e provisionamento eficientes facilitam a administração da rede, otimizando recursos e antecipando problemas. A integração e interoperabilidade com sistemas de TI existentes e novas tecnologias asseguram a flexibilidade e proteção do investimento em infraestrutura.

A escolha de soluções que se alinham com objetivos de sustentabilidade reflete o compromisso da DPE-PA com práticas responsáveis, um aspecto cada vez mais relevante no cenário atual.

Historicamente, a jornada tecnológica transitou por diversas fases, iniciando-se em uma era de simplicidade, onde as redes eram fundamentadas em cabos físicos e topologias básicas, a conectividade era limitada e a segurança focava em medidas periféricas. Esta fase foi seguida por um período de complexidade caracterizado pela adoção de IP, virtualização, e um crescimento exponencial tanto em dispositivos conectados quanto em ameaças de segurança, culminando na era atual de convergência. Neste estágio, tecnologias como Software Defined Networking (SDN), automação, nuvem híbrida, e 5G tornaram-se preponderantes, enquanto a segurança evoluiu para incorporar estratégias como Zero Trust e micro segmentação, amplamente apoiadas pela análise de comportamento e capacidades preditivas da IA.

A IA, nesta sinfonia tecnológica, atua como o maestro, orquestrando uma harmonização entre a otimização da infraestrutura de rede, a personalização da conectividade e a prevenção proativa de ameaças de segurança. Por meio da automação, análise de dados e aprendizado contínuo, a IA permite que redes se ajustem dinamicamente, personalizem a experiência do usuário em dispositivos

e plataformas, e identifica ameaças em potencial antes mesmo que se concretizem, garantindo uma proteção mais robusta e adaptável.

A implementação prática dessa convergência se manifesta através de monitoramento em tempo real, resposta automatizada a incidentes e proteção contra ataques direcionados, demonstrando a capacidade da IA de aprender com o passado para proteger o futuro. Contudo, apesar das oportunidades significativas como aumento de eficiência, segurança aprimorada e experiências de usuário enriquecidas, existem desafios notáveis. A integração de tecnologias emergentes, o gerenciamento eficaz de grandes volumes de dados e o desenvolvimento de competências especializadas em IA representam obstáculos significativos.

Em estudo recente, do renomado Gartner Group, veiculou relatório de janeiro deste ano, 2024, consolidou a abordagem de conectividade cabeada a redes sem fio com detecção de intrusos, abordando aspectos de segurança na infraestrutura de conectividade, escalabilidade, autenticação integrada e telemetria para otimização da rede, assim como a integração e o monitoramento do comportamento das ações de usuários, e aspectos relevantes de inteligência artificial, com visibilidade e gerenciamento de desempenho. Neste viés, apresento o quadrante mágico de fornecedores, onde nomeiam os líderes, no quadrante superior à direita.

https://www.gartner.com/en/documents/5253763

Conclui-se, portanto, que a convergência de infraestrutura de rede, conectividade e segurança da informação, sob a regência da inteligência artificial, não é meramente uma tendência, mas uma evolução inevitável no domínio tecnológico. Esta progressão não apenas habilita organizações a enfrentar desafios futuros com maior resiliência, mas também pavimenta o caminho para uma era de inovações sem precedentes, onde a segurança e a eficiência coexistem em perfeita harmonia.

Esses aspectos sublinham a importância de uma abordagem consolidada nas contratações, na qual a seleção de um fornecedor único capaz de entregar uma solução integrada e holística se

apresenta como a estratégia mais eficaz. Além de mitigar os riscos de incompatibilidade, segurança e gestão, essa abordagem unificada minimiza as chances de desvios nos prazos de entrega e as incertezas relacionadas à seleção dos fornecedores, assegurando uma implementação mais fluida e coordenada das tecnologias necessárias.

Para a Defensoria Pública do Estado do Pará, é imperativo considerar esses fatores ao planejar suas contratações, optando por soluções que promovam a integração, eficiência e resiliência operacional. Uma estratégia de contratação bem delineada, focada na simplificação e na segurança, é fundamental para garantir a continuidade e a qualidade dos serviços oferecidos à população, alinhando-se aos objetivos estratégicos e operacionais da DPE-PA.

Na era contemporânea da tecnologia, observa-se uma tendência inevitável rumo à convergência de infraestrutura de rede, conectividade e segurança da informação, uma transformação amplamente impulsionada pelos avanços em inteligência artificial (IA). Esta metamorfose tecnológica, relembrança da evolução musical de simples melodias para complexas sinfonias, reflete uma resposta versátil aos crescentes desafios de segurança cibernética e à crescente influência da IA sobre o cenário tecnológico.

Em suma, a consolidação das tecnologias de conectividade de rede corporativa é um passo estratégico fundamental para a DPE-PA, promovendo uma gestão mais eficiente, segurança reforçada, e capacidade de adaptar-se às exigências futuras. A implementação de uma infraestrutura unificada traz benefícios tangíveis em termos de redução de custos, aumento da produtividade, e maior flexibilidade, alinhando a organização com as melhores práticas e tendências do mercado. Essa iniciativa posiciona a DPE-PA como uma entidade líder em inovação e eficiência operacional, pronta para enfrentar os desafios do cenário tecnológico dinâmico e garantir a prestação de serviços jurídicos de alta qualidade.

Portanto, em face das razões acima expostas, elaboramos o presente Termo de Referência, com o fim de instruir procedimento administrativo licitatório objetivando contratação de empresa para o fornecimento de solução de cibersegurança e gestão de rede para todas as unidades da Defensoria Pública do Estado do Pará.

DO MODELO DE CONTRATAÇÃO

Esse processo de contratação segue o modelo de contratação que contempla a definição dos procedimentos necessários e suficientes ao adequado fornecimento de Soluções de Tecnologia da Informação-TI, por lote único, envolvendo aquisição, instalação e manutenção.

DA JUSTIFICATIVA PARA LOTE ÚNICO

Os itens deste certame foram agrupados devido à sua necessidade de integração e sua interdependência, ou seja, a exigência de compatibilidade entre as partes e gestão integrada das entregas para garantir o seu funcionamento, dado que a sua implementação é bastante complexa.

Em contraponto, o parcelamento traz mais complexidade gerencial, e é um dos principais desafios trazidos pela separação das contratações. Quando uma entidade como o DPE-PA opta por dividir contratações em lotes distintos, enfrenta uma crescente complexidade operacional devido à necessidade de gerir múltiplos contratos com diferentes fornecedores. Este cenário demanda um aumento significativo dos recursos administrativos, além de elevar o risco de inconsistências e falhas na integração entre sistemas e soluções fornecidos por empresas distintas. Tais falhas de integração podem criar vulnerabilidades na segurança e gerar ineficiências operacionais, afetando diretamente a produtividade e a continuidade dos negócios.

A estratégia de dividir as contratações pode conduzir a custos ocultos que elevam o custo de propriedade ao longo do tempo. Esses custos adicionais, muitas vezes não antecipados, decorrem de despesas com integração, manutenção e suporte técnico. Esse aumento no do custo de propriedade pode diluir o retorno sobre o investimento, impactando negativamente os orçamentos destinados a outras iniciativas estratégicas da organização.

A segurança cibernética é outra área significativamente impactada pela fragmentação das contratações. A gestão de múltiplos fornecedores torna desafiador manter uma postura de segurança consistente e robusta, aumentando a superfície de ataque da organização e potencializando as vulnerabilidades. Este cenário complica a conformidade com normas e padrões de segurança, expondo a organização a riscos elevados de ataques cibernéticos e violações de dados.

A responsabilização e o suporte técnico também se tornam complexos em um cenário de contratações fragmentadas. A distribuição de responsabilidades entre diferentes fornecedores pode levar a dificuldades na resolução de problemas, uma vez que cada fornecedor pode tentar desviar a culpa para outro, complicando a identificação e correção de falhas. Esse cenário resulta em um tempo de resposta e resolução mais longo, aumentando o tempo de inatividade e prejudicando a experiência dos nossos usuários e serviços prestados.

A fragmentação das contratações pode criar barreiras à inovação e à escalabilidade. A dependência de múltiplos fornecedores pode restringir a capacidade da organização de adotar novas tecnologias e inovações, limitando sua flexibilidade e capacidade de resposta às mudanças do mercado. Essa limitação pode impedir o DPE-PA de explorar oportunidades estratégicas de crescimento e inovação.

Portanto, embora a separação das contratações em lotes distintos possa parecer vantajosa a princípio, as consideráveis desvantagens e riscos associados destacam a importância de optar por uma abordagem mais consolidada. Escolher um fornecedor único capaz de oferecer uma solução integrada é uma estratégia que pode mitigar esses riscos, proporcionando benefícios substanciais em termos de eficiência operacional, segurança e retorno sobre o investimento. Para o DPE-PA, adotar essa abordagem significa não apenas simplificar a gestão de suas contratações, mas também assegurar a resiliência, a segurança e a capacidade de inovação necessárias para atender às suas demandas operacionais e estratégicas.

Incorporando essa consideração adicional, a argumentação sobre a problemática da segmentação das contratações em lotes distintos pela Defensoria Pública do Estado do Pará (DPE-PA) ganha ainda mais peso. A subdivisão das contratações em lotes ou processos distintos não somente acarreta as desvantagens e riscos anteriormente mencionados, mas também introduz a complicação adicional relacionada aos prazos das contratações e à possibilidade de não haver vencedores em determinados lotes ou processo, devido a eventualidades.

A divergência nos tempos de contratação entre os diferentes lotes é um ponto crítico que pode gerar atrasos e descoordenação na implementação das soluções tecnológicas. Cada lote, ao seguir seu próprio cronograma, pode enfrentar tempos de entrega distintos, resultando em uma implantação fragmentada e desalinhada das soluções. Esse descompasso compromete não apenas a eficiência da gestão do projeto como um todo, mas também impacta a operacionalidade da Defensoria, podendo atrasar a disponibilização de serviços críticos para o público.

Além disso, a possibilidade de não se identificar vencedores para determinados lotes, seja por insuficiência de propostas qualificadas, questões jurídicas ou falhas no processo licitatório, introduz um risco significativo de interrupção ou atraso na execução do projeto como um todo, até mesmo a não finalização. Tal cenário pode exigir a realização de novos processos licitatórios, prolongando

ainda mais os prazos de implementação e potencializando os custos associados, sem contar o impacto direto nas operações da Defensoria e na entrega de seus serviços à população.

Para atender às demandas do DPE-PA é crucial compreender as implicações da divisão de contratações em lotes distintos em um edital. Embora esta estratégia possa inicialmente parecer uma forma de otimizar custos e eficiência, ela introduz uma série de desvantagens e riscos que podem comprometer significativamente a operacionalidade, a segurança e a capacidade de integração das tecnologias adotadas pela organização.

Nesta esteira, além da interdependência entre os hardwares, software e serviços acessórios devem ser fornecidos por uma única empresa, pois é incoerente no caso desta contratação, que a empresa que forneça a solução e faça sua instalação seja diversa da que prestará o suporte técnico, treinamento e serviços de manutenções evolutivas.

Além disso o agrupamento dos itens em Lote Único é imprescindível, pois em se tratando de gestão contratual torna-se inviável que os serviços acessórios como neste caso sejam fornecidos por diferentes fornecedores, dado que traz maior complexidade, custo de gestão e controle da DEFENSORIA PÚBLICA.

Em se tratando do viés econômico, o parcelamento dos serviços acessórios do objeto pode impactar diretamente os custos da contratação, considerando que a execução desses serviços por uma única empresa se traduz em diluição do custo administrativo, possibilitando menor preço global.

Todas essas razões inviabilizam a deflagração de mais de um procedimento licitatório.

Isso também porque, o objeto possui características de dependências entre os serviços a serem prestados, sendo certo que seu parcelamento aumentaria os riscos de execução insatisfatória do serviço.

DA FUNDAMENTAÇÃO LEGAL

A presente licitação, que trata da aquisição objeto deste Termo de Referência e seus anexos, será realizada conforme regulamentação da Lei nº Lei nº 14.133/2021, na modalidade PREGÃO ELETRÔNICO do tipo SRP – SISTEMA DE REGISTRO DE PREÇOS.

Os serviços que constituem o objeto deste Termo de Referência enquadram- se no conceito de serviço comum, onde os requisitos técnicos são suficientes para determinar o conjunto da solução escolhida, constatando-se, ainda, que a solução é fornecida por mais de uma empresa no mercado.

DA PARTICIPAÇÃO DE EMPRESAS EM CONSÓRCIO

Vedação à participação de consórcios. Quando o objeto a ser licitado envolve questões de alta complexidade, via de regra, a Administração, com intuito de aumentar o número de participantes, admite a formação de consórcio. No entanto, no contexto em análise, essa hipótese não se aplica, pois, o objeto pretendido, Proteção e Gerenciamento Seguro da rede LAN/WLAN/WAN está consolidado no mercado e no âmbito da Administração Pública, vez que são serviços comuns prestados por diversas empresas atualmente.

Destaca-se que a participação de consórcios em processos licitatórios com esse objeto, além de não garantir o aumento de competitividade, poderá causar prejuízos à Administração Pública na sustentação dos serviços em casos de dificuldades operacionais de um dos consorciados, sobrecarregando os demais participantes.

A DEFENSORIA PÚBLICA espera como resultado deste processo, contar com fornecedor único para o processo de atendimento às demandas, com ampla experiência na execução de atividades operacionais e gerenciais de atendimento, suportadas por ferramentas e processos adequados e

aderentes às necessidades de informações, gestão administrativa, execução interna da licitação e execução de contratos e projetos das diversas áreas gestoras do Órgão, facilitando assim o processo de integração de dados e informações vitais ao desenvolvimento da Administração Pública.

Neste modelo de serviço, o atendimento das demandas deve ser estabelecido de forma estruturada e padronizada, de maneira a evitar os riscos operacionais, motivos pelos quais se optou pela vedação da participação de consórcio.

Outra desvantagem em que o consórcio poderá gerar complicações para a Unidade com relação à gerência e garantia da perfeita execução do contrato e a gestão e fiscalização da execução contratual seriam prejudicadas pela dificuldade em lidar com empresas que possuem processos de trabalhos diferentes e remunerações desiguais por profissionais alocados com atribuições similares.

Em relação ao escopo do objeto, é possível a ampla participação de empresas atuantes no mercado, que de forma isolada, consigam atender às condições e os requisitos de habilitação previstos neste documento.

DOS REQUISITOS TÉCNICOS

O presente TERMO DE REFERÊNCIA visa a aquisição de Solução para proteção e gerenciamento seguro da rede LAN/WLAN/WAN da Defensoria Pública do Estado do Pará – DPE/PA, para garantir a segurança da informação fim a fim e que possibilite a visibilidade e controle de tráfego e aplicações, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede. Os detalhamentos dos demais requisitos técnicos e funcionais mínimos obrigatórios estão a seguir:

ITEM	DESCRIÇÃO DO OBJETO	QTD. ESTIMADA
1	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01	2
2	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02	10
3	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 03	20
4	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 04	30
5	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 05	45
6	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO (PACOTE 10 EQUIPAMENTOS)	10
7	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATÓRIOS (PACOTE 5G/LOG DIA)	5
8	SWITCH CONCENTRADOR (CORE)	4
9	SWITCH DE ACESSO 24 PORTAS POE - TIPO 01	16
10	SWITCH DE ACESSO 24 PORTAS POE - TIPO 02	100
11	SWITCH DE ACESSO 48 PORTAS POE - TIPO 01	16
12	SWITCH DE ACESSO 48 PORTAS POE - TIPO 02	20
13	SWITCH DE ACESSO 8 PORTAS POE	77
14	PONTO DE ACESSO - TIPO 01	155
15	PONTO DE ACESSO - TIPO 02	80
16	TRANSCEIVER SFP+ 10GBASE-T	50
17	TRANSCEIVER SFP+ 10GBASE-SR	50
18	TRANSCEIVER SFP+ 10GBASE-LR	50

19	CONTROLE DE ACESSO A REDE (NAC)	1
20	SERVIÇOS DE TREINAMENTO DAS SOLUÇÕES (POR SOLUÇÃO)	14
21	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (POR SOLUÇÃO)	36
22	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPO 1	02
23	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPOS 2, 3, 4 e 5	105
24	SERVIÇOS DE INSTALAÇÃO DE SWITCHES	229
25	SERVIÇOS DE INSTALAÇÃO DE APs	235
26	SERVIÇO DE INSTALAÇÃO DOS ITENS 6, 7 e 19	16

KIT SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NGFW)
CARACTERÍSTICAS GERAIS PARA FIREWALLS DE PRÓXIMA GERAÇÃO TIPOS 01 A 04

- 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.
- Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 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;
- 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;
- 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;
- O fornecedor deverá comprovar que é representante, revenda autorizada ou distribuidor devidamente registrado no Brasil e autorizado pelo fabricante para ofertar, fornecer e prestar serviços especializados nos produtos.
- Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) meses com as seguintes funcionalidades: Firewall, IPS, Threat Prevention, DNS Security, DLP, análise e prevenção de malware avançado, URL Filtering, AntiMalware, Anti-bot, AntiSpam, detecção e prevenção de intrusos (IPS), VPN IPSec e SSL, Controle de Aplicações, contextos virtuais e SD-WAN como parte integrante dos produtos.
- Os desempenhos solicitados para cada tipo de NGFW deverão ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes como comprovação destes itens de desempenho.
- Todos os equipamentos e licenças fornecidos deverão ser novos, atuais, de primeiro uso e não constar de listas de End of Life (EOL) ou End of Support (EOS) do fabricante.
- Todos os equipamentos deverão ser homologados pela ANATEL.

- **FUNCIONALIDADES DE REDE E FIREWALL**

- O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

- Os dispositivos de proteção de rede devem possuir suporte a Vlans;
- Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;
- Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- 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;
- Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- Deverá suportar sFlow ou Netflow;
- Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
- Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;
- Deve suportar o protocolo padrão da indústria VXLAN;
- Deve implementar o protocolo ECMP;
- Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
- Enviar log para sistemas de monitoração externos;
- Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
- Deve possui mecanismos de proteção anti-spoofing;
- Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);
- Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- Suportar OSPF graceful restart;
- Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- Deve suportar Modo Camada - 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
- Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- 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;
- 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;
- O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;
- A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;
- A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;
- 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;

- Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
- Deverá suportar controle por zonas de segurança;
- Deverá suportar controles de políticas por porta e protocolo;
- Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
- Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
- Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);
- Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
- 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;
- Suporte a objetos e regras IPV6;
- Suporte a objetos e regras multicast;
- Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

- Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
- Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
- 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;
- Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
- 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;
- Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
- 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;
- Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
- 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;
- Identificar o uso de táticas evasivas via comunicações criptografadas;

- Atualizar a base de assinaturas de aplicações automaticamente;
- 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;
- 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;
- Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
- 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;
- O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
- Deve alertar o usuário quando uma aplicação for bloqueada;
- Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
- Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
- 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;
- Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
- 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);
- 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;
- Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;
- Deve permitir forçar o uso de portas específicas para determinadas aplicações;

FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS

- 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;
- Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
- Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
- 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;
- As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

- Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
- Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
- 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;
- Deve permitir o bloqueio de vulnerabilidades;
- Deve permitir o bloqueio de exploits conhecidos;
- Deve incluir proteção contra-ataques de negação de serviços;
- Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
- Detectar e bloquear a origem de portscans;
- Bloquear ataques efetuados por worms conhecidos;
- Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
- Possuir assinaturas para bloqueio de ataques de buffer overflow;
- Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
- 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;
- Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- Identificar e bloquear comunicação com botnets;
- 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;
- Os eventos devem identificar o país de onde partiu a ameaça;
- Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- 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.
- A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante;
- As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante e caso o licenciamento/funcionalidade não seja permanente, o fornecedor deverá prover as funcionalidades por mais 12 (doze) meses;
- Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
- 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;

FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS

- 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);
- Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
- 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;
- 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;
- Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
- Possuir pelo menos 70 (setenta) categorias de URLs;
- Deve possuir a função de exclusão de URLs do bloqueio;
- Permitir a customização de página de bloqueio;
- Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;
- 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;
- 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;
- Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS

- 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;
- 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;
- Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;
- 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;
- Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

- Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 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);
- 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;
- Deve suportar o envio e recebimento de credenciais via RADIUS;
- Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

FUNCIONALIDADE DE FILTRO DE DADOS

- Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
- Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 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.

FUNCIONALIDADE DE GEOLOCALIZAÇÃO

- Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

FUNCIONALIDADE DE VPN

- Suportar VPN Site-to-Site e Cliente-To-Site;
- Suportar IPSec VPN;
- Suportar SSL VPN;
- A VPN IPSEc deve suportar 3DES;
- A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
- A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- A VPN IPSEc deve suportar Autenticação via certificado IKE PKI
- Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

- Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 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;
- A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
- 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;
- Atribuição de DNS nos clientes remotos de VPN;
- Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
- Suportar leitura e verificação de CRL (Certificate Revocation List);
- Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
- Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;
- Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;
- Deverá manter uma conexão segura com o portal durante a sessão;
- O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 8.1 (32 e 64 bit), Windows 10 (32 e 64 bit), Windows 11 e Mac OS X (v10.10 ou superior), CentOS (7 ou superior), Redhat (7 ou superior), Fedora (27 ou superior), Ubuntu (16.04 ou superior), e Android e iOS;

FUNCIONALIDADE DE QOS, TRAFFIC SHAPING E PRIORIZAÇÃO DE TRÁFEGO

- 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;
- Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:
- Endereço de origem;
- Endereço de destino;
- Usuário e grupo;
- Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
- Por porta;
- O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
- 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;
- O QoS deve possibilitar a definição de fila de prioridade;
- Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

- Suportar marcação de pacotes Diffserv, inclusive por aplicação;
- Suportar modificação de valores DSCP para o Diffserv;
- Suportar priorização de tráfego usando informação de ToS (Type of Service);
- Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
- Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;
- Deve possibilitar a definição de bandas distintas para download e upload;

FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS

- A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
- A solução deve ser capaz de agregar vários links em uma interface virtual;
- 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);
- 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;
- 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;
- 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);
- 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).
- 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:
- Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.
- 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;
- 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;
- 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;

- A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;
- A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);
- 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);
- Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;
- 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;
- 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;
- 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;
- 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;
- A solução deve suportar nativamente conectores com clouds públicas;
- Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;
- 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);
- Deve implementar balanceamento de link por hash do IP de origem;
- Deve implementar balanceamento de link por hash do IP de origem e destino;
- 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;
- 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;
- 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.

FUNCIONALIDADE DE CONTROLADOR DE REDE SEM FIO

- 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:
- Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;

- Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;
- A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;
- Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;
- 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;
- Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;
- 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;
- 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;
- 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;
- 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;
- 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;
- A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;
- A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;
- 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;
- 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;

- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
- Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
- A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
- 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;
- 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;
- A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

- A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
- A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
- 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;
- 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;
- A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;
- 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;
- A solução deve suportar a configuração do BLE (Blueooth Low Energy) nos pontos de acesso que tenham este recurso;
- 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;
- 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;
- A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;
- A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;
- 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;
- 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;
- 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;
- Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;
- Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;

- A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;
- 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;
- 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;
- 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;
- 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;
- 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;
- A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
- 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;
- A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
- A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
- A solução deve permitir a configuração do captive portal com endereço IPv6;
- 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;
- 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;
- Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
- A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;
- A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;
- A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
- 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;
- A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;
- A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;
- 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;

- A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;
- A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;
- A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;
- A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;
- A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);
- A solução deve permitir a captura de pacotes na rede wireless e exporta-los em arquivos no formato .pcap;
- 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;
- 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;
- A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;
- A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;
- A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;
- 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;
- A solução deve possuir ferramentas de diagnósticos e debug;
- A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;
- A solução deve suportar comunicação com elementos externos através de REST API;
- A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

FUNCIONALIDADE DE CONTROLADOR DE REDE CABEADA

- 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:
- Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;
- Deve possuir interface gráfica para configuração, administração e monitoração dos switches;
- 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;
- Deve montar a topologia da rede de maneira automática;
- Deve ser capaz de configurar os switches da rede;
- Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;

- Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
- Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
- Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
- Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;
- Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
- 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;
- Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
- A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
- Deve ser capaz de configurar parâmetros SNMP dos switches;
- 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;
- A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
- A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;
- A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;
- A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
- Deve prover indicadores de saúde dos elementos críticos do ambiente;
- Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
- Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede.

ITEM 01 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01

- Deve suportar, no mínimo, 12 (doze) Gbps de performance de prevenção de ameaças, com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, firewall e Anti-Malware para tráfego IPv4 e IPv6;
- Deve suportar, no mínimo, 7 (sete) milhões de conexões simultâneas;
- Deve suportar, no mínimo, 370.000 (trezentos e setenta mil) novas conexões por segundo;
- Deve Suportar, no mínimo, 40 (quarenta) Gbps de desempenho VPN IPSec;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 10.000 (dez mil) túneis ou peers do protocolo IKE de VPN IPSEC Site-to-Site simultâneos

- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 12.000 (doze mil) túneis de clientes Global Protect Client VPN simultâneos e caso não estejam inclusas as licenças, devem ser fornecidas licenças para acesso de dispositivos móveis iOS e Android para VPN para a quantidade total do mesmo fabricante;
- Deve suportar, no mínimo, 18 (dezoito) Gbps de throughput de IPS;
- Deve suportar, no mínimo, 6 (seis) Gbps de throughput de Inspeção SSL;
- Deve possuir latência de firewall menor que 5µs baseados na RFC 2544 em pacotes de 64 bytes em formato de protocolo UDP.
- Deve possuir, pelo menos, 8 (oito) interfaces 10 Gigabit Ethernet 10GBase-T com conectores RJ-45;
- Deve possuir, pelo menos, 8 (oito) interfaces com suporte a SFP de 1 Gigabit Ethernet;
- Deve possuir, pelo menos, 8 (oito) interfaces com suporte a SPF+ de 10 Gigabit Ethernet;
- Deve possuir, pelo menos, 8 (oito) interfaces com suporte a conectores SFP28 de 25 Gigabit Ethernet;
- Deve possuir, pelo menos, 2 (duas) interfaces com suporte a conectores QSFP28 de 100 Gigabit Ethernet;
- Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;
- Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para Alta-Disponibilidade;
- Deve estar licenciado para gerenciar até 150 (cem e cinquenta) switches e 500 (quinhentos) pontos de acesso sem fio simultaneamente em um único appliance;
- Deve suportar, no mínimo, de 4094 (quatro mil e noventa e quatro) VLANs;
- Deve possuir, pelo menos, 01 (uma) interface dedicada para gerenciamento segregada das interfaces de tráfego de dados da rede corporativa;
- Deve possuir fonte de alimentação AC redundante e HotSwap;
- Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliances em cluster ativo-passivo;

ITEM 02 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02

- Deve suportar, no mínimo, 3 (três) Gbps de performance de prevenção de ameaças, com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, firewall e Anti-Malware para tráfego IPv4 e IPv6.
- Deve suportar, no mínimo, 3 (três) milhões de conexões simultâneas;
- Deve suportar, no mínimo, 250.000 (duzentas e cinquenta mil) novas conexões por segundo;
- Deve Suportar, no mínimo, 15 (quinze) Gbps de throughput VPN IPSec;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentas) túneis ou peers do protocolo IKE de VPN IPSEC Site-to-Site simultâneos;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 1.500 (mil e quinhentos) túneis de clientes Global Protect Client VPN simultâneos, caso não estejam inclusas as licenças, devem ser fornecidas licenças para acesso de dispositivos móveis iOS e Android para VPN para a quantidade total;
- Deve suportar, no mínimo, 05 (cinco) Gbps de throughput de IPS;

- Deve suportar, no mínimo, 02 (dois) Gbps de throughput de Inspeção SSL;
- Deve possuir latência de firewall menores que 5µs baseados na RFC 2544 em pacotes de 64 bytes em formato de protocolo UDP.
- Deve possuir, pelo menos, 12 (doze) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
- Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet com conectores SFP;
- Deve possuir, pelo menos, 4 (quatro) interfaces 10 Gigabit Ethernet com conectores SFP+;
- Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;
- Deve suportar, no mínimo, de 256 (duzentos e cinquenta e seis) VLANs;
- Deve estar licenciado para gerenciar até 60 (sessenta) switches e 120 (cento e vinte) pontos de acesso sem fio simultaneamente em um único appliance;
- Deve possuir fonte de alimentação AC redundante;
- Deve estar licenciado, sem custo adicional, no mínimo, para 5 (cinco) sistemas virtuais lógicos (Contextos) por appliances em cluster ativo-passivo;

ITEM 03 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL PRÓXIMA GERAÇÃO (NGFW) - TIPO 03

- Deve suportar, no mínimo, 1 (um) Gbps de performance de prevenção de ameaças, com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, firewall e Anti-Malware para tráfego IPv4 e IPv6;
- Deve suportar, no mínimo, 1.5 Milhão (um milhão e quinhentas mil) conexões simultâneas;
- Deve suportar, no mínimo, 50.000 (cinquenta mil) novas conexões por segundo;
- Deve Suportar, no mínimo, 08 (oito) Gbps de throughput VPN IPSec;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 150 (cento e cinquenta) túneis ou peers do protocolo IKE de VPN IPSEC Site-to-Site simultâneos;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de clientes Global Protect Client VPN simultâneos, caso não estejam incluídas as licenças, devem ser fornecidas licenças para acesso de dispositivos móveis iOS e Android para VPN para a quantidade total;
- Deve suportar, no mínimo, 02 (dois) Gbps de throughput de IPS;
- Deve suportar, no mínimo, 01 (um) Gbps de throughput de Inspeção SSL;
- Deve possuir latência de firewall menores que 5µs baseados na RFC 2544 em pacotes de 64 bytes em formato de protocolo UDP.
- Deve possuir, pelo menos, 10 (dez) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
- Deve possuir, pelo menos, 08 (oito) interfaces Gigabit Ethernet com conectores SFP;
- Deve possuir, pelo menos, 02 (duas) interfaces 10 Gigabit Ethernet com conectores SFP+;
- Deve suportar, no mínimo, de 256 (duzentos e cinquenta e seis) VLANs;
- Deve estar licenciado para gerenciar até 30 (trinta) switches e 60 (sessenta) pontos de acesso sem fio simultaneamente em um único appliance;
- Deve possuir fonte de alimentação AC redundante;

- Deve estar licenciado, sem custo adicional, no mínimo, para 5 (cinco) sistemas virtuais lógicos (Contextos) por appliances em cluster ativo-passivo;

ITEM 04 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) – TIPO 04

- Deve suportar, no mínimo, 700 (setecentos) Mbps de performance de prevenção de ameaças, com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, firewall e Anti-Malware para tráfego IPv4 e IPv6;
- Deve suportar, no mínimo, 500.000 (quinhentos mil) conexões simultâneas;
- Deve suportar, no mínimo, 35.000 (trinta e cinco mil) novas conexões por segundo;
- Deve Suportar, no mínimo, 5 (cinco) Gbps de throughput VPN IPSec;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 100 (cem) túneis ou peers do protocolo IKE de VPN IPSEC Site-to-Site simultâneos;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de clientes Global Protect Client VPN simultâneos, caso não estejam inclusas as licenças, devem ser fornecidas licenças para acesso de dispositivos móveis iOS e Android para VPN para a quantidade total;
- Deve suportar, no mínimo, 01 (um) Gbps de throughput de IPS;
- Deve suportar, no mínimo, 500 (quinhentos) Mbps de throughput de Inspeção SSL;
- Deve possuir latência de firewall menores que 5µs baseados na RFC 2544 em pacotes de 64 bytes em formato de protocolo UDP.
- Deve possuir, pelo menos, 10 (dez) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
- Deve suportar, no mínimo, de 256 (duzentos e cinquenta e seis) VLANs;
- Deve estar licenciado para gerenciar até 20 (vinte) switches e 30 (trinta) pontos de acesso sem fio simultaneamente em um único appliance;
- Deve estar licenciado, sem custo adicional, no mínimo, para 5 (cinco) sistemas virtuais lógicos (Contextos) por appliances em cluster ativo-passivo;

ITEM 05 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 05

- Deve suportar, no mínimo, 500 (quinhentos) Mbps de performance de prevenção de ameaças, com as seguintes funcionalidades habilitadas simultaneamente, para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS, firewall e Anti-Malware para tráfego IPv4 e IPv6;
- Deve suportar, no mínimo, 500.000 (quinhentos mil) conexões simultâneas;
- Deve suportar, no mínimo, 30.000 (trinta mil) novas conexões por segundo;
- Deve Suportar, no mínimo, 04 (quatro) Gbps de throughput VPN IPSec;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 100 (cem) túneis ou peers do protocolo IKE de VPN IPSEC Site-to-Site simultâneos;
- Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 100 (cem) túneis de clientes Global Protect Client VPN simultâneos, caso não estejam inclusas as licenças, devem ser

fornecidas licenças para acesso de dispositivos móveis iOS e Android para VPN para a quantidade total;

- Deve suportar, no mínimo, 01 (um) Gbps de throughput de IPS;
- Deve suportar, no mínimo, 300 (trezentos) Mbps de throughput de Inspeção SSL;
- Deve possuir latência de firewall menores que 5µs baseados na RFC 2544 em pacotes de 64 bytes em formato de protocolo UDP.
- Deve possuir, pelo menos, 05 (cinco) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
- Deve suportar, no mínimo, de 256 (duzentos e cinquenta e seis) VLANs;
- Deve estar licenciado para gerenciar até 04 (quatro) switches e 08 (oito) pontos de acesso sem fio simultaneamente em um único appliance;
- Deve estar licenciado, sem custo adicional, no mínimo, para 5 (cinco) sistemas virtuais lógicos (Contextos) por appliance.

ITEM 06 - GERENCIAMENTO DE CONFIGURAÇÃO CENTRALIZADO

- Deve estar dimensionado e licenciado para gerenciar até 10 (dez) Firewalls de Próxima Geração (NGFW) considerando os modelos ofertados neste processo atendendo aos requisitos deste Item;
- 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;
- 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;
- Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;
- Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;
- Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;
- A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;
- 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);
- 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;
- 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;
- Permitir criar templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

- Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.
- A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;
- 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;
- Permitir acesso concorrente de administradores e que seja definida uma cadeia de aprovação das alterações realizadas;
- Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
- Permitir usar palavras chaves ou cores para facilitar identificação de regras;
- Permitir localizar em quais regras um objeto (ex. computador, serviço, etc.) está sendo utilizado;
- Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;
- Permitir criação de regras que fiquem ativas em horário definido;
- Permitir criação de regras com data de expiração;
- Realizar o backup das configurações para permitir o retorno de uma configuração salva;
- 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.
- Gerar alertas automáticos via Email, SNMP e Syslog;
- Deve ser permitido ao administrador transferir os backups para um servidor FTP, SCP ou SFTP.
- Permitir backup das configurações e rollback de configuração para a última configuração salva;
- Deve possibilitar a visualização e comparação de configurações atuais e configurações anteriores;
- 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;
- Deve suportar a distribuição e instalação remota de novas versões de software dos equipamentos, de forma remota e centralizada;
- Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;
- Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, TACACS+ e PKI.
- 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.
- A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances.
- Deve suportar o gerenciamento de pontos de acesso de forma centralizada.
- Deve suportar o gerenciamento centralizado de switches.
- A solução deve possuir garantia, suporte e atualizações ao software durante a vigência do contrato.

ITEM 07 - GERENCIAMENTO DE LOGS E RELATÓRIOS CENTRALIZADO

- Deve suportar o acesso via SSH, WEB (HTTPS) para gerenciamento da solução;
- A solução deve suportar receber, no mínimo, 5 (cinco) GB de logs diários;
- 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;
- 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;
- Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;
- Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;
- Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;
- A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;
- A solução deverá ser capaz de armazenar logs por no mínimo 12 (doze) meses;
- Permitir acesso simultâneo à administração, bem como criar pelo menos 2 (dois) perfis para administração e monitoramento;
- Possuir suporte para SNMP versão 2 e 3;
- Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;
- Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;
- 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;
- Suporte a autenticação de usuários de acesso à plataforma via LDAP, Radius ou TACACS+;
- Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;
- Deve permitir gerar alertas de eventos a partir de logs recebidos;
- A solução deve ter relatórios predefinidos;
- Permitir importação e exportação de relatórios
- Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
- Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
- Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;
- Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
- Deve ter a capacidade de personalizar a capa dos relatórios obtidos;
- Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
- Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;
- Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;
- Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;
- Deve possuir mecanismos de remoção automática para logs antigos;

- Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;
- Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
- Permitir o envio por e-mail relatórios automaticamente;
- Deve permitir que o relatório seja enviado por Email para o destinatário específico;
- Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
- Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;
- Deve permitir o uso de filtros nos relatórios;
- Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
- Permitir especificar o idioma dos relatórios criados;
- Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
- Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
- Deve permitir o envio automático dos logs para um servidor FTP externo a solução;
- Deve permitir exportar os logs no formato CSV;
- Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;
- Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;
- 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;
- Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;
- 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;
- Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;
- Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;
- Deve permitir visualizar em tempo real os logs recebidos;
- Deve permitir o encaminhamento de log no formato syslog e CEF (Common Event Format);
- 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;
- 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;
- Deve possuir um painel de operações que monitore as principais ameaças à segurança da sua rede;
- Deve possuir um painel de operações que monitora o envolvimento do usuário e o uso suspeito da web em sua rede;

- Deve possuir um painel de operações que monitora o tráfego da rede, aplicativos e sites web;
- Deve possuir um painel de operações que monitoram a atividade da VPN em sua rede;
- Deve possuir um painel de operações que monitoram o desempenho dos recursos locais da solução (CPU, Memória)
- Deve permitir a criação de painéis personalizados para monitorar operações de segurança e rede;
- Deve possuir relatório de uso de aplicações e mídias sociais;
- Deve possuir relatório de prevenção de perda de dados (DLP);
- Deve possuir relatório de VPN, Prevenção de Intrusão (IPS), análise de ameaças cibernéticas;
- Deve possuir relatório diário resumido de eventos e incidentes de segurança;
- Deve possuir um relatório de tráfego DNS e e-mail;
- Deve possuir relatório das 10 principais aplicações utilizadas na rede;
- Deve possuir relatório dos 10 principais sites web utilizados na rede;
- 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);
- 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;
- 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;
- Deve suportar a análise detalhada dos computadores comprometidos e exibir os detalhes das ameaças detectadas;
- 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;
- 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;

ITEM 08 – SWITCH CONCENTRADOR (CORE)

- Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
- Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;
- Deve possuir 48 (quarenta e oito) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE;
- Adicionalmente, deve possuir 4 (quatro) slots QSFP28 para conexão de fibras ópticas operando com velocidades de 40 e 100 Gigabit Ethernet;
- Deve permitir a configuração das interfaces QSFP28 para que operem com conexões do tipo "breakout" ou "split", modo em que uma determinada porta 40GbE pode operar com 4 conexões em 10GbE. Deve permitir ainda que as portas 100GbE sejam divididas em 4 conexões de 25GbE;

- 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 interface dedicada para gerenciamento local do tipo "out-of-band". Esta interface de gerenciamento deverá possuir porta 1000Base-T com conector RJ-45;
- Deve possuir 1 (uma) interface USB;
- Deve possuir capacidade de comutação de pelo menos 1.76 Tbps (terabits por segundo) e ser capaz de encaminhar até 1.5 Bpps (bilhões de pacotes por segundo);
- Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
- 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;
- Deve possuir tabela MAC com suporte a 144.000 endereços;
- Deve operar com latência igual ou inferior à 1us (microsegundo);
- Deve implementar Flow Control baseado no padrão IEEE 802.3X;
- 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;
- Deve suportar o padrão IEEE 802.1Qbb (Priority-based Flow Control);
- Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol - LACP);
- 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;
- Deve suportar a comutação de Jumbo Frames;
- Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
- Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
- 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 exija licenciamento adicional para ativação dos protocolos;
- 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 exija licenciamento adicional para ativação dos protocolos;
- 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 exija licenciamento adicional para ativação do protocolo;
- Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;
- 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 exija licenciamento adicional para ativação deste recurso;
- Deve implementar serviço de DHCP Server e DHCP Relay;
- Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) grupos;

- Deve suportar MLD (Multicast Listener Discovery) Snooping para otimizar a transmissão de tráfego multicast em IPv6;
- Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN);
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
- Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
- 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;
- 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);
- Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
- 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;
- Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement;
- Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
- Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

- 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;
- 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;
- Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
- Deve suportar MAC Authentication Bypass (MAB);
- Deve implementar RADIUS CoA (Change of Authorization);
- Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
- 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;
- Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
- 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;
- Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
- Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
- Deve suportar o protocolo PTP (Precision Time Protocol);
- Deve implementar Netflow, sFlow ou similar;
- Deve suportar o envio de mensagens de log para servidores externos através de syslog;
- Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
- Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
- Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
- Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
- Deve permitir ser gerenciado através de IPv6;
- Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 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;
- Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
- Deverá suportar ser configurado e monitorado através de REST API;

- 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;
- Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash;
- Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
- Deve suportar temperatura de operação de até 40º Celsius;
- Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
- Deve ser fornecido com fontes de alimentação redundantes do tipo hot-swap, com capacidade para operar em tensões de 110V e 220V;
- 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;
- Deve ser fornecido com cabo DAC (Direct Attach Cable) 40GbE QSFP+ de 3 metros;

ITEM 09 - SWITCH DE ACESSO 24 PORTAS POE - TIPO 01

- Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
- Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;
- 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);
- 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 180W;
- 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;
- Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo);
- Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
- Deve possuir tabela MAC com suporte a 32.000 endereços;
- Deve operar com latência igual ou inferior à 1us (microsegundo);
- Deve implementar Flow Control baseado no padrão IEEE 802.3X;
- Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);
- Deve suportar a comutação de Jumbo Frames;
- Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

- Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
- Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
- Deve implementar serviço de DHCP Relay;
- Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;
- Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
- Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
- Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;
- Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
- Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
- Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
- 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;
- 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;

- Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
- Deve suportar MAC Authentication Bypass (MAB);
- Deve implementar RADIUS CoA (Change of Authorization);
- Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
- 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;
- Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
- 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;
- Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
- Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
- 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;
- 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);
- 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;
- Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
- Deve suportar o envio de mensagens de log para servidores externos através de syslog;
- Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
- Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
- Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
- Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
- Deve permitir ser gerenciado através de IPv6;
- Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 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;
- Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

- 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;
- Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
- Deverá suportar ser configurado e monitorado através de REST API;
- Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
- Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
- Deve suportar temperatura de operação de até 45º Celsius;
- Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
- Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
- 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 10 - SWITCH DE ACESSO 24 PORTAS POE - TIPO 02

- Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
- Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;
- 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);
- 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 a serem alocados em qualquer uma das portas 1000Base-T;
- 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;
- Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo);
- Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
- Deve possuir tabela MAC com suporte a 32.000 endereços;
- Deve operar com latência igual ou inferior à 1us (microsegundo);
- Deve implementar Flow Control baseado no padrão IEEE 802.3X;
- Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);
- Deve suportar a comutação de Jumbo Frames;

- Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;
- Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
- Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
- Deve implementar serviço de DHCP Relay;
- Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;
- Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
- Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
- Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;
- Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
- Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
- Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
- 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;

- 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;
- Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
- Deve suportar MAC Authentication Bypass (MAB);
- Deve implementar RADIUS CoA (Change of Authorization);
- Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
- 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;
- Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
- 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;
- Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
- Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
- 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;
- 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);
- 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;
- Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
- Deve suportar o envio de mensagens de log para servidores externos através de syslog;
- Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
- Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
- Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
- Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
- Deve permitir ser gerenciado através de IPv6;
- Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 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;

- Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 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;
- Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
- Deverá suportar ser configurado e monitorado através de REST API;
- Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
- Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
- Deve suportar temperatura de operação de até 45º Celsius;
- Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
- Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
- 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 11 - SWITCH DE ACESSO 48 PORTAS POE - TIPO 01

- Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
- Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;
- 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;
- 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;
- Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo);
- Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
- Deve possuir tabela MAC com suporte a 32.000 endereços;
- Deve operar com latência igual ou inferior à 1us (microsegundo);
- Deve implementar Flow Control baseado no padrão IEEE 802.3X;
- Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);
- Deve suportar a comutação de Jumbo Frames;

- Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;
- Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
- Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
- Deve implementar serviço de DHCP Relay;
- Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;
- Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
- Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
- Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;
- Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
- Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
- Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
- 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;

- 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;
- Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
- Deve suportar MAC Authentication Bypass (MAB);
- Deve implementar RADIUS CoA (Change of Authorization);
- Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
- 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;
- Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
- 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;
- Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
- Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
- 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;
- 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);
- 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;
- Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
- Deve suportar o envio de mensagens de log para servidores externos através de syslog;
- Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
- Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
- Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
- Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
- Deve permitir ser gerenciado através de IPv6;
- Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 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;

- Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 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;
- Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
- Deverá suportar ser configurado e monitorado através de REST API;
- Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
- Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
- Deve suportar temperatura de operação de até 45º Celsius;
- Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
- Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
- 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 12 - SWITCH DE ACESSO 48 PORTAS POE - TIPO 02

- Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
- Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;
- 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 740W a serem alocados em qualquer uma das portas 1000Base-T;
- 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;
- Deve possuir capacidade de comutação de pelo menos 176 Gbps e ser capaz de encaminhar até 250 Mpps (milhões de pacotes por segundo);
- Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
- Deve possuir tabela MAC com suporte a 32.000 endereços;
- Deve operar com latência igual ou inferior à 1us (microsegundo);
- Deve implementar Flow Control baseado no padrão IEEE 802.3X;
- Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

- Deve suportar a comutação de Jumbo Frames;
- Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;
- Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
- Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
- Deve implementar serviço de DHCP Relay;
- Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;
- Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
- Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
- Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;
- Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
- Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
- Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

- 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;
- 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;
- Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
- Deve suportar MAC Authentication Bypass (MAB);
- Deve implementar RADIUS CoA (Change of Authorization);
- Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
- 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;
- Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
- 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;
- Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
- Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
- 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;
- 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);
- 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;
- Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
- Deve suportar o envio de mensagens de log para servidores externos através de syslog;
- Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
- Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
- Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
- Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
- Deve permitir ser gerenciado através de IPv6;
- Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

- Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 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;
- Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 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;
- Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
- Deverá suportar ser configurado e monitorado através de REST API;
- Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
- Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
- Deve suportar temperatura de operação de até 45º Celsius;
- Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
- Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
- 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 13 - SWITCH DE ACESSO 8 PORTAS POE

- Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
- Deve possuir 08 (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 02 (dois) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE. 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 65W;
- 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 capacidade de comutação de pelo menos 20 Gbps e ser capaz de encaminhar até 25 Mpps (milhões de pacotes por segundo);
- Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
- Deve possuir tabela MAC com suporte a 8.000 (oito mil) endereços;
- Deve operar com latência igual ou inferior à 4 µs (microsegundo);
- Deve implementar Flow Control baseado no padrão IEEE 802.3X;
- Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

- Deve suportar a comutação de Jumbo Frames;
- Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;
- Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;
- Deve suportar a criação de rotas estáticas em IPv4 e IPv6;
- Deve implementar serviço de DHCP Relay;
- Deve suportar IGMP snooping para controle de tráfego de multicast;
- Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- 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;
- Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;
- Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);
- Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;
- Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;
- Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;
- Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;
- 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;

- 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;
- Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;
- Deve suportar MAC Authentication Bypass (MAB);
- Deve implementar RADIUS CoA (Change of Authorization);
- Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;
- 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;
- Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
- 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;
- Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
- Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
- 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;
- 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);
- 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;
- Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
- Deve suportar o envio de mensagens de log para servidores externos através de syslog;
- Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
- Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
- Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
- Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
- Deve permitir ser gerenciado através de IPv6;
- Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 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;

- Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 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;
- Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
- Deverá suportar ser configurado e monitorado através de REST API;
- Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
- Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
- Deve suportar temperatura de operação de até 45º Celsius;
- Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
- Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

ITEM 14 - PONTO DE ACESSO SEM FIO - TIPO 01

- Ponto de acesso (AP) que permita acesso dos dispositivos à rede wireless e que possua todas as suas configurações centralizadas em controlador wireless;
- 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;
- Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;
- Deve identificar automaticamente o controlador wireless ao qual se conectará;
- Deve permitir ser gerenciado remotamente através de links WAN;
- Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;
- Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;
- O ponto de acesso deve possuir rádio Wi-Fi adicional àqueles 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;
- Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;
- Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;
- Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;
- Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;
- Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;
- 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;

- 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;
- 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;
- 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 listas 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;
- 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;
- Deve permitir operação em modo Mesh;
- Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;
- Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;
- Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);
- Deve suportar OFDMA;
- Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;
- Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;
- Deve suportar BSS Coloring;
- Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;
- Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20);
- Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz;
- 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;
- 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;
- 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;
- Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;
- Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);

- 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;
- Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;
- 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;
- Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
- Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
- 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;
- 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;
- Deve implementar o padrão IEEE 802.11e;
- Deve implementar o padrão IEEE 802.11h;
- Deve implementar o padrão IEEE 802.3az;
- Deve suportar ser gerenciado via SNMP;
- Deve suportar consultas via REST API;
- Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;
- Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;
- Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;
- Deve possuir indicadores luminosos (LED) para indicação de status;
- O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;
- Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
- Deve possuir certificado emitido pela Wi-Fi Alliance;
- Deve estar homologado pela ANATEL na data de execução do pregão;

ITEM 15 - PONTO DE ACESSO SEM FIO - TIPO 02

- Ponto de acesso (AP) apropriado para uso externo, que permita acesso dos dispositivos à rede wireless e que possua todas as suas configurações centralizadas em controlador wireless;
- 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;

- Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;
- Deve identificar automaticamente o controlador wireless ao qual se conectará;
- Deve permitir ser gerenciado remotamente através de links WAN;
- Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;
- Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;
- O ponto de acesso deve possuir rádio Wi-Fi adicional àqueles 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;
- Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;
- Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;
- Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T, ou superior, com conector RJ-45 para permitir a conexão com a rede LAN;
- Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;
- Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;
- Deve permitir sua alimentação através de Power Over Ethernet (PoE). Deve acompanhar injetor PoE para alimentação do equipamento;
- 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;
- 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;
- 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 listas 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;
- 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;
- Deve permitir operação em modo Mesh;
- Deve possuir potência de irradiação de 25dBm em 2.4GHz e 5GHz;
- Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1.2 Gbps em um único rádio;
- Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);

- Deve suportar OFDMA com operações em Downlink (DL) e Uplink (UL);
- Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;
- Deve implementar recurso de Target Wake Time (TWT) configurado por SSID;
- Deve suportar BSS Coloring;
- Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;
- Deve possuir sensibilidade mínima de -91dBm quando operando em 5GHz com MCS0 (HT20);
- Deve possuir antenas internas ao equipamento com ganho mínimo de 6dBi em 2.4GHz e 6dBi em 5GHz;
- 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;
- 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;
- Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;
- Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);
- 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 8 (oito) SSIDs com operação simultânea;
- Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3 com 802.1X;
- 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;
- Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;
- Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
- 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;
- 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;
- Deve implementar o padrão IEEE 802.11e;
- Deve implementar o padrão IEEE 802.11h;
- Deve implementar o padrão IEEE 802.3az;
- Deve suportar consultas SNMP diretamente no ponto de acesso;
- Deve suportar consultas REST API diretamente no ponto de acesso;

- Deve possuir estrutura robusta para operação em ambientes externos e permitir ser instalado em paredes e postes. Deve acompanhar os acessórios para fixação em paredes e postes;
- Deve ser capaz de operar em ambientes com temperaturas entre -10 e 60º C;
- O equipamento deve possuir grau de proteção IP67. Não serão aceitos equipamentos instalados em acessórios, por exemplo caixas herméticas, para que alcancem este grau de proteção;
- Deve possuir indicadores luminosos (LED) para indicação de status das interfaces físicas e dos rádios Wi-Fi;
- O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;
- Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
- Deve possuir certificado emitido pela Wi-Fi Alliance;
- Deve estar homologado pela ANATEL na data de execução do pregão;

ITEM 16 - TRANSCEIVER SFP+ 10GBase-T

- Transceiver SFP+ compatível com o padrão 10GBase-T para cabos de par trançado (cobre) de até 30 metros;
- Deve possuir conector RJ-45;
- Deve ter velocidade de 10GbE;
- Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

ITEM 17 - 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 (fibra OM3) e fibras ópticas de até 400m (fibra OM4);
- Deve ter velocidade de 10GbE;
- Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

ITEM 18 - TRANSCEIVER SFP+ 10GBase-LR

- Transceiver SFP+ para conexão de fibras ópticas monomodo;
- Deve ser compatível com o padrão 10GBase-LR para fibras ópticas de até 10km;
- Deve possuir conector LC;
- Deve ter velocidade de 10GbE;
- Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

ITEM 19 - SOLUÇÃO DE CONTROLE DE ACESSO À REDE
CARACTERÍSTICAS GERAIS

- 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;
- Deve ser uma solução multi-vendor capaz de suportar os switches e concentrador VPN do orgão;

- Deve suportar variadas soluções de Wi-Fi do mercado, tais como: Aruba, Ruckus, Cisco, Fortinet, Aerohive e Enterasys, pelo menos;
- A solução deve suportar capacidade de expansão para até 2.000 (dois mil) endpoints simultâneos, sem demandar do cliente a troca do hardware/VM;
- A solução deve estar licenciada para operação com, pelo menos, 400 (quatrocentos) endpoints conectados simultaneamente;
- A solução deve ser entregue em alta disponibilidade;
- A solução deve ser capaz de inspecionar tanto IoT quanto estações/notebooks, sem depender de recursos como 802.1X e Mac-address bypass (MAB);
- Para estações de trabalho, deve suportar verificação de compliance em VPN IPsec e SSL;
- A licença contemplada deverá suportar todas as características exigidas neste termo de referência;
- 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;
- Deve detectar e classificar automaticamente o tipo dos dispositivos conectados na rede sem a necessidade de softwares instalados nos dispositivos;
- Deve permitir determinar o perfil dos dispositivos descobertos por meio de métodos que não exigem a instalação de agentes, incluindo pelo menos os seguintes:
- Consultas em DHCP Fingerprint;
- Consultas via protocolos HTTP/HTTPS;
- Consultas via protocolo SNMP;
- Consultas via protocolo SSH;
- Consultas via protocolo Telnet;
- Consultas de portas TCP;
- Consultas de portas UDP;
- MAC OUI;
- Consultas via protocolo WMI;
- Protocolo ONVIF;
- Protocolo NetFlow;
- Base assinaturas pré-definidas;
- A solução deve ser capaz de reconhecer as seguintes informações sobre os dispositivos conectados à rede:
- Endereço MAC;
- Endereço IP;
- Sistema operacional;
- Nome do host;
- Horário de conexão;
- Usuário conectado;
- Localização.
- A solução deve ser capaz de reconhecer os seguintes sistemas operacionais em execução nos dispositivos conectados à rede:
- Android;
- Apple iOS para iPhone, iPod e iPad;

- Chrome OS;
- Linux;
- MacOS X;
- Windows 7, 8 e 10;
- Deve lembrar o perfil atribuído a cada dispositivo e verificar sua validade a cada conexão;
- Deve permitir a designação de um sponsor para autorizar a categorização dos dispositivos;
- Deve permitir a recategorização periódica de dispositivos;
- Deve permitir a importação de um arquivo CSV contendo informações sobre os dispositivos a serem registrados;
- A solução deve incluir a detecção de dispositivos desconhecidos conectados à rede e adotar medidas de controle para limitar o acesso;
- A solução deve suportar autenticação através de EAP-PEAP e EAP-TLS;
- A solução deve suportar RADIUS Change of Authorization;
- A solução deve suportar MAC Address Bypass;
- A solução deve consultar bases LDAP e Active Directory para a identificação de usuários e grupos de usuários;
- 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 dinamicamente o acesso à rede;
- Deve permitir a definição dos horários em que os dispositivos serão autorizados a conectar na rede;
- 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;
- 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;
- A solução deve permitir o cadastro dos usuários visitantes na base interna da ferramenta para que não seja necessário realizar consultas em bases externas;
- A solução deve possuir ferramenta que permita a geração automática de credenciais para usuários visitantes com login e respectivas senhas;
- A solução deve possuir ferramenta que permita a criação de credenciais para eventos;
- Deve permitir a definição de complexidade da senha dos usuários visitantes;
- Deve ser possível definir um período de validade para as contas de usuários visitantes;
- Deve ser possível definir data e horário para início e encerramento das contas de usuários visitantes;
- A autenticação e autorização dos usuários visitantes deve ocorrer através de portal captivo acessível via browser web;
- Os visitantes em hipótese alguma deverão ter acesso à Internet e rede interna antes que a autenticação seja concluída e o usuário seja autorizado;
- A solução deve vincular o login do visitante à máquina utilizada no acesso;
- Deve suportar a validação de credenciais:
- Em base local interna à ferramenta;
- Em servidores RADIUS;
- Em servidores LDAP.

- A solução deve autenticar usuários visitantes através das seguintes redes sociais: Facebook, LinkedIn e Twitter;
- A ferramenta deve permitir que os usuários visitantes possam realizar auto-registro através do preenchimento de cadastro disponível em portal web;
- Deve permitir a customização dos campos obrigatórios e opcionais para o cadastro de auto-registro;
- A solução deve suportar o envio da senha de acesso aos visitantes através de SMS e e-mail;
- Deve ser possível definir um período para que os usuários visitantes sejam obrigados a se reautenticar;
- 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;
- Os usuários do tipo sponsor poderão cadastrar previamente um usuário visitante. O portal de cadastro e gerenciamento de usuários visitantes não deve permitir gerência administrativa dos demais recursos da solução;
- A solução deve permitir a customização da aparência do captive portal, permitindo editar textos e inserir imagens;
- 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;
- 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;
- Deve permitir o uso de software agente instalado no dispositivo e agentes evanescentes que não precisam ser instalados;
- 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;
- Se um dispositivo não passar os testes de conformidade, deve ser possível:
- Não forçar a remediação;
- Forçar a remediação imediatamente enviando o dispositivo à rede de quarentena;
- 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;
- A solução deve permitir verificações de conformidade em endpoints que façam uso do sistema operacional:
- Windows 7;
- Windows 8;
- Windows 10;
- MacOS;
- Linux.
- 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:
- Presença de software de anti-vírus instalado e em execução;
- Versão do sistema operacional;
- Nome de domínio do Active Directory ao qual a estação Windows pertença;
- Serviços em execução para estações Windows;
- Informações sobre um determinado certificado digital em estações Windows;

- Registros ou chaves de registro para estações Windows;
- Processos em execução para estações Windows, Linux e MacOS;
- Arquivo armazenado em um determinado diretório para estações Windows, Linux e MacOS;
- Pacotes instalados em estações Linux e MacOS.
- 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;
- Deve possuir serviço RADIUS interno, além de permitir o uso de RADIUS externos;
- Deve permitir a distribuição de agentes através de, pelo menos, os seguintes métodos:
- Programas de gerenciamento e distribuição de software;
- GPO do Active Directory;
- Captive Portal;
- Deve permitir a atualização automática ou programada dos agentes instalados nas máquinas;
- O agente instalado nos computadores deve notificar os usuários com mensagens informativas em casos de eventos;
- Quando em quarentena, um portal web deve ser apresentado aos usuários com informações sobre as razões pelas quais estes foram movidos para o isolamento;
- 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;
- 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;
- A solução deve integrar com plataformas de MDM, suportando pelo menos: FortiClient, In Tune, Mobile Iron e Air Watch;
- Deve suportar integração com soluções de patching;
- Deve suportar integração com soluções de análise de vulnerabilidades;
- A solução deve possuir dashboard que apresente informações e estatísticas relevantes de forma resumida;
- A solução deve permitir a customização do dashboard para apresentar as informações que o administrador considera relevante;
- A solução deve permitir a consulta de informações e alteração de parâmetros de configuração via REST API;
- A solução deve armazenar os eventos internamente e permitir que sejam exportados;
- A solução deve permitir a exportação dos eventos através de syslog;
- Deve suportar alta disponibilidade, suportando todos os registros e autenticações caso um nó da solução esteja indisponível;
- 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;
- Deve possuir registro dos eventos ocorridos na solução, bem como auditoria das configurações efetuadas;
- Suportar integração com soluções de segurança de fabricantes como: Fortinet, Palo Alto, FireEye, etc, para correlacionar alertas de segurança e restringir, isolar ou bloquear dispositivos

comprometidos que estejam conectados na rede, reduzindo assim o tempo de contenção de ameaças;

- Suportar método genérico para integração de dispositivos, usando o recebimento, envio, análise e interpretação de mensagens do tipo syslog;
- Deve possibilitar o rastreio de dispositivos, notificando a localização dos mesmos quando se conectarem à rede;
- 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;
- 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 20 – TREINAMENTO DAS SOLUÇÕES
CARACTERÍSTICAS GERAIS DOS TREINAMENTOS

- Treinamento com material oficial das soluções fornecidas.
- Deverá ser abordado conceitos teóricos e atividades práticas de laboratório;
- Todos os treinamentos deverão ser realizados de forma presencial ou híbrida (quando a DPE autorizar);
- O idioma das aulas deverá ser em português;
- Deverá ser entregue material didático composto de apostila em formato digital ou impresso. O material didático poderá ser em português ou inglês.
- Ao final do treinamento deverá ser emitido certificado de conclusão a cada participante, devidamente assinado pela empresa promovente, especificando conteúdo programático completo do curso, corpo docente e carga horária.
- O treinamento pode ser separado conforme o produto a ser instalado no ambiente da Contratante, contendo ao menos os seguintes módulos:
- Descrição e configuração de todas as funcionalidades contratadas da solução;
- Resolução de problemas – troubleshooting;
- Melhores práticas utilizadas no mercado para aproveitamento dos hardwares e softwares e suas funcionalidades.
- O treinamento terá um total de cinco (5) participantes definidos pela Contratante;
- O material didático fornecido deve abordar todos os tópicos do curso;
- A CONTRATADA deverá fornecer apostilas em formato digital que incluam o conteúdo referente ao produto;
- É de responsabilidade da contratante a disponibilização de instalações físicas para a realização do treinamento;
- Após a conclusão, o serviço de treinamento deverá ser formalmente homologado pela Contratante, o qual possuirá o prazo de 5 (quinze) dias consecutivos contados a partir da data de conclusão do treinamento contratado, para emitir o relatório de homologação (aceite).

CARACTERÍSTICAS ESPECÍFICAS DO TREINAMENTO DA SOLUÇÃO DE FIREWALLS DE PRÓXIMA GERAÇÃO

- Carga horária mínima de 36 (trinta e seis) horas;
- Deverá ser abordado, no mínimo, os seguintes tópicos:
- Configurações iniciais e avançadas;
- Configurações de VLANs, LACP, DHCP e tipos de NAT;
- Políticas de segurança;
- Prevenção de ameaças, anti-malware, filtro URL e controle de aplicações;
- Identificação de usuários, qualidade de serviço e regras por aplicação;
- Filtro de dados;
- VPN Site-to-Site e Client-To-Site;
- ZTNA;
- Análise de malwares modernos;
- Alta disponibilidade;
- Gerenciamento centralizado e relatórios;
- Avaliação de boas práticas;
- Otimização de políticas de firewall.

CARACTERÍSTICAS ESPECÍFICAS DO TREINAMENTO DA SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO

- Carga horária mínima de 12 (doze) horas;
- Deverá ser abordado, no mínimo, os seguintes tópicos:
- Configurações iniciais e avançadas;
- Instalação, gerenciamento e administração de dispositivos, políticas e objetos;
- Configuração e administração de instâncias de virtualização;
- Diagnóstico e resolução de problemas.

CARACTERÍSTICAS ESPECÍFICAS DO TREINAMENTO DA SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATÓRIOS

- Carga horária mínima de 12 (doze) horas;
- Deverá ser abordado, no mínimo, os seguintes tópicos:
- Configurações iniciais e avançadas;
- Configuração, visualização e gerenciamento de logs;
- Configuração, visualização e gerenciamento de relatórios;
- Gerenciamento de eventos, incidentes e recursos de automação (playbooks);
- Configuração e administração de instâncias de virtualização.

CARACTERÍSTICAS ESPECÍFICAS DO TREINAMENTO DE ADMINISTRAÇÃO DE SWITCHES E PONTOS DE ACESSO

- Carga horária mínima de 24 (vinte e quatro) horas;
- Deverá ser abordado, no mínimo, os seguintes tópicos:
- Fundamentos básicos de switches e pontos de acesso;

- Configurações iniciais e avançadas de switches e pontos de acesso;
- Gerenciamento de controlador wireless;
- Configuração de autenticação 802.1X, com VLANs dinâmicas;
- Priorização de tráfego;
- Monitoramento, diagnóstico e resolução de problemas.

CARACTERÍSTICAS ESPECÍFICAS DO TREINAMENTO DA SOLUÇÃO DE CONTROLE DE ACESSO A REDE (NAC)

- Carga horária mínima de 16 (dezesseis) horas;
- Deverá ser abordado, no mínimo, os seguintes tópicos:
- Configurações iniciais e visibilidade de rede;
- Identificação e Classificação de Dispositivos Não Autorizados;
- Controle Baseado em Estado;
- Políticas de Segurança;
- Gerenciamento de convidados e de terceiros;
- Integração de dispositivos de segurança e resposta automatizada;
- Alta disponibilidade;
- Monitoramento, diagnóstico e resolução de problemas.

ITEM 21 – SERVIÇO DE SUPORTE PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS, PRÓ-ATIVOS E RESPOSTAS A INCIDENTES:

- A Contratada deverá prover garantia, suporte técnico, e atualização de versões das licenças fornecidas, pelo prazo de trinta meses, contados da data do recebimento definitivo dessas licenças;
- Inclui todas as atualizações de versões, pequenas atualizações de release e reparos de defeitos (bug fixing patches);
- Os serviços de suporte técnico aos produtos deverão incluir, dentre outros:
- Orientações sobre uso, configuração e instalação do software ofertado;
- Questões sobre compatibilidade e interoperabilidade do produto ofertado (hardware e software);
- Interpretação da documentação do software ofertado;
- Orientações para identificar a causa de uma falha de software;
- Orientação para solução de problemas de “performance” e “tuning” das configurações do software ofertado;
- Orientação quanto às melhores práticas para implementação do software adquirido;
- Apoio na recuperação de ambientes em caso de panes ou perda de dados;
- Apoio para execução de procedimentos de atualização para novas versões do software instalado;
- A contratada deverá gerar relatório mensal, analítico e sintético, indicando todos os eventos relevantes ocorridos durante o período de execução do mesmo a ser entregue até o 5 (quinto) dia útil do mês subsequente.
- Durante o período de garantia, suporte técnico e manutenção, a Contratada deverá atender às solicitações da DPE/PA, em qualquer horário, respeitando as condições e níveis de serviços especificados a seguir:

- SEVERIDADE ALTA: Aplicado quando há indisponibilidade do ambiente tecnológico;
- SEVERIDADE MÉDIA: Aplicado quando há falha no uso dos softwares, estando ainda disponíveis, porém apresentando problemas ou instabilidade;
- SEVERIDADE BAIXA: Aplicado para instalação, configuração, manutenção preventivas, aplicações de atualização e esclarecimento técnico relativo ao uso das ferramentas.
- Os prazos estabelecidos nos níveis de serviços serão contados a partir da abertura do chamado, o qual será classificado conforme as severidades especificadas no item anterior.
- Os prazos máximos para o atendimento dos chamados obedecerão ao disposto na tabela a seguir, contados a partir da data e hora de abertura do chamado:

SEVERIDADE	ATENDIMENTO	SOLUÇÃO / PALIATIVO
ALTA	4 (QUATRO) HORAS	12 (DOZE) HORAS
MÉDIA	6 (SEIS) HORAS	24 (VINTE E QUATRO) HORAS
BAIXA	24 (VINTE E QUATRO) HORAS	48 (QUARENTA E OITO) HORAS
LOCAIS REMOTOS	96 (NOVENTA E SEIS) HORAS	120 (CENTO E VINTE) HORAS

- Para os chamados severidade LOCAIS REMOTOS (paralisação TOTAL das funcionalidades elencadas nas especificações técnicas), o início do atendimento deverá ocorrer no máximo em 96 (noventa e seis) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 120 (centro e vinte) horas corridas a contar do início do atendimento.
- Para os chamados de severidade ALTA (paralisação de pelo menos 1 (uma) das funcionalidades elencadas nas especificações técnicas), o início do atendimento deverá ocorrer no máximo em 4 (quatro) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 12 (doze) horas corridas a contar do início do atendimento.
- Para os chamados severidade MÉDIA (degradação na performance, funcionamento ou serviço da solução), o início do atendimento deverá ocorrer no máximo em 6 (seis) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 24 (vinte e quatro) horas corridas a contar do início do atendimento.
- Para os chamados severidade BAIXA (quando há comprometimento do desempenho), o início do atendimento deverá ocorrer no máximo em 24 (vinte e quatro) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 48 (quarenta e oito) horas corridas a contar do início do atendimento.
- Para os chamados de qualquer severidade, a critério da DPE/PA, poderá ser agendado o melhor horário para atendimento.
- O fechamento de qualquer chamado só poderá ocorrer mediante consulta prévia à DPE/PA quanto à efetiva solução do problema.
- Qualquer chamado fechado, sem anuência da DPE/PA ou sem que o problema tenha sido resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas.
- A Contratada manterá cadastro das pessoas indicadas pela DPE/PA que poderão efetuar abertura e autorizar o fechamento de chamados.
- A Contratada deverá fornecer relatório de atendimento técnico, referente a cada chamado, contendo no mínimo as seguintes informações:

- Data e hora da abertura do chamado;
- Data e hora do início do atendimento;
- Responsável pelo atendimento da solicitação;
- Motivo da ocorrência (indicação do defeito);
- Status do chamado (aberto, em tratamento, fechado etc.);
- Data e hora do fechamento do chamado;
- Solução adotada (resolução);
- O atendimento de suporte para a solução deverá ser do tipo 8 x 5 (oito horas por dia, cinco dias por semana), e deverá ser realizado por profissionais especializados.
- Não haverá limite para o número de chamados de suporte técnico.
- Nos casos em que as manutenções necessitarem de paradas do ambiente, a CONTRATANTE deverá ser imediatamente notificada para que se proceda a aprovação da manutenção, ou para que seja agendada nova data, a ser definida pelo CONTRATANTE, para execução das atividades de manutenção;

ITENS 22 A 25 – SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DOS EQUIPAMENTOS

- Caso ocorra alguma divergência entre as especificações técnicas constantes na tabela com aquelas lançadas no sistema eletrônico (Comprasnet), prevalecerá o constante neste instrumento;
- O prazo de vigência da contratação é de 36 (trinta e seis), conforme vier a constar do(s) contrato(s) ou instrumento substituto (se for o caso).
- Caberá à CONTRATADA a implantação da solução sob o acompanhamento da CONTRATANTE;
- No que tange ao processo de implantação da solução, a CONTRATADA deve apresentar um cronograma para a implantação e seguir as atividades tomando como base o seguinte escopo do serviço:
- Planejamento da instalação incluindo identificação de pré-requisitos;
- Instalação e configuração do módulo de gerenciamento central;
- Criar a senha de acesso com privilégio Administrativo para a Contratante.
- Instalação e configuração dos hardwares e softwares;
- Realizar customizações caso sejam solicitadas ou necessárias;
- Realizar testes e apresentar os resultados que comprovem a correta e completa implantação da solução;
- Realizar backup das configurações;
- Documentar todas as configurações realizadas no ambiente.
- Os serviços de instalação serão para os seguintes itens:
- SERVIÇOS DE INSTALAÇÃO FIREWALL TIPO 1
- SERVIÇOS DE INSTALAÇÃO FIREWALL TIPOS 2, 3, 4 e 5
- SERVIÇOS DE INSTALAÇÃO DE SWITCHES
- SERVIÇOS DE INSTALAÇÃO DE APs
- SERVIÇO DE INSTALAÇÃO DOS ITENS 6, 7 e 19
- Após a conclusão da instalação e implantação, a solução deverá ser formalmente homologada pela Contratante, o qual possuirá o prazo de 5 (cinco) dias consecutivos contados a partir da data de conclusão do serviço de instalação e configuração contratado, para emitir o relatório de homologação (aceite). O conteúdo do treinamento deve abordar os assuntos de natureza teórica e

prática, abrangendo todos os módulos envolvidos na solução de segurança em seus aspectos mais relevantes;

- A instalação e configuração, serviços opcionais, deverá ocorrer em até 15 (quinze) dias corridos, contados a partir da data de entrega da ordem de serviço. Para as unidades que optarem pelo saque do referido serviço, esse prazo deverá constar na cláusula da Minuta contratual.
- Para as unidades que contratarem o serviço de "Instalação para Equipamentos na capital e em localidades com distância até 200 km da Capital ou superior a 200 km da Capital" a entrega efetiva está condicionada a conclusão da instalação e configuração dos equipamentos;
- A CONTRATADA deverá cumprir com todas as exigências técnicas e funcionais relacionadas com a solução ofertada, que devem ser implantadas durante o período contratado, sem ônus para a CONTRATANTE;
- O serviço de instalação consiste na acomodação física, incluindo patch cord e configuração lógica dos equipamentos;
- Caberá à CONTRATADA a disponibilização de todos os recursos necessários, como hardware, software e recursos humanos necessários à execução dessa atividade;
- O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção individual, bem como materiais complementares estritamente necessários à instalação ou à assistência técnica é de inteira responsabilidade da CONTRATADA e não deverá gerar ônus à CONTRATANTE;
- No tocante a equipamentos, periféricos, acessórios, técnicos de instalação, técnicos de manutenção, translado, transporte, estada, embalagens, necessários à execução da instalação e assistência técnica deverão ser de responsabilidade da CONTRATADA e não deverão gerar qualquer ônus à CONTRATANTE;
- No processo de instalação o Responsável Técnico da CONTRATADA deverá tomar todas as medidas necessárias visando garantir a perfeita execução do serviço (instalação e configuração).

DA ENTREGA E DO RECEBIMENTO

Quanto à entrega:

O objeto contratual deverá ser entregue em conformidade com as especificações estabelecidas neste instrumento no prazo máximo de 30 (trinta) dias, contado a partir da assinatura do contrato, recebimento da ordem de serviço, ordem de fornecimento ou instrumento hábil.

Os atrasos ocasionados por motivo de força maior ou caso fortuito, desde que justificados até 2 (dois) dias úteis antes do término do prazo de entrega, e aceitos pela contratante, não serão considerados como inadimplemento contratual.

Quanto ao recebimento:

PROVISORIAMENTE, mediante recibo, para efeito de posterior verificação da conformidade do objeto com as especificações, devendo ser feito por pessoa credenciada pela contratante.

DEFINITIVAMENTE, sendo expedido termo de recebimento definitivo, após verificação da qualidade e da quantidade do objeto, certificando-se de que todas as condições estabelecidas foram atendidas e, consequente aceitação das notas fiscais pelo gestor da contratação, devendo haver rejeição no caso de desconformidade.

DO PAGAMENTO

O pagamento será efetuado, em até 30 (trinta) dias, pelo Departamento Financeiro do DPE/PA, devendo a Contratada apresentar a respectiva Nota Fiscal/Fatura, emitidos de acordo com a legislação vigente, a partir da qual se contará o prazo para pagamento.

Os pagamentos serão efetuados através de crédito aberto em conta corrente da Contratada.

O pagamento somente será autorizado depois de efetuado o "atesto" pelo servidor competente na Nota Fiscal apresentada.

No caso de atraso no pagamento por culpa do Contratante, os valores devidos serão acrescidos de encargos financeiros de 1% (hum por cento) ao mês, calculados "pro rata die" até a data do efetivo pagamento.

No preço contratado estão incluídas todas e quaisquer despesas com mão-de-obra, material de consumo, equipamentos, treinamentos, prêmios de seguro, taxas, inclusive de administração, emolumentos e quaisquer despesas operacionais, bem como todos os encargos trabalhistas, previdenciários, fiscais e comerciais, despesas e obrigações financeiras de qualquer natureza e outras despesas diretas e indiretas necessárias à perfeita execução do objeto DO CONTRATO, além de auxílio alimentação ou refeição, vale-transporte e quaisquer outras vantagens pagas aos empregados, enfim, todos os componentes de custo dos serviços, inclusive o lucro.

Quando houver erro, de qualquer natureza na emissão da nota fiscal/fatura, o documento será devolvido, imediatamente, para substituição e/ou emissão de nota de correção, não devendo ser computado nesse intervalo de tempo, para efeito de qualquer reajuste ou atualização do valor contratado;

Nota Fiscal apresentada para pagamento deverá ser emitida com o mesmo número do CNPJ participante da licitação e da Nota de Empenho;

Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

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 do CONTRATANTE.

Não havendo regularização ou sendo a defesa considerada improcedente, o 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.

Persistindo a irregularidade, o CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada o direito ao contraditório e ampla defesa.

DAS SANÇÕES ADMINISTRATIVAS

Comete infração administrativa, nos termos da Lei no 14.133, de 2021, o Contratado que:

- der causa à inexecução parcial do contrato;
- der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- der causa à inexecução total do contrato;
- deixar de entregar a documentação exigida para o certame;
- não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;
- não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
- ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;

- apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou execução do contrato;
- fraudar a contratação ou praticar ato fraudulento na execução do contrato;
- comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- praticar atos ilícitos com vistas a frustrar os objetivos da contratação;

Serão aplicadas ao responsável pelas infrações administrativas acima descritas as seguintes sanções:

- Advertência, quando o Contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;
- Multa:
- moratória de 1 % (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;
- compensatória de 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto ou sobre o valor da parcela inadimplida, no caso de inexecução parcial;

A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Contratante;

Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa;

Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação;

Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pela Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente;

Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (trinta) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei no 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

Na aplicação das sanções serão considerados:

- a natureza e a gravidade da infração cometida;
- as peculiaridades do caso concreto;
- as circunstâncias agravantes ou atenuantes;
- os danos que dela provierem para a Contratante;
- a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

Os atos previstos como infrações administrativas na Lei no 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei no 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159)

A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste

Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia;

A Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal;

As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei no 14.133/21.

DAS OBRIGAÇÕES DA CONTRATADA

- Executar o objeto em conformidade com as condições deste instrumento.
- Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.
- Aceitar, nas mesmas condições contratuais, os percentuais de acréscimos ou supressões limitados ao estabelecido no art. 125, da Lei Federal nº 14.133/21, tomando-se por base o valor contratual.
- Responsabilizar-se pelos danos causados diretamente à contratante ou a terceiros, decorrentes da sua culpa ou dolo, quando da execução do objeto, não podendo ser arguido para efeito de exclusão ou redução de sua responsabilidade o fato de a contratante proceder à fiscalização ou acompanhar a execução contratual.
- Responder por todas as despesas diretas e indiretas que incidam ou venham a incidir sobre a execução contratual, inclusive as obrigações relativas a salários, previdência social, impostos, encargos sociais e outras providências, respondendo obrigatoriamente pelo fiel cumprimento das leis trabalhistas e específicas de acidentes do trabalho e legislação correlata, aplicáveis ao pessoal empregado na execução contratual.
- Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela contratante, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.
- Refazer, substituir ou reparar o objeto contratual que comprovadamente apresente condições de defeito ou em desconformidade com as especificações deste termo, no prazo fixado pelo DPE/PA, contado da sua notificação.
- Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta comercial, observando o prazo mínimo exigido pela Administração.
- Providenciar a substituição de qualquer profissional envolvido na execução do objeto contratual, cuja conduta seja considerada indesejável pela fiscalização da contratante.
- Responsabilizar-se integralmente pela observância do dispositivo no título II, capítulo V, da CLT, e na Portaria n.º 3.460/77, do Ministério do Trabalho, relativos à segurança e higiene do trabalho, bem como a Legislação correlata em vigor a ser exigida.

DAS OBRIGAÇÕES DA CONTRATANTE

- Solicitar a execução do objeto à contratada através da emissão de Ordem de Serviço / Ordem de Fornecimento.
- Proporcionar à contratada todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual, consoante estabelece a Lei Federal no 14.133/21 e suas alterações.
- Fiscalizar a execução do objeto contratual, através de sua unidade competente, podendo, em decorrência, solicitar providências da contratada, que atenderá ou justificará de imediato.
- Notificar a contratada de qualquer irregularidade decorrente da execução do objeto contratual.
- Efetuar os pagamentos devidos à contratada nas condições estabelecidas neste Termo.
- Aplicar as penalidades previstas em lei e neste instrumento.

DA FISCALIZAÇÃO

O CONTRATANTE, por meio do setor competente, exercerá ampla fiscalização sobre a execução do contrato, ficando a CONTRATADA obrigada a facilitar o exercício desse direito.

O servidor do DPE/PA designado para atuar como fiscal do contrato terá, dentre outras, as seguintes atribuições:

O fiscal designado pelo DPE/PA anotará, em registro próprio, todas as ocorrências relacionadas com a execução do contrato, inclusive quanto à observância do prazo de vigência do mesmo e aos pagamentos efetuados pelo DPE/PA, determinando o que for necessário à regularização das faltas ou defeitos existentes e encaminhar cópia à CONTRATADA para a imediata correção das irregularidades apontadas, sem prejuízo das penalidades previstas neste contrato e na lei.

As decisões e providências que ultrapassarem a competência deste fiscal deverão ser encaminhadas, em tempo hábil, ao superior para adoção das medidas necessárias e/ou convenientes.

Conferir se a aquisição está de acordo com as especificações técnicas exigidas.

Rejeitar no todo ou em parte os bens entregues, se considerados em desacordo ou insuficientes, conforme os termos discriminados na proposta da CONTRATADA e no Termo de Referência do Edital.

A fiscalização da contratação pelo CONTRATANTE não exime, nem diminui a completa responsabilidade da CONTRATADA, por qualquer inobservância ou omissão às cláusulas contratuais.

PRAZO DE VIGÊNCIA E DE EXECUÇÃO DO CONTRATO

Os prazos de vigência do contrato será de 36 (trinta e seis) meses a contar da data da sua assinatura.

O contrato poderá ser renovado por até 10 (dez) anos nos contratos administrativos, nos termos do art. 107 da Lei nº 14.133/2021.

DOS CRITÉRIOS DE HABILITAÇÃO

Os requisitos de habilitação serão definidos junto ao edital e nos termos da legislação vigente.

Quanto a habilitação técnica, temos:

Será requerida das empresas licitantes, para fins de habilitação, a comprovação do pleno atendimento a partir de apresentação de comparativo Ponto-a-ponto referente aos itens licitados.

Será requerida das empresas licitantes, para fins de habilitação, a comprovação de aptidão para a prestação dos serviços em características técnicas compatíveis com o objeto desta licitação, mediante a apresentação de:

Atestado(s) de capacidade técnica, emitido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) ter fornecido ou estar fornecendo os quantitativos compatíveis em características e prazos de cada item do objeto da licitação;

Não será definido um quantitativo mínimo aceitável para ampliar a competitividade do certame e consequentemente, obter preços mais vantajosos em meio a possibilidade de participação de um número maior.

Declaração informando se a licitante é a fabricante, revendedora ou distribuidora autorizada do fabricante, ou ainda, revendedora autorizada de distribuidor autorizado pelo fabricante dos produtos. Caso a licitante não possua uma das qualificações exigidas anteriormente, deverá ser apresentada declaração do próprio licitante de que a aquisição dos softwares, objeto desse edital, será realizada através de um canal do fabricante, para softwares especificados pelo fabricante para uso no Brasil.

Tais declarações deverão ser emitidas em papel timbrado, com assinatura, identificação e telefone do emitente.

Admite-se mais de um atestado com vistas a comprovar o atendimento a todos os requisitos de capacidade técnica que asseguram a similaridade do objeto.

A licitante disponibilizará todas as informações necessárias à comprovação da legitimidade do(s) atestado(s).

A comprovação de capacidade deverá ser realizada por meio de atestado ou conjunto de atestados que totalizados atendam aos critérios exigidos.

No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da licitante. Serão consideradas como pertencentes ao mesmo grupo empresarial as empresas controladas ou controladoras da empresa licitante, e ainda as que tenham pelo menos uma pessoa física ou jurídica como sócia em comum.

O CONTRATANTE reserva-se o direito de realizar diligências, a qualquer momento, com o objetivo de verificar se o(s) atestado(s) e demais documentos são adequados e atendem às exigências contidas neste Termo de Referência, podendo exigir apresentação de documentação complementar referente à prestação de serviços relativos aos atestados apresentados.

Caso a licitante não comprove as exigências do Edital por meio das documentações requeridas, será desclassificada.

O pregoeiro examinará a proposta classificada em primeiro lugar quanto à compatibilidade do preço em relação ao estimado para a contratação, de acordo com as exigências do Edital.

DA PROVA DE CONCEITO

A licitante melhor classificada será convocada para realizar a Prova de Conceito – POC, com vistas a demonstrar que a solução ofertada atende os requisitos exigidos.

A POC somente será realizada para a proponente melhor classificada, não sendo requisito prévio de habilitação.

Caso a licitante melhor classificada não esteja ofertando uma solução que atenda os requisitos exigidos, ela será inabilitada, passando a convocar as licitantes na ordem de classificação da fase de lances.

A Prova de Conceito acontecerá em até 03 (três) dias úteis, contados da convocação oficial por parte da Defensoria.

A Prova de Conceito será realizada nas dependências da Defensoria Pública do Estado do Pará - DPE/PA, no horário acordado entre as partes.

Qualquer licitante poderá participar da Prova de Conceito, entretanto, será na condição de ouvinte e não poderá se manifestar durante a realização.

A Prova de Conceito consistirá na comprovação de requisitos técnicos existentes neste Termo de Referência, entretanto, a Defensoria Pública do Estado do Pará - DPE/PA se reserva ao direito de somente divulgar os requisitos que deverão ser comprovados no momento da realização da POC, para evitar que as licitantes preparem a solução somente para passar na Prova de Conceito.

No momento da realização, a equipe de TI irá anotar em registro próprio, todos os requisitos comprováveis e o seu respectivo atendimento, podendo, inclusive, incluir comprovações.

Somente com a apresentação do(s) atestado(s) de capacidade técnica, declaração e a Prova de Conceito, a proposta será tecnicamente aceita.

Belém (PA), 13 de novembro de 2023.

(Assinatura)
Cesar Augusto Cavalcante Valente
Assessor Técnico - Matrícula 5967671
Coordenadoria De Estratégia E Governança de TIC

APÊNDICE 01

ESTUDO TÉCNICO PRELIMINAR

Este Estudo Técnico Preliminar tem como objetivo principal prover embasamento para criar melhores condições de sustentação e funcionamento do ambiente de processamento de dados da DEFENSORIA PÚBLICA DO ESTADO DO PARÁ, notadamente em relação às aplicações que servem de base ao desenvolvimento das atividades finalísticas ou de meio.

Histórico

A Defensoria Pública do Estado do Pará – DPE/PA tem como meta estratégica na Tecnologia da Informação e Comunicação - TIC a disponibilização de ferramentas tecnológicas que garantam o adequado funcionamento do ambiente tecnológico e que colaborem com a melhoria da produtividade dos seus usuários. Portanto, assim como os outros poderes que compõem a estrutura de Estado, a DPE/PA necessita de proteção e segurança sobre o conteúdo armazenado e manipulado internamente nos respectivos ambientes para que sejam mantidas a confidencialidade, a integridade e a disponibilidade das informações existentes.

Tendo em vista a necessidade de ter uma infraestrutura padronizada adequada para a guarda e operação dos equipamentos de Tecnologia da Informação da DPE/PA e, buscando atender o compromisso do Governo do Estado do Pará em garantir eficiência da gestão pública, é essencial a adequação do Data Center atual visando obter um ambiente computacional seguro para a DPE/PA.
Esta é uma ação de essencial importância para o processo de estruturação de TIC no âmbito da Defensoria Pública do Estado do Pará, promovendo o compartilhamento de uma infraestrutura estável, segura, ágil, robusta e moderna.

Esta ação promoverá a eficiência e a consolidação dos investimentos em uma plataforma centralizada, segura, padronizada e com um alto desempenho projetado para o Data Center atual da DPE/PA, a qual necessita de uma reestruturação lógica e elétrica, fundamentada nas normas vigentes:

a) ISO – International Standard Association;
b) TIA 942 – Telecommunications Infrastructure Standard for Data Centers;
c) TIA – Telecommunications Industry Association;
d) CENELEC – Comité Européen de Normalisation Electrotechnique;
e) ABNT – Associação Brasileira de Normas Técnicas;
f) NBR 14565 – Procedimento básico para elaboração de projetos de cabeamento de telecomunicações para rede interna estruturada;
g) ANSI/EIA/TIA 568 – B e suas atualizações “Commercial Building Telecommunications Cabling Standard” - Essa norma regula a padronização do material a ser instalado em um sistema de cabeamento, as práticas de instalação dos produtos e as suas aplicações apropriadas em cada situação. Traz também as definições de cada componente do cabeamento;
h) ANSI/EIA/TIA 569 – B e suas atualizações “Commercial Building Standard for Telecommunications Pathways and Spaces” - Esta padronização visa estabelecer os métodos de projeto e utilização de dutos e espaços dedicados ao uso de sistemas de telecomunicação, durante a construção de um edifício, em suas reformas ou readequações;

i) ANSI/EIA/TIA 606 – A “Administration Standard for the Telecommunications Infraestructure of Commercial Building” - Esta norma tem como objetivo apresentar os conceitos básicos para a administração da infraestrutura de telecomunicações;
j) EIA/TIA TSB – 67 “Transmission Performance Specifications for Field Testing of Unshield Twisted-Pair Cabling Systems” - Boletim técnico adicional da 568-A que estabelece os critérios de certificação e testes do cabeamento;
k) EIA/TIA TSB- 75 “Additional Horizontal Cabling Practices for Open Offices” - Boletim técnico adicional da 568-A que trata das instalações do cabeamento em ambientes que sofrem mudanças constantes de layout.

Essencial para o provimento da Infraestrutura de TIC, a aquisição de solução integrada para gerenciamento do ciclo de vida, proteção, identificação e rastreabilidade dos dados corporativos irá auxiliar na disponibilidade dos serviços e informações críticas fornecidos pela DPE/PA aos públicos interno e externo.

Esta aquisição é fundamental para a melhoria da inteligência organizacional, integração dos dados, continuidade dos serviços, preservação das informações críticas ao negócio, bem como para resguardar o uso de dados e informações pessoais, e garantir a recuperação e acesso a essas informações, conforme exigência prevista na Lei 13.709/18 - Lei Geral de Proteção de Dados.

Percebe-se claramente que além de um ambiente desatualizado (sem suporte) não há ferramental específico destinado à proteção de dados, além dos elementos de interconexão, são usadas medidas paliativas e/ou rudimentares para que seja possível manter o mínimo necessário de segurança lógica que um ambiente corporativo exige. A aquisição de uma solução de Next Generation Firewall – NGFW, composta com Access Points e Switches integrados, irão garantir que todo escopo de segurança da informação seja protegido contra os mais modernos ataques cibernéticos.

Tais medidas são fundamentais para manter e assegurar a disponibilidade adequada dos serviços de TI, que dão apoio a alta gestão da DPE/PA, em casos de tentativa de exploração de vulnerabilidade, além de permitir a continuidade das operações, apoiando os demais setores desta instituição, de forma a manter seus dados íntegros, seguros e disponíveis.

Aquisição de hardwares, softwares e licenciamentos para implantação e modernização tecnológica da infraestrutura de segurança da informação, tem o objetivo de não só aumentar a capacidade de proteção de todos os ativos de TI, mas também as informações elencadas como estratégica pela Defensoria Pública do PA, sendo possível o reconhecimento e padronização de uso das aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões de acesso a sistemas, sites web e dados na DPE/PA.

A infraestrutura de T.I.C é elemento fundamental para a gestão do ambiente tecnológico da Assembleia Legislativa e o alcance do bom desempenho de suas atribuições institucionais. Uma solução integrada de gerenciamento do ciclo de vida das informações, é composta por componentes de software que permitem gerenciar e monitorar o fluxo das informações trafegadas, além de uma infraestrutura de hardware, que se destina basicamente ao efetivo processamento desse fluxo.

Nesse mesmo tema, destaca-se que atualmente a DPE/PA mantém uma diversidade de Soluções de Tecnologia, nos quais vários softwares e equipamentos de diversos fabricantes interagem com serviços providos por uma gama de outros prestadores.

Isso eleva o nível complexidade tecnológica do ambiente computacional da DPE/PA, isto é, fatores que exigem da Equipe Técnica do NTI, um grande esforço no sentido de torná-lo íntegro e, tanto quanto possível, disponível para os seus usuários internos e externos, cujos trabalhos

dependem de forma direta e incisiva do pleno funcionamento e da alta disponibilidade deste ambiente computacional.

Entende-se, portanto, que a atual infraestrutura de segurança da informação da DPE/PA apresenta sinais claros de necessidade de novos investimentos, considerando-se, nesse caso, as perspectivas de modernização e de expansão no âmbito da Entidade para atendimento geral.

Dessa forma, a DPE/PA, por intermédio de seu Núcleo de Tecnologia da Informação - NTI, necessita planejar e executar a expansão dos seus recursos tecnológicos, pela qual, tomando como referência os atos normativos e instrumentos legais afetos a esse propósito, bem como os padrões atuais de mercado de hardware, software, associados às políticas para proteção e armazenamento de dados e relacionadas a serviços de infraestrutura de TI, proporcione uma solução integrada para provimento de serviços por meio de alta disponibilidade tecnológica.

Por razões como essas, considera-se que os processos de gestão das demandas institucionais que envolvem TI precisam ser dotados de agilidade, confiança, segurança, bem como de prestação eficaz de serviços e de infraestrutura adequada, esta disponibilizada por meio de softwares, equipamentos e componentes eficientes e funcionais, para suportar os sistemas corporativos e, finalmente, atender às reais necessidades da DPE/PA e corresponder, positivamente, às expectativas dos assistidos e usuários envolvidos no contexto da Defensoria Pública do Estado do Pará.

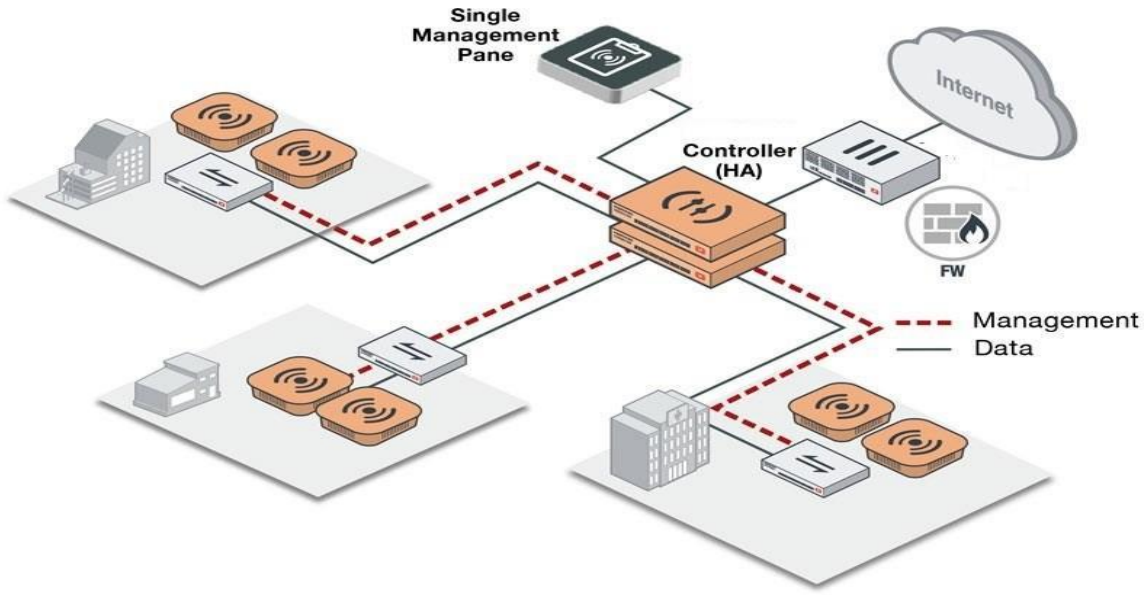
Portanto, em face das razões acima expostas, elaboramos o presente Termo de Referência, com o fim de instruir procedimento administrativo licitatório objetivando contratação de empresa para o fornecimento de Solução de INFRAESTRUTURA DE DATACENTER SEGURO para a Defensoria Pública do Estado do Pará.

- Quadro de estimativa de equipamentos e software de segurança:

ITEM	DESCRIÇÃO DO OBJETO	QTD. ESTIMADA
1	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01	2
2	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02	10
3	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 03	20
4	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 04	30
5	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 05	45
6	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO (PACOTE 10 EQUIPAMENTOS)	10
7	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATORIA (PACOTE 5G/LOG DIA)	5
8	SWITCH CONCENTRADOR (CORE)	4
9	SWITCH DE ACESSO 24 PORTAS POE - TIPO 01	16
10	SWITCH DE ACESSO 24 PORTAS POE - TIPO 02	100
11	SWITCH DE ACESSO 48 PORTAS POE - TIPO 01	16
12	SWITCH DE ACESSO 48 PORTAS POE - TIPO 02	20

13	SWITCH DE ACESSO 8 PORTAS POE	77
14	PONTO DE ACESSO - TIPO 01	155
15	PONTO DE ACESSO - TIPO 02	80
16	TRANSCEIVER SFP+ 10GBASE-T	50
17	TRANSCEIVER SFP+ 10GBASE-SR	50
18	TRANSCEIVER SFP+ 10GBASE-LR	50
19	CONTROLE DE ACESSO A REDE (NAC)	1
20	SERVIÇOS DE TREINAMENTO DAS SOLUÇÕES (POR SOLUÇÃO)	14
21	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (POR SOLUÇÃO)	36
22	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPO 1	2
23	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPOS 2, 3, 4 e 5	105
24	SERVIÇOS DE INSTALAÇÃO DE SWITCHES	229
25	SERVIÇOS DE INSTALAÇÃO DE APs	235
26	SERVIÇO DE INSTALAÇÃO DOS ITENS 6, 7 e 19	16

As atividades acima descritas são sugestões de trabalho, não sendo o único modelo ou sequência de possível, todavia almeja-se, ao final, das atividades que a DPE/PA alcance a arquitetura ilustrada abaixo.



Com o objetivo de otimizar as atividades a serem desempenhadas, pela equipe técnica da DITEC, com a eventual aquisição das soluções em estudo, busca-se padronizar ao máximo os fabricantes itens apresentados na tabela acima. Mais especificamente quanto ao Firewall de próxima Geração (NGFW), switches e Pontos de acesso. Desta forma, um único painel de gerência dos ativos será utilizado (o que torna eficiente o trabalho realizado pela equipe técnica, fazendo mais com menos), a diminuição de números de contratos a serem geridos (facilitando possíveis resoluções de problemas – tanto técnicos quanto jurídicos).

As quantidades foram calculadas com base nas capacidades finais desejadas para cada estação de trabalho e do número de computadores atualmente disponíveis no parque, com uma sobra se segurança operacional de cerca de 30% a ser implantado ao longo de 24 meses.

ESPECIFICAÇÕES TÉCNICAS

1. KIT SOLUÇÃO DE FIREWALL DE PRÓXIMA GERAÇÃO (NGFW)

1.1. CARACTERÍSTICAS GERAIS PARA FIREWALLS DE PRÓXIMA GERAÇÃO TIPOS 01 A 04

1.1.1. 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.

1.1.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

1.1.3. 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;

1.1.4. 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;

1.1.5. 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;

1.1.6. Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) 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.

1.2. FUNCIONALIDADES DE REDE E FIREWALL

1.2.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;

1.2.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;

1.2.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);

1.2.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;

1.2.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;

1.2.6. 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;

1.2.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

1.2.8. Deverá suportar sFlow ou Netflow;

1.2.9. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;

1.2.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;

1.2.11. Deve suportar o protocolo padrão da indústria VXLAN;

1.2.12. Deve implementar o protocolo ECMP;

1.2.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;

1.2.14. Enviar log para sistemas de monitoração externos;

1.2.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;

1.2.16. Deve possui mecanismos de proteção anti-spoofing;

1.2.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);

1.2.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

1.2.19. Suportar OSPF graceful restart;

1.2.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

1.2.21. Deve suportar Modo Camada - 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;

1.2.22. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;

1.2.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;

1.2.24. 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;

1.2.25. 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;

1.2.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;

1.2.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;

1.2.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;

1.2.29. 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;

1.2.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;

1.2.31. Deverá suportar controle por zonas de segurança;

1.2.32. Deverá suportar controles de políticas por porta e protocolo;

1.2.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
1.2.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
1.2.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
1.2.36. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);
1.2.37. Deve decriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;
1.2.38. 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;
1.2.39. Suporte a objetos e regras IPV6;
1.2.40. Suporte a objetos e regras multicast;
1.2.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.3. FUNCIONALIDADE DE CONTROLE DE APLICAÇÕES

1.3.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
1.3.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
1.3.3. 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;
1.3.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;
1.3.5. 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;
1.3.6. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
1.3.7. 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;
1.3.8. Para tráfego criptografado SSL, deve decriptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
1.3.9. 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;
1.3.10. Identificar o uso de táticas evasivas via comunicações criptografadas;
1.3.11. Atualizar a base de assinaturas de aplicações automaticamente;
1.3.12. 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;

1.3.13. 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;

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

1.3.15. 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;

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

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

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

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

1.3.20. 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;

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

1.3.22. 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);

1.3.23. 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;

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

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

1.4. FUNCIONALIDADE DE PREVENÇÃO DE INTRUSÃO E AMEAÇAS

1.4.1. 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;

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

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

1.4.4. 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;

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

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

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

1.4.8. 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;

1.4.9. Deve permitir o bloqueio de vulnerabilidades;

1.4.10. Deve permitir o bloqueio de exploits conhecidos;

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

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

1.4.13. Detectar e bloquear a origem de portscans;

1.4.14. Bloquear ataques efetuados por worms conhecidos;

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

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

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

1.4.18. 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;

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

1.4.20. Identificar e bloquear comunicação com botnets;

1.4.21. 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;

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

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

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

1.4.25. 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.

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

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

1.4.28. 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;

1.5. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB E DNS

1.5.1. 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);

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

1.5.3. 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;

1.5.4. 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;

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

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

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

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

1.5.9. Permitir a customização de página de bloqueio;

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

1.5.11. 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;

1.5.12. 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;

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

1.6. FUNCIONALIDADE DE IDENTIFICAÇÃO DE USUÁRIOS

1.6.1. 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;

1.6.2. 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;

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

1.6.4. 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;

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

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

1.6.7. 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);

1.6.8. 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;
1.6.9. Deve suportar o envio e recebimento de credenciais via RADIUS;
1.6.10. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

1.7. FUNCIONALIDADE DE FILTRO DE DADOS
1.7.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
1.7.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
1.7.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
1.7.4. 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.

1.8. FUNCIONALIDADE DE GEOLOCALIZAÇÃO
1.8.1. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
1.8.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.9. FUNCIONALIDADE DE VPN
1.9.1. Suportar VPN Site-to-Site e Cliente-To-Site;
1.9.2. Suportar IPSec VPN;
1.9.3. Suportar SSL VPN;
1.9.4. A VPN IPSEc deve suportar 3DES;
1.9.5. A VPN IPSEc deve suportar Autenticação MD5 e SHA-1;
1.9.6. A VPN IPSEc deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
1.9.7. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
1.9.8. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
1.9.9. A VPN IPSEc deve suportar Autenticação via certificado IKE PKI
1.9.10. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
1.9.11. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
1.9.12. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;
1.9.13. 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;
1.9.14. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
1.9.15. 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;
1.9.16. Atribuição de DNS nos clientes remotos de VPN;

1.9.17. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
1.9.18. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
1.9.19. Suportar leitura e verificação de CRL (Certificate Revocation List);
1.9.20. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
1.9.21. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;
1.9.22. Deve permitir que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;
1.9.23. Deverá manter uma conexão segura com o portal durante a sessão;
1.9.24. 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);

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

1.10.1. 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;
1.10.2. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:
10.10.1.1. Endereço de origem;
10.10.1.2. Endereço de destino;
10.10.1.3. Usuário e grupo;
10.10.1.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
10.10.1.5. Por porta;
1.10.3. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
1.10.4. 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;
1.10.5. O QoS deve possibilitar a definição de fila de prioridade;
10.10.2. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;
10.10.3. Suportar marcação de pacotes Diffserv, inclusive por aplicação;
10.10.4. Suportar modificação de valores DSCP para o Diffserv;
10.10.5. Suportar priorização de tráfego usando informação de ToS (Type of Service);
10.10.6. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;
10.10.7. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;
10.10.8. Deve possibilitar a definição de bandas distintas para download e upload;

1.11. FUNCIONALIDADE DE BALANCEAMENTO INTELIGENTE DE LINKS

1.11.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

1.11.2. A solução deve ser capaz de agregar vários links em uma interface virtual;

1.11.3. 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);

1.11.4. 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;

1.11.5. 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;

1.11.6. 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);

1.11.7. 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).

1.11.8. 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:

1.11.8.1. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.

1.11.8.2. 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;

1.11.8.3. 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;

1.11.8.4. 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;

1.11.9. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;

1.11.10. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);

1.11.11. 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);

1.11.12. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;

1.11.13. 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;

1.11.14. 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;

1.11.15. 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;

1.11.16. 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;

1.11.17. A solução deve suportar nativamente conectores com clouds públicas;

1.11.18. Deve possibilitar a definição de largura de banda distintas nas interfaces para download e upload;

1.11.19. 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);

1.11.20. Deve implementar balanceamento de link por hash do IP de origem;

1.11.21. Deve implementar balanceamento de link por hash do IP de origem e destino;

1.11.22. 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;

1.11.23. 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;

1.11.24. 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.

1.12. FUNCIONALIDADE DE CONTROLADOR DE REDE SEM FIO

1.12.1. 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:

1.12.1.1. Deve permitir a conexão de dispositivos sem fio que implementem os padrões IEEE 802.11a/b/g/n/ac/ax;

1.12.1.2. Deve permitir a conexão de dispositivos wireless que transmitam tráfego IPv4 e IPv6;

1.12.1.3. A solução deverá ser capaz de gerenciar pontos de acesso que estejam conectados remotamente através de links WAN e Internet;

1.12.1.4. Deve permitir ser descoberto automaticamente pelos pontos de acesso através de Broadcast, DHCP e consulta DNS;

1.12.1.5. 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;

1.12.1.6. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points;

1.12.1.7. 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;

1.12.1.8. 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;

1.12.1.9. 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;

1.12.1.10. 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;

1.12.1.11. 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;

1.12.1.12. A solução deve permitir definir quais redes serão tuneladas até o controlador e quais redes serão comutadas diretamente pela interface do ponto de acesso;

1.12.1.13. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

1.12.1.14. 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;

1.12.1.15. 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;

1.12.1.16. 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;

1.12.1.17. 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;

1.12.1.18. 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;

1.12.1.19. 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;

1.12.1.20. 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;

1.12.1.21. 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;

1.12.1.22. 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;

1.12.1.23. 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;

1.12.1.24. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;

1.12.1.25. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;

1.12.1.26. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

1.12.1.27. 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;

1.12.1.28. 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;

1.12.1.29. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;

1.12.1.30. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;

1.12.1.31. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;

1.12.1.32. 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;

1.12.1.33. 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;

1.12.1.34. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;

1.12.1.35. 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;

1.12.1.36. A solução deve suportar a configuração do BLE (Blueooth Low Energy) nos pontos de acesso que tenham este recurso;

1.12.1.37. 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;

1.12.1.38. 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;

1.12.1.39. A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;

1.12.1.40. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;

1.12.1.41. 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;

1.12.1.42. 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;

1.12.1.43. 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;

1.12.1.44. Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;

1.12.1.45. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

1.12.1.46. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;

1.12.1.47. A solução deve permitir a configuração de múltplas chaves de autenticação PSK para utilização em um determinado SSID;

1.12.1.48. 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;

1.12.1.49. 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;

1.12.1.50. 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;

1.12.1.51. 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;

1.12.1.52. 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;

1.12.1.53. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;

1.12.1.54. 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;

1.12.1.55. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;

1.12.1.56. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;

1.12.1.57. A solução deve permitir a configuração do captive portal com endereço IPv6;

1.12.1.58. 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;

1.12.1.59. 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;

1.12.1.60. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;

1.12.1.61. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;

1.12.1.62. A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;

1.12.1.63. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;

1.12.1.64. 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;

1.12.1.65. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados;

1.12.1.66. A solução deve permitir a configuração de rede Mesh entre pontos de acesso indoor e outdoor;

1.12.1.67. 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;

1.12.1.68. A solução deve permitir ser gerenciada através dos protocolos HTTPS e SSH via IPv4 e IPv6;

1.12.1.69. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos;

1.12.1.70. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps;

1.12.1.71. A solução deve permitir que softwares de gerenciamento realizem consultas diretamente nos pontos de acesso via protocolo SNMP;

1.12.1.72. A solução deve incluir suporte para as RFCs 1213 (MIB II) e RFC 2665 (Ethernet-like MIB);

1.12.1.73. A solução deve permitir a captura de pacotes na rede wireless e exportá-los em arquivos no formato .pcap;

1.12.1.74. 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;

1.12.1.75. 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;

1.12.1.76. A solução deve permitir o gerenciamento unificado e de forma gráfica para redes WiFi e redes cabeadas;

1.12.1.77. A solução deve permitir a atualização de firmware do controlador wireless mesmo quando conectado remotamente;

1.12.1.78. A solução deve permitir a identificação do firmware utilizado por cada ponto de acesso gerenciado e permitir a atualização via interface gráfica;

1.12.1.79. 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;

1.12.1.80. A solução deve possuir ferramentas de diagnósticos e debug;

1.12.1.81. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de um ponto de acesso;

1.12.1.82. A solução deve suportar comunicação com elementos externos através de REST API;

1.12.1.83. A solução deverá ser compatível e gerenciar os pontos de acesso deste processo;

1.13. FUNCIONALIDADE DE CONTROLADOR DE REDE CABEADA

1.13.1. 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:

1.13.1.1. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;
1.13.1.2. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;
1.13.1.3. 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;
1.13.1.4. Deve montar a topologia da rede de maneira automática;
1.13.1.5. Deve ser capaz de configurar os switches da rede;
1.13.1.6. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribui-las automaticamente em todos os switches gerenciados;
1.13.1.7. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
1.13.1.8. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
1.13.1.9. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
1.13.1.10. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;
1.13.1.11. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
1.13.1.12. 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,;
1.13.1.13. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
1.13.1.14. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
1.13.1.15. Deve ser capaz de configurar parâmetros SNMP dos switches;
1.13.1.16. 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;
1.13.1.17. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
1.13.1.18. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;
1.13.1.19. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;
1.13.1.20. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
1.13.1.21. Deve prover indicadores de saúde dos elementos críticos do ambiente;
1.13.1.22. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
1.13.1.23. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede.

1.14. ITEM 01 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01

1.14.1. Deve suportar, no mínimo, 130 (cento e trinta) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

1.14.2. Deve suportar, no mínimo, 7 (sete) milhões de conexões simultâneas;

1.14.3. Deve suportar, no mínimo, 600.000 (seiscentas mil) novas conexões por segundo;

1.14.4. Deve Suportar, no mínimo, 50 (cinquenta) Gbps de throughput VPN IPSec;

1.14.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 10.000 (dez mil) túneis de VPN IPSEC Site-to-Site simultâneos;

1.14.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 50.000 (cinquenta mil) túneis de clientes VPN IPSEC simultâneos;

1.14.7. Deve suportar, no mínimo, 5 (cinco) Gbps de throughput de VPN SSL;

1.14.8. Deve suportar, no mínimo, 10.000 (dez mil) clientes de VPN SSL simultâneos;

1.14.9. Deve suportar, no mínimo, 18 (dezoito) Gbps de throughput de IPS;

1.14.10. Deve suportar, no mínimo, 10 (dez) Gbps de throughput de Inspeção SSL;

1.14.11. Deve suportar, no mínimo, 12 (doze) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware.

1.14.12. Deve possuir, pelo menos, 8 (oito) interfaces 10 Gigabit Ethernet 10GBase-T com conectores RJ-45;

1.14.13. Deve possuir, pelo menos, 16 (dezesseis) interfaces com suporte a conectores SFP+ de 10 Gigabit Ethernet e SFP de 1 Gigabit Ethernet;

1.14.14. Deve possuir, pelo menos, 8 (oito) interfaces com suporte a conectores SFP28 de 25 Gigabit Ethernet, SFP+ de 10 Gigabit Ethernet e SFP de 1 Gigabit Ethernet;

1.14.15. Deve possuir, pelo menos, 2 (duas) interfaces com suporte a conectores QSFP28 de 100 Gigabit Ethernet e QSFP+ de 40 Gigabit Ethernet;

1.14.16. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;

1.14.17. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para Alta-Disponibilidade;

1.14.18. Deve estar licenciado para gerenciar até 190 (cento e noventa) switches e 2.000 (dois mil) pontos de acesso sem fio simultaneamente em um único appliance;

1.14.19. Deve possuir fonte de alimentação AC redundante e HotSwap;

1.14.20. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

1.15. ITEM 02 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02

1.15.1. Deve suportar, no mínimo, 10 (dez) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

1.15.2. Deve suportar, no mínimo, 3 (três) milhões de conexões simultâneas;

1.15.3. Deve suportar, no mínimo, 250.000 (duzentas e cinquenta mil) novas conexões por segundo;

1.15.4. Deve Suportar, no mínimo, 12 (doze) Gbps de throughput VPN IPSec;

1.15.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de VPN IPSEC Site-to-Site simultâneos;
1.15.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 10.000 (dez mil) túneis de clientes VPN IPSEC simultâneos;
1.15.7. Deve suportar, no mínimo, 02 (dois) Gbps de throughput de VPN SSL;
1.15.8. Deve suportar, no mínimo, 500 (quinhentos) clientes de VPN SSL simultâneos;
1.15.9. Deve suportar, no mínimo, 05 (cinco) Gbps de throughput de IPS;
1.15.10. Deve suportar, no mínimo, 04 (quatro) Gbps de throughput de Inspeção SSL;
1.15.11. Deve suportar, no mínimo, 03 (três) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware.
1.15.12. Deve possuir, pelo menos, 16 (dezesseis) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
1.15.13. Deve possuir, pelo menos, 8 (oito) interfaces Gigabit Ethernet com conectores SFP;
1.15.14. Deve possuir, pelo menos, 4 (quatro) interfaces 10 Gigabit Ethernet com conectores SFP+;
1.15.15. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para gerenciamento;
1.15.16. Deve possuir 1 (uma) Interface Ethernet RJ45 10/100/1000 dedicada para Alta-Disponibilidade;
1.15.17. Deve estar licenciado para gerenciar até 60 (sessenta) switches e 120 (cento e vinte) pontos de acesso sem fio simultaneamente em um único appliance;
1.15.18. Deve possuir fonte de alimentação AC redundante;
1.15.19. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

1.16. ITEM 03 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL PRÓXIMA GERAÇÃO (NGFW) - TIPO 03

1.16.1. Deve suportar, no mínimo, 10 (dez) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;
1.16.2. Deve suportar, no mínimo, 1.5 Milhão (um milhão e quinhentas mil) conexões simultâneas;
1.16.3. Deve suportar, no mínimo, 50.000 (cinquenta mil) novas conexões por segundo;
1.16.4. Deve Suportar, no mínimo, 10 (dez) Gbps de throughput VPN IPSec;
1.16.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2.000 (dois mil) túneis de VPN IPSEC Site-to-Site simultâneos;
1.16.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 10.000 (dez mil) túneis de clientes VPN IPSEC simultâneos;
1.16.7. Deve suportar, no mínimo, 01 (um) Gbps de throughput de VPN SSL;
1.16.8. Deve suportar, no mínimo, 500 (quinhentos) clientes de VPN SSL simultâneos;
1.16.9. Deve suportar, no mínimo, 02 (dois) Gbps de throughput de IPS;
1.16.10. Deve suportar, no mínimo, 01 (um) Gbps de throughput de Inspeção SSL;
1.16.11. Deve suportar, no mínimo, 01 (um) Gbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware.

1.16.12. Deve possuir, pelo menos, 16 (dezesseis) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
1.16.13. Deve possuir, pelo menos, 08 (oito) interfaces Gigabit Ethernet com conectores SFP;
1.16.14. Deve possuir, pelo menos, 02 (duas) interfaces 10 Gigabit Ethernet com conectores SFP+;
1.16.15. Deve estar licenciado para gerenciar até 30 (trinta) switches e 60 (sessenta) pontos de acesso sem fio simultaneamente em um único appliance;
1.16.16. Deve possuir fonte de alimentação AC redundante;
1.16.17. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

1.17. ITEM 04 - CARACTERÍSTICAS ESPECÍFICAS E PERFORMANCE DO FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) – TIPO 04

1.17.1. Deve suportar, no mínimo, 05 (cinco) Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;
1.17.2. Deve suportar, no mínimo, 700.000 (setecentos mil) conexões simultâneas;
1.17.3. Deve suportar, no mínimo, 35.000 (trinta e cinco mil) novas conexões por segundo;
1.17.4. Deve Suportar, no mínimo, 06 (seis) Gbps de throughput VPN IPSec;
1.17.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Site-to-Site simultâneos;
1.17.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 400 (quatrocentos) túneis de clientes VPN IPSEC simultâneos;
1.17.7. Deve suportar, no mínimo, 800 (oitocentos) Mbps de throughput de VPN SSL;
1.17.8. Deve suportar, no mínimo, 200 (duzentos) clientes de VPN SSL simultâneos;
1.17.9. Deve suportar, no mínimo, 01 (um) Gbps de throughput de IPS;
1.17.10. Deve suportar, no mínimo, 600 (seiscentos) Mbps de throughput de Inspeção SSL;
1.17.11. Deve suportar, no mínimo, 700 (setecentos) Mbps de throughput com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação, IPS e AntiMalware.
1.17.12. Deve possuir, pelo menos, 10 (dez) interfaces Gigabit Ethernet 1000Base-T com conectores RJ-45;
1.17.13. Deve estar licenciado para gerenciar até 20 (vinte) switches e 30 (trinta) pontos de acesso sem fio simultaneamente em um único appliance;
1.17.14. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;

1.18. ITEM 05 - GERENCIAMENTO DE CONFIGURAÇÃO CENTRALIZADO

1.18.1. Deve estar dimensionado e licenciado para gerenciar até 10 (dez) Firewalls de Próxima Geração (NGFW) considerando os modelos ofertados neste processo atendendo aos requisitos deste Item;
1.18.2. 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;

1.18.3. 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;

1.18.4. Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;

1.18.5. Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;

1.18.6. Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;

1.18.7. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;

1.18.8. 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);

1.18.9. 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;

1.18.10. 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;

1.18.11. Permitir criar templates de configuração dos dispositivos com informações de DNS, SNMP, Configurações de LOG e Administração;

1.18.12. Deve suportar o conceito de multi-tenancy visando permitir a gestão de ambientes independentes uns dos outros a partir da mesma solução.

1.18.13. A solução deve permitir o uso de APIs RESTful para permitir a interação com portais personalizados na configuração de objetos e políticas de segurança;

1.18.14. 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;

1.18.15. Permitir acesso concorrente de administradores e que seja definida uma cadeia de aprovação das alterações realizadas;

1.18.16. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;

1.18.17. Permitir usar palavras chaves ou cores para facilitar identificação de regras;

1.18.18. Permitir localizar em quais regras um objeto (ex. computador, serviço, etc.) está sendo utilizado;

1.18.19. Atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;

1.18.20. Permitir criação de regras que fiquem ativas em horário definido;

1.18.21. Permitir criação de regras com data de expiração;

1.18.22. Realizar o backup das configurações para permitir o retorno de uma configuração salva;

1.18.23. 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.

1.18.24. Gerar alertas automáticos via Email, SNMP e Syslog;

1.18.25. Deve ser permitido ao administrador transferir os backups para um servidor FTP, SCP ou SFTP.

1.18.26. Permitir backup das configurações e rollback de configuração para a última configuração salva;

1.18.27. Deve possibilitar a visualização e comparação de configurações atuais e configurações anteriores;

1.18.28. 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;

1.18.29. Deve suportar a distribuição e instalação remota de novas versões de software dos equipamentos, de forma remota e centralizada;

1.18.30. Permitir criar os objetos que serão utilizados nas políticas de forma centralizada;

1.18.31. Deve suportar autenticação de administradores em base local e de modo remoto por meio de RADIUS, LDAP, TACACS+ e PKI.

1.18.32. 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.

1.18.33. A solução deve possibilitar a distribuição e instalação remota, de maneira centralizada, de novas versões de software dos appliances.

1.18.34. Deve suportar o gerenciamento de pontos de acesso de forma centralizada.

1.18.35. Deve suportar o gerenciamento centralizado de switches.

1.18.36. A solução deve possuir garantia, suporte e atualizações ao software durante a vigência do contrato.

2. ITEM 06 - GERENCIAMENTO DE LOGS E RELATORIA CENTRALIZADO

2.1. Deve suportar o acesso via SSH, WEB (HTTPS) para gerenciamento da solução;

2.2. A solução deve suportar receber, no mínimo, 5 (cinco) GB de logs diários;

2.3. 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;

2.4. 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;

2.5. Caso a solução seja entregue em appliance virtual, não deve possuir limite na quantidade de múltiplas vCPU;

2.6. Caso a solução seja entregue em appliance virtual, não deve possuir limite para suporte a expansão de memória RAM;

2.7. Caso a solução seja ofertada em appliance físico, deverá ser em hardware do próprio fabricante;

2.8. A solução deverá estar devidamente licenciada com suporte durante todo o tempo de contrato;

2.9. A solução deverá ser capaz de armazenar logs por no mínimo 12 (doze) meses;

2.10. Permitir acesso simultâneo à administração, bem como criar pelo menos 2 (dois) perfis para administração e monitoramento;

2.11. Possuir suporte para SNMP versão 2 e 3;

2.12. Permitir a virtualização do gerenciamento e administração dos dispositivos, onde cada administrador tem acesso apenas aos equipamentos autorizados;
2.13. Deve permitir a criação de um administrador geral, que tenha acesso geral a todas as instâncias de virtualização da solução;
2.14. 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;
2.15. Suporte a autenticação de usuários de acesso à plataforma via LDAP, Radius ou TACACS+;
2.16. Deve suportar a configuração Master / Slave de alta disponibilidade em camada 3;
2.17. Deve permitir gerar alertas de eventos a partir de logs recebidos;
2.18. A solução deve ter relatórios predefinidos;
2.19. Permitir importação e exportação de relatórios
2.20. Suporte a geração de relatórios de tráfego em tempo real, em formato de mapa geográfico;
2.21. Suporte a geração de relatórios de tráfego em tempo real, no formato de gráfico de bolhas;
2.22. Suporte a geração de relatórios de tráfego em tempo real, em formato de tabela gráfica;
2.23. Deve ter a capacidade de personalizar gráficos em relatórios, como barras, linhas e tabelas;
2.24. Deve ter a capacidade de personalizar a capa dos relatórios obtidos;
2.25. Deve ter a capacidade de gerar e enviar relatórios periódicos automaticamente;
2.26. Deve ter a capacidade de criar relatórios no formato HTML, CSV, XML e PDF;
2.27. Deve conter um assistente gráfico para adicionar novos dispositivos, usando seu endereço IP, usuário e senha;
2.28. Deve ser possível ver a quantidade de logs enviados de cada dispositivo monitorado;
2.29. Deve possuir mecanismos de remoção automática para logs antigos;
2.30. Deve ter um mecanismo de "pesquisa detalhada" ou "Drill-Down" para navegar pelos relatórios em tempo real;
2.31. Permitir a personalização de qualquer relatório pré-estabelecido pela solução, exclusivamente pelo Administrador, para adotá-lo de acordo com suas necessidades;
2.32. Permitir o envio por e-mail relatórios automaticamente;
2.33. Deve permitir que o relatório seja enviado por Email para o destinatário específico;
2.34. Permitir a programação da geração de relatórios, conforme calendário definido pelo administrador;
2.35. Permitir a exibição graficamente e em tempo real da taxa de geração de logs para cada dispositivo gerenciado;
2.36. Deve permitir o uso de filtros nos relatórios;
2.37. Deve permitir definir o design dos relatórios, incluir gráficos, adicionar texto e imagens, alinhamento, quebras de página, fontes, cores, entre outros;
2.38. Permitir especificar o idioma dos relatórios criados;
2.39. Gerar alertas automáticos via e-mail, SNMP e Syslog, com base em eventos especiais em logs, gravidade do evento, entre outros;
2.40. Deve permitir o envio automático de relatórios para um servidor SFTP ou FTP externo;
2.41. Deve permitir o envio automático dos logs para um servidor FTP externo a solução;
2.42. Deve permitir exportar os logs no formato CSV;

2.43. Deve permitir que os arquivos de log sejam baixados da plataforma para uso externo;

2.44. Deve permitir a geração de logs de auditoria, com detalhes da configuração efetuada, o administrador que efetuou a alteração e seu horário;

2.45. 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;

2.46. Deve ser capaz de criar consultas SQL ou similares nos bancos de dados de logs, para uso em gráficos e tabelas em relatórios;

2.47. 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;

2.48. Deve fornecer as informações da quantidade de logs armazenados e as estatísticas do tempo restante armazenado;

2.49. Deve permitir aplicar políticas para o uso de senhas para administradores de plataforma, como tamanho mínimo e caracteres permitidos;

2.50. Deve permitir visualizar em tempo real os logs recebidos;

2.51. Deve permitir o encaminhamento de log no formato syslog e CEF (Common Event Format);

2.52. 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;

2.53. 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;

2.54. Deve possuir um painel de operações que monitore as principais ameaças à segurança da sua rede;

2.55. Deve possuir um painel de operações que monitora o envolvimento do usuário e o uso suspeito da web em sua rede;

2.56. Deve possuir um painel de operações que monitora o tráfego da rede, aplicativos e sites web;

2.57. Deve possuir um painel de operações que monitoram a atividade da VPN em sua rede;

2.58. Deve possuir um painel de operações que monitoram o desempenho dos recursos locais da solução (CPU, Memória)

2.59. Deve permitir a criação de painéis personalizados para monitorar operações de segurança e rede;

2.60. Deve possuir relatório de uso de aplicações e mídias sociais;

2.61. Deve possuir relatório de prevenção de perda de dados (DLP);

2.62. Deve possuir relatório de VPN, Prevenção de Intrusão (IPS), análise de ameaças cibernéticas;

2.63. Deve possuir relatório diário resumido de eventos e incidentes de segurança;

2.64. Deve possuir um relatório de tráfego DNS e e-mail;

2.65. Deve possuir relatório das 10 principais aplicações utilizadas na rede;

2.66. Deve possuir relatório dos 10 principais sites web utilizados na rede;

2.67. 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);

2.68. 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;

2.69. 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;

2.70. Deve suportar a análise detalhada dos computadores comprometidos e exibir os detalhes das ameaças detectadas;

2.71. 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;

2.72. 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;

3. ITEM 07 – SWITCH CONCENTRADOR (CORE)

3.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

3.2. Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

3.3. Deve possuir 48 (quarenta e oito) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE;

3.4. Adicionalmente, deve possuir 4 (quatro) slots QSFP28 para conexão de fibras ópticas operando com velocidades de 40 e 100 Gigabit Ethernet;

3.5. Deve permitir a configuração das interfaces QSFP28 para que operem com conexões do tipo "breakout" ou "split", modo em que uma determinada porta 40GbE pode operar com 4 conexões em 10GbE. Deve permitir ainda que as portas 100GbE sejam divididas em 4 conexões de 25GbE;

3.6. 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;

3.7. Deve possuir interface dedicada para gerenciamento local do tipo "out-of-band". Esta interface de gerenciamento deverá possuir porta 1000Base-T com conector RJ-45;

3.8. Deve possuir 1 (uma) interface USB;

3.9. Deve possuir capacidade de comutação de pelo menos 1.76 Tbps (terabits por segundo) e ser capaz de encaminhar até 1.5 Bpps (bilhões de pacotes por segundo);

3.10. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

3.11. 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;

3.12. Deve possuir tabela MAC com suporte a 144.000 endereços;

3.13. Deve operar com latência igual ou inferior à 1us (microsegundo);

3.14. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

3.15. 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;

3.16. Deve suportar o padrão IEEE 802.1Qbb (Priority-based Flow Control);

3.17. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol - LACP);

3.18. 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;

3.19. Deve suportar a comutação de Jumbo Frames;

3.20. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

3.21. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

3.22. 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 exija licenciamento adicional para ativação dos protocolos;

3.23. 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 exija licenciamento adicional para ativação dos protocolos;

3.24. 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 exija licenciamento adicional para ativação do protocolo;

3.25. Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo;

3.26. 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 exija licenciamento adicional para ativação deste recurso;

3.27. Deve implementar serviço de DHCP Server e DHCP Relay;

3.28. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) grupos;

3.29. Deve suportar MLD (Multicast Listener Discovery) Snooping para otimizar a transmissão de tráfego multicast em IPv6;

3.30. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN);

3.31. 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;

3.32. 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;

3.33. 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;

3.34. 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;

3.35. 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;

3.36. 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;

3.37. 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;

3.38. 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;

3.39. 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;

3.40. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

3.41. Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

3.42. 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;

3.43. 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);

3.44. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

3.45. 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;

3.46. Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement;

3.47. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

3.48. Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

3.49. 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;

3.50. 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;

3.51. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

3.52. Deve suportar MAC Authentication Bypass (MAB);

3.53. Deve implementar RADIUS CoA (Change of Authorization);

3.54. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

3.55. 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;

3.56. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

3.57. 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;

3.58. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

3.59. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

3.60. Deve suportar o protocolo PTP (Precision Time Protocol);

3.61. Deve implementar Netflow, sFlow ou similar;

3.62. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

3.63. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

3.64. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

3.65. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

3.66. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

3.67. Deve permitir ser gerenciado através de IPv6;

3.68. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

3.69. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

3.70. 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;

3.71. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

3.72. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;

3.73. Deverá suportar ser configurado e monitorado através de REST API;

3.74. 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;

3.75. Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash;

3.76. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

3.77. Deve suportar temperatura de operação de até 40º Celsius;

3.78. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

3.79. Deve ser fornecido com fontes de alimentação redundantes do tipo hot-swap, com capacidade para operar em tensões de 110V e 220V;

3.80. 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;

3.81. Deve ser fornecido com cabo DAC (Direct Attach Cable) 40GbE QSFP+ de 3 metros;

4. ITEM 08 - SWITCH DE ACESSO 24 PORTAS POE - TIPO 01

4.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;

4.2. Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

4.3. 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);

4.4. 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;

4.5. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 180W;

4.6. 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;

4.7. Deve possuir 1 (uma) interface USB;

4.8. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo);

4.9. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;

4.10. Deve possuir tabela MAC com suporte a 32.000 endereços;

4.11. Deve operar com latência igual ou inferior à 1us (microsegundo);

4.12. Deve implementar Flow Control baseado no padrão IEEE 802.3X;

4.13. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

4.14. Deve suportar a comutação de Jumbo Frames;

4.15. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;

4.16. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

4.17. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

4.18. Deve implementar serviço de DHCP Relay;

4.19. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

4.20. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

4.21. 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;

4.22. 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;

4.23. 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;

4.24. 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;

4.25. 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;

4.26. 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;

4.27. 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;

4.28. 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;

4.29. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

4.30. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

4.31. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;

4.32. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

4.33. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

4.34. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

4.35. 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;

4.36. 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;

4.37. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

4.38. Deve suportar MAC Authentication Bypass (MAB);

4.39. Deve implementar RADIUS CoA (Change of Authorization);

4.40. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

4.41. 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;

4.42. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

4.43. 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;

4.44. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

4.45. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

4.46. 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;

4.47. 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);

4.48. 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;

4.49. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

4.50. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

4.51. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

4.52. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

4.53. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

4.54. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

4.55. Deve permitir ser gerenciado através de IPv6;

4.56. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

4.57. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

4.58. 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;

4.59. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

4.60. 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;

4.61. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;
4.62. Deverá suportar ser configurado e monitorado através de REST API;
4.63. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
4.64. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
4.65. Deve suportar temperatura de operação de até 45º Celsius;
4.66. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
4.67. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
4.68. 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;

5. ITEM 09 - SWITCH DE ACESSO 24 PORTAS POE - TIPO 02
5.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
5.2. Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;
5.3. 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);
5.4. 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;
5.5. 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 a serem alocados em qualquer uma das portas 1000Base-T;
5.6. 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;
5.7. Deve possuir 1 (uma) interface USB;
5.8. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 180 Mpps (milhões de pacotes por segundo);
5.9. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
5.10. Deve possuir tabela MAC com suporte a 32.000 endereços;
5.11. Deve operar com latência igual ou inferior à 1us (microsegundo);
5.12. Deve implementar Flow Control baseado no padrão IEEE 802.3X;
5.13. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);
5.14. Deve suportar a comutação de Jumbo Frames;
5.15. Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz;
5.16. Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs;

5.17. Deve suportar a criação de rotas estáticas em IPv4 e IPv6;

5.18. Deve implementar serviço de DHCP Relay;

5.19. Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) entradas na tabela;

5.20. Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch (port mirroring / SPAN);

5.21. 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;

5.22. 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;

5.23. 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;

5.24. 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;

5.25. 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;

5.26. 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;

5.27. 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;

5.28. 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;

5.29. Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede;

5.30. Deverá implementar priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS);

5.31. Deverá implementar priorização de tráfego baseada nos valores do campo “Differentiated Services Code Point” (DSCP) do cabeçalho IP, conforme definições do IETF;

5.32. Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta;

5.33. Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP;

5.34. Deve implementar DHCP Snooping para mitigar problemas com servidores DHCP que não estejam autorizados na rede;

5.35. 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;

5.36. 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;

5.37. Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X;

5.38. Deve suportar MAC Authentication Bypass (MAB);

5.39. Deve implementar RADIUS CoA (Change of Authorization);

5.40. Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS;

5.41. 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;

5.42. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;

5.43. 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;

5.44. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;

5.45. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;

5.46. 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;

5.47. 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);

5.48. 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;

5.49. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;

5.50. Deve suportar o envio de mensagens de log para servidores externos através de syslog;

5.51. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;

5.52. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);

5.53. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;

5.54. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);

5.55. Deve permitir ser gerenciado através de IPv6;

5.56. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;

5.57. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;

5.58. 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;

5.59. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;

5.60. 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;

5.61. Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN;

5.62. Deverá suportar ser configurado e monitorado através de REST API;

5.63. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);

5.64. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;

5.65. Deve suportar temperatura de operação de até 45º Celsius;

5.66. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;

5.67. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;

5.68. 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;

6. ITEM 10 - SWITCH DE ACESSO 48 PORTAS POE - TIPO 01

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 pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

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;

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;

7. ITEM 11 - SWITCH DE ACESSO 48 PORTAS POE - TIPO 02

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 pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

7.3. 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);

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 740W a serem alocados em qualquer uma das portas 1000Base-T;

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 176 Gbps e ser capaz de encaminhar até 250 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;

8. ITEM 12 - PONTO DE ACESSO SEM FIO - TIPO 01

8.1. Ponto de acesso (AP) que permita acesso dos dispositivos à rede wireless e que possua todas as suas configurações centralizadas em controlador wireless;

8.2. 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;

8.3. Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

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 àqueles 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 listas 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;

9. ITEM 13 - PONTO DE ACESSO SEM FIO - TIPO 02

9.1. Ponto de acesso (AP) apropriado para uso externo, que permita acesso dos dispositivos à rede wireless e que possua todas as suas configurações centralizadas em controlador wireless;
9.2. 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;
9.3. Deve ser compatível e gerenciado pelos itens “Firewall de Próxima Geração (NGFW) - Tipo 01, 02, 03 e 04” deste termo ou por solução do mesmo fabricante que possua gerência centralizada;
9.4. Deve identificar automaticamente o controlador wireless ao qual se conectará;
9.5. Deve permitir ser gerenciado remotamente através de links WAN;
9.6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;
9.7. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;
9.8. O ponto de acesso deve possuir rádio Wi-Fi adicional àqueles 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;
9.9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;
9.10. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente;
9.11. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T, ou superior, com conector RJ-45 para permitir a conexão com a rede LAN;
9.12. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;
9.13. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

9.14. Deve permitir sua alimentação através de Power Over Ethernet (PoE). Deve acompanhar injetor PoE para alimentação do equipamento;

9.15. 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;

9.16. 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;

9.17. 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 listas 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;

9.18. 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;

9.19. Deve permitir operação em modo Mesh;

9.20. Deve possuir potência de irradiação de 25dBm em 2.4GHz e 5GHz;

9.21. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1.2 Gbps em um único rádio;

9.22. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);

9.23. Deve suportar OFDMA com operações em Downlink (DL) e Uplink (UL);

9.24. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax;

9.25. Deve implementar recurso de Target Wake Time (TWT) configurado por SSID;

9.26. Deve suportar BSS Coloring;

9.27. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;

9.28. Deve possuir sensibilidade mínima de -91dBm quando operando em 5GHz com MCS0 (HT20);

9.29. Deve possuir antenas internas ao equipamento com ganho mínimo de 6dBi em 2.4GHz e 6dBi em 5GHz;

9.30. 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;

9.31. 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;

9.32. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;

9.33. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS);

9.34. 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 8 (oito) SSIDs com operação simultânea;

9.35. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

9.36. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3 com 802.1X;

9.37. 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;

9.38. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

9.39. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

9.40. 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;

9.41. 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;

9.42. Deve implementar o padrão IEEE 802.11e;

9.43. Deve implementar o padrão IEEE 802.11h;

9.44. Deve implementar o padrão IEEE 802.3az;

9.45. Deve suportar consultas SNMP diretamente no ponto de acesso;

9.46. Deve suportar consultas REST API diretamente no ponto de acesso;

9.47. Deve possuir estrutura robusta para operação em ambientes externos e permitir ser instalado em paredes e postes. Deve acompanhar os acessórios para fixação em paredes e postes;

9.48. Deve ser capaz de operar em ambientes com temperaturas entre -10 e 60º C;

9.49. O equipamento deve possuir grau de proteção IP67. Não serão aceitos equipamentos instalados em acessórios, por exemplo caixas herméticas, para que alcancem este grau de proteção;

9.50. Deve possuir indicadores luminosos (LED) para indicação de status das interfaces físicas e dos rádios Wi-Fi;

9.51. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;

9.52. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;

9.53. Deve possuir certificado emitido pela Wi-Fi Alliance;

9.54. Deve estar homologado pela ANATEL na data de execução do pregão;

10. ITEM 14 - TRANSCEIVER SFP+ 10GBase-T

10.1. Transceiver SFP+ compatível com o padrão 10GBase-T para cabos de par trançado (cobre) de até 30 metros;

10.2. Deve possuir conector RJ-45;

10.3. Deve ter velocidade de 10GbE;

10.4. Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

11. ITEM 15 - TRANSCEIVER SFP+ 10GBase-SR

11.1. Transceiver SFP+ para conexão de fibras ópticas multimodo;

11.2. Deve ser compatível com o padrão 10GBase-SR para fibras ópticas de até 300m (fibra OM3) e fibras ópticas de até 400m (fibra OM4);

11.3. Deve ter velocidade de 10GbE;

11.4. Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

12. ITEM 16 - TRANSCEIVER SFP+ 10GBase-LR

12.1. Transceiver SFP+ para conexão de fibras ópticas monomodo;

12.2. Deve ser compatível com o padrão 10GBase-LR para fibras ópticas de até 10km;

12.3. Deve possuir conector LC;

12.4. Deve ter velocidade de 10GbE;

12.5. Deve ser do mesmo fabricante e compatível com os equipamentos deste processo.

13. ITEM 17 - SOLUÇÃO DE CONTROLE DE ACESSO À REDE

13.1. CARACTERÍSTICAS GERAIS

13.1.1. 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;

13.1.2. Deve ser uma solução multi-vendor capaz de suportar os switches e concentrador VPN do orgão;

13.1.3. Deve suportar variadas soluções de Wi-Fi do mercado, tais como: Aruba, Ruckus, Cisco, Fortinet, Aerohive e Enterasys, pelo menos;

13.1.4. A solução deve suportar capacidade de expansão para até 2.000 (dois mil) endpoints simultâneos, sem demandar do cliente a troca do hardware/VM;

13.1.5. A solução deve estar licenciada para operação com, pelo menos, 400 (quatrocentos) endpoints conectados simultaneamente;

13.1.6. A solução deve ser entregue em alta disponibilidade;

13.1.7. A solução deve ser capaz de inspecionar tanto IoT quanto estações/notebooks, sem depender de recursos como 802.1X e Mac-address bypass (MAB);

13.1.8. Para estações de trabalho, deve suportar verificação de compliance em VPN IPsec e SSL;

13.1.9. A licença contemplada deverá suportar todas as características exigidas neste termo de referência;

13.1.10. 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;

13.1.11. Deve detectar e classificar automaticamente o tipo dos dispositivos conectados na rede sem a necessidade de softwares instalados nos dispositivos;

13.1.12. Deve permitir determinar o perfil dos dispositivos descobertos por meio de métodos que não exigem a instalação de agentes, incluindo pelo menos os seguintes:
13.1.12.1. Consultas em DHCP Fingerprint;
13.1.12.2. Consultas via protocolos HTTP/HTTPS;
13.1.12.3. Consultas via protocolo SNMP;
13.1.12.4. Consultas via protocolo SSH;
13.1.12.5. Consultas via protocolo Telnet;
13.1.12.6. Consultas de portas TCP;
13.1.12.7. Consultas de portas UDP;
13.1.12.8. MAC OUI;
13.1.12.9. Consultas via protocolo WMI;
13.1.12.10. Protocolo ONVIF;
13.1.12.11. Protocolo NetFlow;
13.1.12.12. Base assinaturas pré-definidas;
13.1.13. A solução deve ser capaz de reconhecer as seguintes informações sobre os dispositivos conectados à rede:
13.1.13.1. Endereço MAC;
13.1.13.2. Endereço IP;
13.1.13.3. Sistema operacional;
13.1.13.4. Nome do host;
13.1.13.5. Horário de conexão;
13.1.13.6. Usuário conectado;
13.1.13.7. Localização.
13.1.14. A solução deve ser capaz de reconhecer os seguintes sistemas operacionais em execução nos dispositivos conectados à rede:
13.1.14.1. Android;
13.1.14.2. Apple iOS para iPhone, iPod e iPad;
13.1.14.3. Chrome OS;
13.1.14.4. Linux;
13.1.14.5. MacOS X;
13.1.14.6. Windows 7, 8 e 10;
13.1.15. Deve lembrar o perfil atribuído a cada dispositivo e verificar sua validade a cada conexão;
13.1.16. Deve permitir a designação de um sponsor para autorizar a categorização dos dispositivos;
13.1.17. Deve permitir a recategorização periódica de dispositivos;
13.1.18. Deve permitir a importação de um arquivo CSV contendo informações sobre os dispositivos a serem registrados;
13.1.19. A solução deve incluir a detecção de dispositivos desconhecidos conectados à rede e adotar medidas de controle para limitar o acesso;
13.1.20. A solução deve suportar autenticação através de EAP-PEAP e EAP-TLS;
13.1.21. A solução deve suportar RADIUS Change of Authorization;
13.1.22. A solução deve suportar MAC Address Bypass;
13.1.23. A solução deve consultar bases LDAP e Active Directory para a identificação de usuários e grupos de usuários;

13.1.24. 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 dinamicamente o acesso à rede;

13.1.25. Deve permitir a definição dos horários em que os dispositivos serão autorizados a conectar na rede;

13.1.26. 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;

13.1.27. 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;

13.1.28. A solução deve permitir o cadastro dos usuários visitantes na base interna da ferramenta para que não seja necessário realizar consultas em bases externas;

13.1.29. A solução deve possuir ferramenta que permita a geração automática de credenciais para usuários visitantes com login e respectivas senhas;

13.1.30. A solução deve possuir ferramenta que permita a criação de credenciais para eventos;

13.1.31. Deve permitir a definição de complexidade da senha dos usuários visitantes;

13.1.32. Deve ser possível definir um período de validade para as contas de usuários visitantes;

13.1.33. Deve ser possível definir data e horário para início e encerramento das contas de usuários visitantes;

13.1.34. A autenticação e autorização dos usuários visitantes deve ocorrer através de portal captivo acessível via browser web;

13.1.35. Os visitantes em hipótese alguma deverão ter acesso à Internet e rede interna antes que a autenticação seja concluída e o usuário seja autorizado;

13.1.36. A solução deve vincular o login do visitante à máquina utilizada no acesso;

13.1.37. Deve suportar a validação de credenciais:

13.1.37.1. Em base local interna à ferramenta;

13.1.37.2. Em servidores RADIUS;

13.1.37.3. Em servidores LDAP.

13.1.38. A solução deve autenticar usuários visitantes através das seguintes redes sociais: Facebook, LinkedIn e Twitter;

13.1.39. A ferramenta deve permitir que os usuários visitantes possam realizar auto-registro através do preenchimento de cadastro disponível em portal web;

13.1.40. Deve permitir a customização dos campos obrigatórios e opcionais para o cadastro de auto-registro;

13.1.41. A solução deve suportar o envio da senha de acesso aos visitantes através de SMS e e-mail;

13.1.42. Deve ser possível definir um período para que os usuários visitantes sejam obrigados a se reautenticar;

13.1.43. 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;

13.1.44. Os usuários do tipo sponsor poderão cadastrar previamente um usuário visitante. O portal de cadastro e gerenciamento de usuários visitantes não deve permitir gerência administrativa dos demais recursos da solução;

13.1.45. A solução deve permitir a customização da aparência do captive portal, permitindo editar textos e inserir imagens;
13.1.46. 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;
13.1.47. 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;
13.1.48. Deve permitir o uso de software agente instalado no dispositivo e agentes evanescentes que não precisam ser instalados;
13.1.49. 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;
13.1.50. Se um dispositivo não passar os testes de conformidade, deve ser possível:
13.1.50.1. Não forçar a remediação;
13.1.50.2. Forçar a remediação imediatamente enviando o dispositivo à rede de quarentena;
13.1.50.3. 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;
13.1.51. A solução deve permitir verificações de conformidade em endpoints que façam uso do sistema operacional:
13.1.51.1. Windows 7;
13.1.51.2. Windows 8;
13.1.51.3. Windows 10;
13.1.51.4. MacOS;
13.1.51.5. Linux.
13.1.52. 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:
13.1.52.1. Presença de software de anti-vírus instalado e em execução;
13.1.52.2. Versão do sistema operacional;
13.1.52.3. Nome de domínio do Active Directory ao qual a estação Windows pertença;
13.1.52.4. Serviços em execução para estações Windows;
13.1.52.5. Informações sobre um determinado certificado digital em estações Windows;
13.1.52.6. Registros ou chaves de registro para estações Windows;
13.1.52.7. Processos em execução para estações Windows, Linux e MacOS;
13.1.52.8. Arquivo armazenado em um determinado diretório para estações Windows, Linux e MacOS;
13.1.52.9. Pacotes instalados em estações Linux e MacOS.
13.1.53. 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;
13.1.54. Deve possuir serviço RADIUS interno, além de permitir o uso de RADIUS externos;
13.1.55. Deve permitir a distribuição de agentes através de, pelo menos, os seguintes métodos:
13.1.55.1. Programas de gerenciamento e distribuição de software;
13.1.55.2. GPO do Active Directory;
13.1.55.3. Captive Portal;

13.1.56. Deve permitir a atualização automática ou programada dos agentes instalados nas máquinas;

13.1.57. O agente instalado nos computadores deve notificar os usuários com mensagens informativas em casos de eventos;

13.1.58. Quando em quarentena, um portal web deve ser apresentado aos usuários com informações sobre as razões pelas quais estes foram movidos para o isolamento;

13.1.59. 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;

13.1.60. 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;

13.1.61. A solução deve integrar com plataformas de MDM, suportando pelo menos: FortiClient, In Tune, Mobile Iron e Air Watch;

13.1.62. Deve suportar integração com soluções de patching;

13.1.63. Deve suportar integração com soluções de análise de vulnerabilidades;

13.1.64. A solução deve possuir dashboard que apresente informações e estatísticas relevantes de forma resumida;

13.1.65. A solução deve permitir a customização do dashboard para apresentar as informações que o administrador considera relevante;

13.1.66. A solução deve permitir a consulta de informações e alteração de parâmetros de configuração via REST API;

13.1.67. A solução deve armazenar os eventos internamente e permitir que sejam exportados;

13.1.68. A solução deve permitir a exportação dos eventos através de syslog;

13.1.69. Deve suportar alta disponibilidade, suportando todos os registros e autenticações caso um nó da solução esteja indisponível;

13.1.70. 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;

13.1.71. Deve possuir registro dos eventos ocorridos na solução, bem como auditoria das configurações efetuadas;

13.1.72. Suportar integração com soluções de segurança de fabricantes como: Fortinet, Palo Alto, FireEye, etc, para correlacionar alertas de segurança e restringir, isolar ou bloquear dispositivos comprometidos que estejam conectados na rede, reduzindo assim o tempo de contenção de ameaças;

13.1.73. Suportar método genérico para integração de dispositivos, usando o recebimento, envio, análise e interpretação de mensagens do tipo syslog;

13.1.74. Deve possibilitar o rastreio de dispositivos, notificando a localização dos mesmos quando se conectarem à rede;

13.1.75. 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;

13.1.76. 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;

14. ITEM 18 – TREINAMENTO DAS SOLUÇÕES

14.1. CARACTERÍSTICAS GERAIS DOS TREINAMENTOS

14.1.1. Treinamento com material oficial das soluções fornecidas.

14.1.2. Deverá ser abordado conceitos teóricos e atividades práticas de laboratório;

14.1.3. Todos os treinamentos poderão ser realizados de forma híbrida (presencial ou remota), conforme necessidade da Defensoria ;

14.1.4. O idioma das aulas deverá ser em português;

14.1.5. Deverá ser entregue material didático composto de apostila em formato digital ou impresso. O material didático poderá ser em português ou inglês.

14.1.6. Ao final do treinamento deverá ser emitido certificado de conclusão a cada participante, devidamente assinado pela empresa promovente, especificando conteúdo programático completo do curso, corpo docente e carga horária.

14.1.7. O treinamento pode ser separado conforme o produto a ser instalado no ambiente da Contratante, contendo ao menos os seguintes módulos:

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

14.1.9. Resolução de problemas – troubleshooting;

14.1.10. Melhores práticas utilizadas no mercado para aproveitamento dos hardwares e softwares e suas funcionalidades.

14.1.11. O treinamento terá um total de cinco (5) participantes definidos pela Contratante;

14.1.12. O material didático fornecido deve abordar todos os tópicos do curso;

14.1.13. A CONTRATADA deverá fornecer apostilas em formato digital que incluam o conteúdo referente ao produto;

14.1.14. É de responsabilidade da contratante a disponibilização de instalações físicas para a realização do treinamento;

14.1.15. Após a conclusão, o serviço de treinamento deverá ser formalmente homologado pela Contratante, o qual possuirá o prazo de 5 (quinze) dias consecutivos contados a partir da data de conclusão do treinamento contratado, para emitir o relatório de homologação (aceite).

14.2. CARACTERÍSTICAS ESPECÍFICAS DO TREINAMENTO DA SOLUÇÃO DE FIREWALLS DE PRÓXIMA GERAÇÃO

14.2.1. Carga horária mínima de 36 (trinta e seis) horas;

14.2.2. Deverá ser abordado, no mínimo, os seguintes tópicos:

14.2.2.1. Configurações iniciais e avançadas;

14.2.2.2. Configurações de VLANs, LACP, DHCP e tipos de NAT;

14.2.2.3. Políticas de segurança;

14.2.2.4. Prevenção de ameaças, anti-malware, filtro URL e controle de aplicações;

14.2.2.5. Identificação de usuários, qualidade de serviço e regras por aplicação;

14.2.2.6. Filtro de dados;

14.2.2.7. VPN Site-to-Site e Client-To-Site;

14.2.2.8. ZTNA;

14.2.2.9. Análise de malwares modernos;

14.2.2.10. Alta disponibilidade;

14.2.2.11. Gerenciamento centralizado e relatórios;

14.2.2.12. Avaliação de boas práticas;
14.2.2.13. Otimização de políticas de firewall.

14.3. CARACTERÍSTICAS ESPECÍFICAS DO TREINAMENTO DA SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO
14.3.1. Carga horária mínima de 12 (doze) horas;
14.3.2. Deverá ser abordado, no mínimo, os seguintes tópicos:
14.3.2.1. Configurações iniciais e avançadas;
14.3.2.2. Instalação, gerenciamento e administração de dispositivos, políticas e objetos;
14.3.2.3. Configuração e administração de instâncias de virtualização;
14.3.2.4. Diagnóstico e resolução de problemas.

14.4. CARACTERÍSTICAS ESPECÍFICAS DO TREINAMENTO DA SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATORIA
14.4.1. Carga horária mínima de 12 (doze) horas;
14.4.2. Deverá ser abordado, no mínimo, os seguintes tópicos:
14.4.2.1. Configurações iniciais e avançadas;
14.4.2.2. Configuração, visualização e gerenciamento de logs;
14.4.2.3. Configuração, visualização e gerenciamento de relatórios;
14.4.2.4. Gerenciamento de eventos, incidentes e recursos de automação (playbooks);
14.4.2.5. Configuração e administração de instâncias de virtualização.

14.5. CARACTERÍSTICAS ESPECÍFICAS DO TREINAMENTO DE ADMINISTRAÇÃO DE SWITCHES E PONTOS DE ACESSO
14.5.1. Carga horária mínima de 24 (vinte e quatro) horas;
14.5.2. Deverá ser abordado, no mínimo, os seguintes tópicos:
14.5.2.1. Fundamentos básicos de switches e pontos de acesso;
14.5.2.2. Configurações iniciais e avançadas de switches e pontos de acesso;
14.5.2.3. Gerenciamento de controlador wireless;
14.5.2.4. Configuração de autenticação 802.1X, com VLANs dinâmicas;
14.5.2.5. Priorização de tráfego;
14.5.2.6. Monitoramento, diagnóstico e resolução de problemas.

14.6. CARACTERÍSTICAS ESPECÍFICAS DO TREINAMENTO DA SOLUÇÃO DE CONTROLE DE ACESSO A REDE (NAC)
14.6.1. Carga horária mínima de 16 (dezesseis) horas;
14.6.2. Deverá ser abordado, no mínimo, os seguintes tópicos:
14.6.2.1. Configurações iniciais e visibilidade de rede;
14.6.2.2. Identificação e Classificação de Dispositivos Não Autorizados;
14.6.2.3. Controle Baseado em Estado;
14.6.2.4. Políticas de Segurança;
14.6.2.5. Gerenciamento de convidados e de terceiros;
14.6.2.6. Integração de dispositivos de segurança e resposta automatizada;
14.6.2.7. Alta disponibilidade;
14.6.2.8. Monitoramento, diagnóstico e resolução de problemas.

15.6 ITEM 19 – SERVIÇO DE SUPORTE PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS, PRÓ-ATIVOS E RESPOSTAS À INCIDENTES:

15.6.1 A Contratada deverá prover garantia, suporte técnico, e atualização de versões das licenças fornecidas, pelo prazo de trinta meses, contados da data do recebimento definitivo dessas licenças;
15.6.1.1 Inclui todas as atualizações de versões, pequenas atualizações de release e reparos de defeitos (bug fixing patches);
15.6.1.2 Os serviços de suporte técnico aos produtos deverão incluir, dentre outros:
15.6.1.2.1 Orientações sobre uso, configuração e instalação do software ofertado;
15.6.1.2.2 Questões sobre compatibilidade e interoperabilidade do produto ofertado (hardware e software);
15.6.1.2.3 Interpretação da documentação do software ofertado;
15.6.1.2.4 Orientações para identificar a causa de uma falha de software;
15.6.1.2.5 Orientação para solução de problemas de "performance" e "tuning" das configurações do software ofertado;
15.6.1.2.6 Orientação quanto às melhores práticas para implementação do software adquirido;
15.6.1.2.7 Apoio na recuperação de ambientes em caso de panes ou perda de dados;
15.6.1.2.8 Apoio para execução de procedimentos de atualização para novas versões do software instalado;
15.6.1.3 A contratada deverá gerar relatório mensal, analítico e sintético, indicando todos os eventos relevantes ocorridos durante o período de execução do mesmo a ser entregue até o 5 (quinto) dia útil do mês subsequente.
15.6.1.4 Durante o período de garantia, suporte técnico e manutenção, a Contratada deverá atender às solicitações da DPE/PA, em qualquer horário, respeitando as condições e níveis de serviços especificados a seguir:
15.6.1.4.1 SEVERIDADE ALTA: Aplicado quando há indisponibilidade do ambiente tecnológico;
15.6.1.4.2 SEVERIDADE MÉDIA: Aplicado quando há falha no uso dos softwares, estando ainda disponíveis, porém apresentando problemas ou instabilidade;
15.6.1.4.3 SEVERIDADE BAIXA: Aplicado para instalação, configuração, manutenção preventivas, aplicações de atualização e esclarecimento técnico relativo ao uso das ferramentas.
15.6.1.5 Os prazos estabelecidos nos níveis de serviços serão contados a partir da abertura do chamado, o qual será classificado conforme as severidades especificadas no item anterior.
15.6.1.6 Os prazos máximos para o atendimento dos chamados obedecerão ao disposto na tabela a seguir, contados a partir da data e hora de abertura do chamado:

SEVERIDADE	ATENDIMENTO	SOLUÇÃO / PALEATIVO
ALTA	4 (QUATRO) HORAS	12 (DOZE) HORAS
MÉDIA	6 (SEIS) HORAS	24 (VINTE E QUATRO) HORAS

BAIXA	24 (VINTE E QUATRO) HORAS	48 (QUARENTA E OITO) HORAS
LOCAIS REMOTOS	96 (NOVENTA E SEIS) HORAS	120 (CENTO E VINTE) HORAS

15.6.1.1 Para os chamados severidade LOCAIS REMOTOS (paralisação TOTAL das funcionalidades elencadas nas especificações técnicas), o início do atendimento deverá ocorrer no máximo em 96 (noventa e seis) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 120 (centro e vinte) horas corridas a contar do início do atendimento.

15.6.1.2 Para os chamados de severidade ALTA (paralisação de pelo menos 1 (uma) das funcionalidades elencadas nas especificações técnicas), o início do atendimento deverá ocorrer no máximo em 4 (quatro) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 12 (doze) horas corridas a contar do início do atendimento.

15.6.1.3 Para os chamados severidade MÉDIA (degradação na performance, funcionamento ou serviço da solução), o início do atendimento deverá ocorrer no máximo em 6 (seis) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 24 (vinte e quatro) horas corridas a contar do início do atendimento.

15.6.1.4 Para os chamados severidade BAIXA (quando há comprometimento do desempenho), o início do atendimento deverá ocorrer no máximo em 24 (vinte e quatro) horas corridas, a contar da abertura do chamado e a solução deverá ocorrer em até 48 (quarenta e oito) horas corridas a contar do início do atendimento.

15.6.1.5 Para os chamados de qualquer severidade, a critério da DPE/PA, poderá ser agendado o melhor horário para atendimento.

15.6.1.6 O fechamento de qualquer chamado só poderá ocorrer mediante consulta prévia à DPE/PA quanto à efetiva solução do problema.

15.6.1.7 Qualquer chamado fechado, sem anuência da DPE/PA ou sem que o problema tenha sido resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas.

15.6.1.8 A Contratada manterá cadastro das pessoas indicadas pela DPE/PA que poderão efetuar abertura e autorizar o fechamento de chamados.

15.6.1.9 A Contratada deverá fornecer relatório de atendimento técnico, referente a cada chamado, contendo no mínimo as seguintes informações:

15.6.1.9.1 Data e hora da abertura do chamado;

15.6.1.9.2 Data e hora do início do atendimento;

15.6.1.9.3 Responsável pelo atendimento da solicitação;

15.6.1.9.4 Motivo da ocorrência (indicação do defeito);

15.6.1.9.5 Status do chamado (aberto, em tratamento, fechado etc.);

15.6.1.9.6 Data e hora do fechamento do chamado;

15.6.1.9.7 Solução adotada (resolução);

15.6.1.10 O atendimento de suporte para a solução deverá ser do tipo 8 x 5 (oito horas por dia, cinco dias por semana), e deverá ser realizado por profissionais especializados.

15.6.1.11 Não haverá limite para o número de chamados de suporte técnico.

15.6.1.12 Nos casos em que as manutenções necessitarem de paradas do ambiente, a CONTRATANTE deverá ser imediatamente notificada para que se proceda a aprovação da

manutenção, ou para que seja agendada nova data, a ser definida pelo CONTRATANTE, para execução das atividades de manutenção;

15.7 ITENS 20 E 24 – SERVIÇOS DE INSTALAÇÃO E CONFIGURAÇÃO DOS EQUIPAMENTOS

15.7.1 Caso ocorra alguma divergência entre as especificações técnicas constantes na tabela com aquelas lançadas no sistema eletrônico (Comprasnet), prevalecerá o constante neste instrumento;

15.7.2 O prazo de vigência da contratação é de 36 (trinta e seis), conforme vier a constar do(s) contrato(s) ou instrumento substituto (se for o caso).

15.7.3 Caberá à CONTRATADA a implantação da solução sob o acompanhamento da CONTRATANTE;

15.7.4 No que tange ao processo de implantação da solução, a CONTRATADA deve apresentar um cronograma para a implantação e seguir as atividades tomando como base o seguinte escopo do serviço:

15.7.4.1 Planejamento da instalação incluindo identificação de pré-requisitos;

15.7.4.2 Instalação e configuração do módulo de gerenciamento central;

15.7.4.3 Criar a senha de acesso com privilégio Administrativo para a Contratante.

15.7.4.4 Instalação e configuração dos hardwares e softwares;

15.7.4.5 Realizar customizações caso sejam solicitadas ou necessárias;

15.7.4.6 Realizar testes e apresentar os resultados que comprovem a correta e completa implantação da solução;

15.7.4.7 Realizar backup das configurações;

15.7.4.8 Documentar todas as configurações realizadas no ambiente.

15.7.4.9 Os serviços de instalação serão para os seguintes itens:

15.7.4.9.1 SERVIÇO DE INSTALAÇÃO DE FIREWALL TIPO 1

15.7.4.9.2 SERVIÇOS DE INSTALAÇÃO DE FIREWALL TIPOS 2,3 e 4

15.7.4.9.3 SERVIÇOS DE INSTALAÇÃO DE SWITCHES

15.7.4.9.4 SERVIÇOS DE INSTALAÇÃO DE APs

15.7.4.9.5 SERVIÇO DE INSTALAÇÃO DOS ITENS 5, 6 e 17.

15.7.5 Após a conclusão da instalação e implantação, a solução deverá ser formalmente homologada pela Contratante, o qual possuirá o prazo de 5 (cinco) dias consecutivos contados a partir da data de conclusão do serviço de instalação e configuração contratado, para emitir o relatório de homologação (aceite). O conteúdo do treinamento deve abordar os assuntos de natureza teórica e prática, abrangendo todos os módulos envolvidos na solução de segurança em seus aspectos mais relevantes;

15.7.6 A instalação e configuração, serviços opcionais, deverá ocorrer em até 15 (quinze) dias corridos, contados a partir da data de entrega da ordem de serviço. Para as unidades que optarem pelo saque do referido serviço, esse prazo deverá constar na cláusula da Minuta contratual.

15.7.7 Para as unidades que contratarem o serviço de “Instalação para Equipamentos na capital e em localidades com distância até 200 km da Capital ou superior a 200 km da Capital” a entrega efetiva está condicionada a conclusão da instalação e configuração dos equipamentos;

15.7.8 A CONTRATADA deverá cumprir com todas as exigências técnicas e funcionais relacionadas com a solução ofertada, que devem ser implantadas durante o período contratado, sem ônus para a CONTRATANTE;

15.7.9 O serviço de instalação consiste na acomodação física, incluindo patch cord e configuração lógica dos equipamentos;

15.7.10 Caberá à CONTRATADA a disponibilização de todos os recursos necessários, como hardware, software e recursos humanos necessários à execução dessa atividade;

15.7.11 O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção individual, bem como materiais complementares estritamente necessários à instalação ou à assistência técnica é de inteira responsabilidade da CONTRATADA e não deverá gerar ônus à CONTRATANTE;

15.7.12 No tocante a equipamentos, periféricos, acessórios, técnicos de instalação, técnicos de manutenção, translado, transporte, estada, embalagens, necessários à execução da instalação e assistência técnica deverão ser de responsabilidade da CONTRATADA e não deverão gerar qualquer ônus à CONTRATANTE;

15.7.13 No processo de instalação o Responsável Técnico da CONTRATADA deverá tomar todas as medidas necessárias visando garantir a perfeita execução do serviço (instalação e configuração).

RESULTADOS PRETENDIDOS

O Estudo Técnico Preliminar proposto tem o intuito de apresentar elementos que demonstrem que a solução a ser contratada será de grande relevância para que a DPE/PA desempenhe sua função institucional.

Além disso, o fornecimento e manutenção de um ambiente seguro e protegido, certificado, moderno e com serviços de alta disponibilidade, proporciona aos servidores virtuais maior estabilidade nas operações de tecnologia que sustentam a atuação desta casa, onde destacamos os seguintes objetivos pretendidos:

- Alta disponibilidade do ambiente de TIC;
- Manutenção e preservação dos investimentos já realizados em infraestrutura de TIC;
- Disponibilidade dos sistemas providos pela DPE/PA;
- Diminuição nos prazos de atendimento de incidentes, solução de problemas e execução de mudanças, associadas ao aumento da taxa de sucesso em tais processos;
- Viabilizar a proposição de projetos de TI mais modernos e versáteis, de modo que as demandas da área de negócio sejam atendidas com maior celeridade;
- Aumento da capacidade da infraestrutura de TI;
- Compatibilidade de integração de novos componentes;
- Maior governança, confiabilidade e escalabilidade aos serviços de TI providos pelo NTI;
- Garantia de maior retenção dos dados e conformidade com as legislações vigentes;
- Promoverá segurança de dados e informações, agregando valor à imagem institucional da Defensoria Pública do Estado do Pará.

DECLARAÇÃO DA VIABILIDADE OU NÃO DA CONTRATAÇÃO:

Diante de todo o exposto, com base nas informações levantadas e nas análises apresentadas no presente documento, a Equipe de Planejamento da Contratação declara a VIABILIDADE da contratação da solução de segurança da informação para infraestrutura de redes lan/wan pelo período de 36 meses.

Belém, 16 de abril de 2024.

Cesar Augusto Cavalcante Valente

Coordenadoria De Estratégia E Governança de TIC
DEFENSORIA PÚBLICA DO ESTADO DO PARÁ

ANEXO II

PREGÃO ELETRÔNICO Nº. 0XX/2024-DPE
PROCESSO/PROTOCOLO Nº. 2024/2096228
MODELO DE PROPOSTA

À DEFENSORIA PÚBLICA DO ESTADO DO PARÁ
Referência: PREGÃO ELETRÔNICO SRP Nº 0XX/2024- DPE/PA
Nesta
Prezados Senhores,

Registro de Preços para a Contratação de empresa para fornecimento de solução integrada, contemplando licença perpétua, instalação, implantação, treinamento, customização, manutenção e suporte dos módulos de Acompanhamento da Execução Orçamentária e Financeira (integrada ao SIAFE - Sistema Integrado de Administração Financeira para Estados), Orçamento de Obra, Gestão de Obra, Gestão de Diário Oficial e Serviços Variáveis, conforme condições e exigências constante, no Edital e seus Anexos, assumindo responsabilidade pela qualidade dos mesmos e, para esse fim fornecemos os seguintes dados:

A empresa _____, localizada na_____,
CNPJ: _____signatária desta proposta, apresenta-se como licitante a assumir o fornecimento do objeto da licitação em estrita conformidade com os documentos pertinentes. A signatária propõe-se a fornecer integralmente o objeto desta licitação, nos preços descritos abaixo:

ITEM	DESCRIÇÃO DO OBJETO	QTD. ESTIMADA	Valor Unitário
1	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01	2	
2	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02	10	
3	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 03	20	
4	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 04	30	
5	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 05	45	
6	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO (PACOTE 10 EQUIPAMENTOS)	10	
7	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATORIA (PACOTE 5G/LOG DIA)	5	
8	SWITCH CONCENTRADOR (CORE)	4	
9	SWITCH DE ACESSO 24 PORTAS POE - TIPO 01	16	
10	SWITCH DE ACESSO 24 PORTAS POE - TIPO 02	100	
11	SWITCH DE ACESSO 48 PORTAS POE - TIPO 01	16	
12	SWITCH DE ACESSO 48 PORTAS POE - TIPO 02	20	

13	SWITCH DE ACESSO 8 PORTAS POE	77	
14	PONTO DE ACESSO - TIPO 01	155	
15	PONTO DE ACESSO - TIPO 02	80	
16	TRANSCEIVER SFP+ 10GBASE-T	50	
17	TRANSCEIVER SFP+ 10GBASE-SR	50	
18	TRANSCEIVER SFP+ 10GBASE-LR	50	
19	CONTROLE DE ACESSO A REDE (NAC)	1	
20	SERVIÇOS DE TREINAMENTO DAS SOLUÇÕES (POR SOLUÇÃO)	14	
21	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (POR SOLUÇÃO)	36	
22	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPO 1	2	
23	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPOS 2, 3, 4 e 5	105	
24	SERVIÇOS DE INSTALAÇÃO DE SWITCHES	229	
25	SERVIÇOS DE INSTALAÇÃO DE APs	235	
26	SERVIÇO DE INSTALAÇÃO DOS ITENS 6, 7 e 19	16	

A apresentação da proposta implicará na plena aceitação e concordância, por parte da licitante, de todas as exigências, termos e condições estabelecidas no edital e seus anexos, em especial à descrição do item constante no Anexo I - Termo de Referência.

01. O prazo de validade da proposta deverá ser de, no mínimo 90 (noventa) dias contados da sua emissão.

02. Declaramos que nos valores estão inclusos todos os custos e despesas diretas e indiretas decorrentes do fornecimento dos produtos, tais como tributos, taxas, encargos, frete, transporte, remunerações, de acordo com as especificações, quantidades, condições de execução e faturamento.

Razão Social:
CNPJ:
Endereço completo:
Telefone:
Endereço Correio Eletrônico:
Domicílio bancário

Belém, XX de abril de 2024.

_____

Nome e Assinatura do Representante Legal

ANEXO III
MINUTA ATA DE REGISTRO DE PREÇOS Nº XX/2024
PREGÃO ELETRÔNICO Nº 90010/2022-DPE
PROCESSO/PROTOCOLO Nº. 2024/2096228

Aos _____ dias do mês de _____ do ano de dois mil e vinte e quatro, a **DEFENSORIA PÚBLICA DO ESTADO DO PARÁ**, criada pela Lei Complementar Estadual nº. 13/93 e reorganizada pela Lei Complementar Estadual 054/2006 de 07 de fevereiro de 2006 e Lei Complementar 091/2014 de 13 de janeiro de 2014, inscrita no CNPJ sob o nº. 34.639.526/0001-38, situada na Rua Padre Prudêncio nº. 154 em Belém/PA, por sua Defensora Pública Geral, **Dra. MÔNICA PALHETA FURTADO BELÉM**, brasileira, portador da Carteira de Identidade 0.000.000 SSP/PA, CPF/MF nº 000.000.000-00, residente e domiciliado nesta cidade, no uso de suas competências e nos termos da Lei nº 14.133, de 1º de abril de 2021, do Decreto nº 11.462, de 31 de março de 2023, regulamentada pelo o Decreto Estadual no 2.939, de 10 de março de 2023, Decreto Estadual no 2.940, de 10 de março de 2023, Decreto estadual Nº 3.371, de 29 de setembro de 2023, e suas posteriores alterações e demais normas legais aplicáveis, em face da classificação da proposta apresentada no PREGÃO ELETRÔNICO SRP – 0XX/2024 - DPE, RESOLVE registrar o(s) preço(s) ofertado pela(s) empresa(s) relacionada(s) de acordo com a classificação por ela(s) alcançada(s), conforme informações a seguir:

EMPRESA: ENDEREÇO: CNPJ: FONE/FAX: EMAIL: RESPONSÁVEL LEGAL: QUALIFICAÇÃO:

QUANTITATIVO TOTAL DA ATA SRP

ITEM	DESCRIÇÃO DO OBJETO	QTD. ESTIMADA	Valor Unitário
1	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01	2	
2	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02	10	
3	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 03	20	
4	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 04	30	
5	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 05	45	
6	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO (PACOTE 10 EQUIPAMENTOS)	10	
7	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATORIA (PACOTE 5G/LOG DIA)	5	
8	SWITCH CONCENTRADOR (CORE)	4	

9	SWITCH DE ACESSO 24 PORTAS POE - TIPO 01	16	
10	SWITCH DE ACESSO 24 PORTAS POE - TIPO 02	100	
11	SWITCH DE ACESSO 48 PORTAS POE - TIPO 01	16	
12	SWITCH DE ACESSO 48 PORTAS POE - TIPO 02	20	
13	SWITCH DE ACESSO 8 PORTAS POE	77	
14	PONTO DE ACESSO - TIPO 01	155	
15	PONTO DE ACESSO - TIPO 02	80	
16	TRANSCEIVER SFP+ 10GBASE-T	50	
17	TRANSCEIVER SFP+ 10GBASE-SR	50	
18	TRANSCEIVER SFP+ 10GBASE-LR	50	
19	CONTROLE DE ACESSO A REDE (NAC)	1	
20	SERVIÇOS DE TREINAMENTO DAS SOLUÇÕES (POR SOLUÇÃO)	14	
21	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (POR SOLUÇÃO)	36	
22	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPO 1	2	
23	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPOS 2, 3, 4 e 5	105	
24	SERVIÇOS DE INSTALAÇÃO DE SWITCHES	229	
25	SERVIÇOS DE INSTALAÇÃO DE APs	235	
26	SERVIÇO DE INSTALAÇÃO DOS ITENS 6, 7 e 19	16	

1. DO OBJETO

1.1. A presente Ata tem por objeto assegurar o compromisso de possível contratação entre a Defensoria Pública do Estado do Pará e a(s) empresa(s) vencedora(s) do certame licitatório referente PREGÃO ELETRÔNICO SRP – 0XX/2024 - DPE, cujo objeto é o Registro de Preços para futura Contratação de solução de cibersegurança e gestão de rede com fornecimento de equipamentos, licenças de softwares e serviços, para solução de proteção e gerenciamento seguro da rede LAN/WLAN/WAN da Defensoria Pública do Estado do Pará – DPE/PA, para garantir a segurança da informação fim a fim e que possibilite a visibilidade e controle de tráfego e aplicações, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, conforme especificações constantes no Termo de Referência.

2. ÓRGÃO(S) GERENCIADOR E PARTICIPANTE(S)

2.1. O órgão gerenciador será a DEFENSORIA PÚBLICA DO ESTADO DO PARÁ.

2.2. Além do gerenciador, São órgãos e entidades públicas participantes do registro de preços:

Item nº	Órgão Gerenciador e Participante UASG 925989 DEFENSORIA PÚBLICA DO ESTADO DO PARÁ	Cidade	Quantidade
1	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01	Belém/PA	2
2	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02	Belém/PA	10
3	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 03	Belém/PA	20
4	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 04	Belém/PA	30
5	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 05	Belém/PA	45
6	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO (PACOTE 10 EQUIPAMENTOS)	Belém/PA	10
7	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATORIA (PACOTE 5G/LOG DIA)	Belém/PA	5
8	SWITCH CONCENTRADOR (CORE)	Belém/PA	4
9	SWITCH DE ACESSO 24 PORTAS POE - TIPO 01	Belém/PA	16
10	SWITCH DE ACESSO 24 PORTAS POE - TIPO 02	Belém/PA	100
11	SWITCH DE ACESSO 48 PORTAS POE - TIPO 01	Belém/PA	16
12	SWITCH DE ACESSO 48 PORTAS POE - TIPO 02	Belém/PA	20
13	SWITCH DE ACESSO 8 PORTAS POE	Belém/PA	77
14	PONTO DE ACESSO - TIPO 01	Belém/PA	155
15	PONTO DE ACESSO - TIPO 02	Belém/PA	80
16	TRANSCEIVER SFP+ 10GBASE-T	Belém/PA	50
17	TRANSCEIVER SFP+ 10GBASE-SR	Belém/PA	50
18	TRANSCEIVER SFP+ 10GBASE-LR	Belém/PA	50
19	CONTROLE DE ACESSO A REDE (NAC)	Belém/PA	1
20	SERVIÇOS DE TREINAMENTO DAS SOLUÇÕES (POR SOLUÇÃO)	Belém/PA	14
21	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (POR SOLUÇÃO)	Belém/PA	36
22	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPO 1	Belém/PA	2
23	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPOS 2, 3, 4 e 5	Belém/PA	105
24	SERVIÇOS DE INSTALAÇÃO DE SWITCHES	Belém/PA	229
25	SERVIÇOS DE INSTALAÇÃO DE APs	Belém/PA	235
26	SERVIÇO DE INSTALAÇÃO DOS ITENS 6, 7 e 19	Belém/PA	16

Item nº	Órgão Participante: 93642 - DEFENSORIA PÚBLICA DO ESTADO DE RORAIMA	Cidade	Quantidade
2	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02	Boa Vista/RR	2

Item nº	Órgão Participante: 925853 - CORPO DE BOMBEIROS MILITAR DO PARÁ	Cidade	Quantidade
2	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02	Belém/PA	2
3	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 03	Belém/PA	2
6	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO (PACOTE 10 EQUIPAMENTOS)	Belém/PA	24
7	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATORIA (PACOTE 5G/LOG DIA)	Belém/PA	2
9	SWITCH DE ACESSO 24 PORTAS POE - TIPO 01	Belém/PA	90
14	PONTO DE ACESSO - TIPO 01	Belém/PA	140
20	SERVIÇOS DE TREINAMENTO DAS SOLUÇÕES (POR SOLUÇÃO)	Belém/PA	5
21	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (POR SOLUÇÃO)	Belém/PA	5
23	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPOS 2, 3, 4 e 5	Belém/PA	2
24	SERVIÇOS DE INSTALAÇÃO DE SWITCHES	Belém/PA	90
25	SERVIÇOS DE INSTALAÇÃO DE APs	Belém/PA	140
26	SERVIÇO DE INSTALAÇÃO DOS ITENS 6, 7 e 19	Belém/PA	2

Item nº	Órgão Participante: 928497 - SECRETARIA DE EST.DE C.T.E.S.P. E TECNOLOGIA DO ESTADO DO PARÁ	Unidade	Quantidade
2	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02	Belém/PA	2
5	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 05	Belém/PA	40
6	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO (PACOTE 10 EQUIPAMENTOS)	Belém/PA	5
7	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATORIA (PACOTE 5G/LOG DIA)	Belém/PA	2
9	SWITCH DE ACESSO 24 PORTAS POE - TIPO 01	Belém/PA	50
10	SWITCH DE ACESSO 24 PORTAS POE - TIPO 02	Belém/PA	50
11	SWITCH DE ACESSO 48 PORTAS POE - TIPO 01	Belém/PA	25
12	SWITCH DE ACESSO 48 PORTAS POE - TIPO 02	Belém/PA	25
14	PONTO DE ACESSO - TIPO 01	Belém/PA	24
16	TRANSCEIVER SFP+ 10GBASE-T	Belém/PA	250
17	TRANSCEIVER SFP+ 10GBASE-SR	Belém/PA	250
19	CONTROLE DE ACESSO A REDE (NAC)	Belém/PA	4
20	SERVIÇOS DE TREINAMENTO DAS SOLUÇÕES (POR SOLUÇÃO)	Belém/PA	5
21	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (POR SOLUÇÃO)	Belém/PA	5
23	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPOS 2, 3, 4 e 5	Belém/PA	42
24	SERVIÇOS DE INSTALAÇÃO DE SWITCHES	Belém/PA	200
25	SERVIÇOS DE INSTALAÇÃO DE APs	Belém/PA	24
26	SERVIÇO DE INSTALAÇÃO DOS ITENS 6, 7 e 19	Belém/PA	3

Item nº	Órgão Participante: 926931 - DEFENSORIA PÚBLICA DO ESTADO DE GOIÁS	Cidade	Quantidade
1	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01	Aparecida de Goiânia/GO 1 Goiânia/GO 2	3
3	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 03	Anápolis/GO 1 Goiânia/GO 5 Inhumas/GO 1 Luziânia/GO 1 Trindade/GO 1 Valparaiso de Goiás/GO 1	10
4	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 04	Goiânia/GO 4 Aparecida de Goiânia/GO 3 Trindade/GO 1 BRASÍLIA/DF 1	9
6	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO (PACOTE 10 EQUIPAMENTOS)	Goiânia/GO	3
7	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATORIA (PACOTE 5G/LOG DIA)	Goiânia/GO	3
8	SWITCH CONCENTRADOR (CORE)	Goiânia/GO 4 Aparecida de Goiânia/GO 2	6
14	PONTO DE ACESSO - TIPO 01	Anápolis/GO 8 Aparecida de Goiânia/GO 4 Goiânia/GO 82 Inhumas/GO 2 Luziânia/GO 12 Trindade/GO 4 Valparaiso de Goiás/GO 9	121
15	PONTO DE ACESSO - TIPO 02	Goiânia/GO	9
16	TRANSCEIVER SFP+ 10GBASE-T	Goiânia/GO	10
17	TRANSCEIVER SFP+ 10GBASE-SR	Goiânia/GO	96
18	TRANSCEIVER SFP+ 10GBASE-LR	Goiânia/GO	4
19	CONTROLE DE ACESSO A REDE (NAC)	Goiânia/GO	3
20	SERVIÇOS DE TREINAMENTO DAS SOLUÇÕES (POR	Goiânia/GO	5

	SOLUÇÃO)		
21	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (POR SOLUÇÃO)	Goiânia/GO	36
22	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPO 1	Goiânia/GO 2 Aparecida de Goiânia/GO 1	3
23	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPOS 2, 3, 4 e 5	Anápolis/GO 1 Aparecida de Goiânia/GO 3 BRASÍLIA/DF 1 Goiânia/GO 9 Inhumas/GO 1 Luziânia/GO 1 Trindade/GO 2 Valparaiso de Goiás/GO 1	19
24	SERVIÇOS DE INSTALAÇÃO DE SWITCHES	Goiânia/GO 4 Aparecida de Goiânia/GO 2	6
25	SERVIÇOS DE INSTALAÇÃO DE APs	Anápolis/GO 8 Aparecida de Goiânia/GO 4 Goiânia/GO 91 Inhumas/GO 2 Luziânia/GO 12 Trindade/GO 4 Valparaiso de Goiás/GO 9	130
26	SERVIÇO DE INSTALAÇÃO DOS ITENS 6, 7 e 19	Goiânia/GO	9

Item nº	Órgão Participante: 925801 - SECRETARIA DE ESTADO DE SEGURANÇA PÚBLICA DO ESTADO DO PARÁ	Cidade	Quantidade
2	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02	Belém/PA	2
3	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 03	Belém/PA	2
5	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 05	Belém/PA	30
6	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO (PACOTE 10 EQUIPAMENTOS)	Belém/PA	20
7	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATORIA (PACOTE 5G/LOG DIA)	Belém/PA	5
8	SWITCH CONCENTRADOR (CORE)	Belém/PA	2

9	SWITCH DE ACESSO 24 PORTAS POE - TIPO 01	Belém/PA	30
13	SWITCH DE ACESSO 8 PORTAS POE	Belém/PA	20
14	PONTO DE ACESSO - TIPO 01	Belém/PA	60
16	TRANSCEIVER SFP+ 10GBASE-T	Belém/PA	10
17	TRANSCEIVER SFP+ 10GBASE-SR	Belém/PA	10
18	TRANSCEIVER SFP+ 10GBASE-LR	Belém/PA	10
19	CONTROLE DE ACESSO A REDE (NAC)	Belém/PA	6
20	SERVIÇOS DE TREINAMENTO DAS SOLUÇÕES (POR SOLUÇÃO)	Belém/PA	5
21	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (POR SOLUÇÃO)	Belém/PA	3
23	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPOS 2, 3, 4 e 5	Belém/PA	4
24	SERVIÇOS DE INSTALAÇÃO DE SWITCHES	Belém/PA	50
25	SERVIÇOS DE INSTALAÇÃO DE APs	Belém/PA	60
26	SERVIÇO DE INSTALAÇÃO DOS ITENS 6, 7 e 19	Belém/PA	3

Item nº	Órgão Participante: 925402 - TRIBUNAL DE CONTAS DO ESTADO DE TOCANTINS	Cidade	Quantidade
1	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01	Palmas/TO	2
6	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO (PACOTE 10 EQUIPAMENTOS)	Palmas/TO	1
7	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATORIA (PACOTE 5G/LOG DIA)	Palmas/TO	2
20	SERVIÇOS DE TREINAMENTO DAS SOLUÇÕES (POR SOLUÇÃO)	Palmas/TO	3
22	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPO 1	Palmas/TO	2

3. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

3.1. 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:

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

3.1.2. 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

3.1.3. consulta e aceitação prévias do órgão ou da entidade gerenciadora e do fornecedor.

3.2. A autorização do órgão ou entidade gerenciadora apenas será realizada após a aceitação da adesão pelo fornecedor.

3.2.1. 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.

3.3. Após a autorização do órgão ou da entidade gerenciadora, o órgão ou entidade não participante deverá efetivar a aquisição ou a contratação solicitada em até noventa dias, observado o prazo de vigência da ata.

3.4. O prazo de que trata o subitem anterior, relativo à efetivação da contratação, poderá ser prorrogado excepcionalmente, mediante solicitação do órgão ou da entidade não participante aceita pelo órgão ou pela entidade gerenciadora, desde que respeitado o limite temporal de vigência da ata de registro de preços.

3.5. O órgão ou a entidade poderá aderir a item da ata de registro de preços da qual seja integrante, na qualidade de não participante, para aqueles itens para os quais não tenha quantitativo registrado, observados os requisitos do item 3.1.

Dos limites para as adesões

3.6. As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o gerenciador e para os participantes.

3.7. O quantitativo decorrente das adesões não poderá exceder, na totalidade, ao quíntuplo do quantitativo de cada item registrado na Ata de Registro de Preços (ARP) para o órgão ou entidade gerenciador(a) e os órgãos ou as entidades participantes, independentemente do número de órgãos ou entidades não participantes que a ela aderirem, nos termos do Decreto Estadual Nº 3.371, de 29 de setembro de 2023.

Vedação a acréscimo de quantitativos

3.8. É vedado efetuar acréscimos nos quantitativos fixados na ata de registro de preços.

4. VALIDADE, FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS E CADASTRO RESERVA

4.1. A validade da Ata de Registro de Preços será de 1 (um) ano, contado a partir do primeiro dia útil subsequente à data de divulgação no PNCP, podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso.

4.1.1. O contrato decorrente da ata de registro de preços terá sua vigência estabelecida no próprio instrumento contratual e observará no momento da contratação e a cada exercício financeiro a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro.

4.1.2. Na formalização do contrato ou do instrumento substituto deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.

4.2. A contratação com os fornecedores registrados na ata será formalizada pelo órgão ou pela entidade interessada por intermédio de instrumento contratual, emissão de nota de empenho de despesa, autorização de compra ou outro instrumento hábil, conforme o art. 95 da Lei nº 14.133, de 2021.

4.2.1. O instrumento contratual de que trata o item 4.2. deverá ser assinado no prazo de validade da ata de registro de preços.

4.3. Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o art. 124 da Lei nº 14.133, de 2021 e Decreto Estadual Nº 3.371, de 2023.

4.4. Após a homologação da licitação ou da contratação direta, deverão ser observadas as seguintes condições para formalização da ata de registro de preços:

4.4.1. Serão registrados na ata os preços e os quantitativos do adjudicatário, devendo ser observada a possibilidade de o licitante oferecer ou não proposta em quantitativo inferior ao máximo previsto *no edital* e se obrigar nos limites dela;

4.4.2. Será incluído na ata, na forma de anexo, o registro dos licitantes ou dos fornecedores que:

4.4.2.1. Aceitarem cotar os bens, as obras ou os serviços com preços iguais aos do adjudicatário, observada a classificação da licitação; e

4.4.2.2. Mantiverem sua proposta original.

4.4.3. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou dos fornecedores registrados na ata.

4.5. O registro a que se refere o item 4.4.2 tem por objetivo a formação de cadastro de reserva para o caso de impossibilidade de atendimento pelo signatário da ata.

4.6. Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem reduzir suas propostas para o preço do adjudicatário antecederão aqueles que mantiverem sua proposta original.

4.7. A habilitação dos licitantes que comporão o cadastro de reserva a que se refere o item 4.4.2.2 somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

4.7.1. Quando o licitante vencedor não assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital; e

4.7.2. Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas no item 8.

4.8. O preço registrado com indicação dos licitantes e fornecedores será divulgado no PNCP e ficará disponibilizado durante a vigência da ata de registro de preços.

4.9. A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no Sistema de Registro de Preços.

4.10. Quando o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital ou no aviso de contratação, e observado o disposto no item 4.7, observando o item 4.7 e subitens, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

4.11. Na hipótese de nenhum dos licitantes que trata o item 4.4.2.1, aceitar a contratação nos termos do item anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital, poderá:

4.11.1. Convocar para negociação os demais licitantes ou fornecedores remanescentes cujos preços foram registrados sem redução, observada a ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

4.11.2. Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes ou fornecedores remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

4.12. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.

5. ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS

5.1. Os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

5.1.1. Em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos da alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

5.1.2. Em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou a superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

5.1.3. Na hipótese de previsão no edital o de cláusula de reajustamento ou repactuação sobre os preços registrados, nos termos da Lei nº 14.133, de 2021.
5.1.4. No caso do reajustamento, deverá ser respeitada a contagem da anualidade e o índice previstos para a contratação;
No caso da repactuação, poderá ser a pedido do interessado, conforme critérios definidos para a contratação.

6. NEGOCIAÇÃO DE PREÇOS REGISTRADOS

6.1. Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão ou entidade gerenciadora convocará o fornecedor para negociar a redução do preço registrado.
6.1.1. Caso não aceite reduzir seu preço aos valores praticados pelo mercado, o fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas.
6.1.2. Na hipótese prevista no item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado e não convocará os licitantes ou fornecedores que tiveram seu registro cancelado.
6.1.3. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, adotando as medidas cabíveis para obtenção de contratação mais vantajosa.
6.1.4. Na hipótese de redução do preço registrado, o gerenciador comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços para que avaliem a conveniência e a oportunidade de diligenciarem negociação com vistas à alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.
6.2. Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao gerenciador a alteração do preço registrado, mediante comprovação de fato superveniente que supostamente o impossibilite de cumprir o compromisso.
6.2.1. Neste caso, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória ou a planilha de custos que demonstre a inviabilidade do preço registrado em relação às condições inicialmente pactuadas.
6.2.2. Na hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo órgão ou entidade gerenciadora e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, nos termos do item 8, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.
6.2.3. Na hipótese de cancelamento do registro do fornecedor, nos termos do item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados, observado o disposto no item 5.7.
6.2.4. Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, nos termos do item 8, e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa.
6.2.5. Na hipótese de comprovação da majoração do preço de mercado que inviabilize o preço registrado, conforme previsto no item 6 e no item 6.2.1, o órgão ou entidade gerenciadora atualizará o preço registrado, de acordo com a realidade dos valores praticados pelo mercado.

6.2.6. O órgão ou entidade gerenciadora comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços sobre a efetiva alteração do preço registrado, para que avaliem a necessidade de alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

7. REMANEJAMENTO DAS QUANTIDADES REGISTRADAS NA ATA DE REGISTRO DE PREÇOS

7.1. As quantidades previstas para os itens com preços registrados nas atas de registro de preços poderão ser remanejadas pelo órgão ou entidade gerenciadora entre os órgãos ou as entidades participantes e não participantes do registro de preços.

7.2. O remanejamento somente poderá ser feito:

7.2.1. De órgão ou entidade participante para órgão ou entidade participante; ou

7.2.2. De órgão ou entidade participante para órgão ou entidade não participante.

7.3. O órgão ou entidade gerenciadora que tiver estimado as quantidades que pretende contratar será considerado participante para efeito do remanejamento.

7.4. Na hipótese de remanejamento de órgão ou entidade participante para órgão ou entidade não participante, serão observados os limites previstos no art. 32 do Decreto Estadual nº 3.371, de 2023.

7.5. Competirá ao órgão ou à entidade gerenciadora autorizar o remanejamento solicitado, com a redução do quantitativo inicialmente informado pelo órgão ou pela entidade participante, desde que haja prévia anuência do órgão ou da entidade que sofrer redução dos quantitativos informados.

7.6. Caso o remanejamento seja feito entre órgãos ou entidades dos Estados, do Distrito Federal ou de Municípios distintos, caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente do remanejamento dos itens.

8. CANCELAMENTO DO REGISTRO DO LICITANTE VENCEDOR E DOS PREÇOS REGISTRADOS

8.1. O registro do fornecedor será cancelado pelo gerenciador, quando o fornecedor:

8.1.1. Descumprir as condições da ata de registro de preços, sem motivo justificado;

8.1.2. Não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração Pública Estadual sem justificativa razoável;

8.1.3. Não aceitar manter seu preço registrado, na hipótese prevista no artigo 27, § 2º, do Decreto nº 11.462, de 2023; ou

8.1.4. Sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021.

Na hipótese de aplicação de sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021, caso a penalidade aplicada ao fornecedor não ultrapasse o prazo de vigência da ata de registro de preços, poderá o órgão ou a entidade gerenciadora poderá, mediante decisão fundamentada, decidir pela manutenção do registro de preços, vedadas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

8.2. O cancelamento de registros nas hipóteses previstas no item 8.1 será formalizado por despacho do órgão ou da entidade gerenciadora, garantidos os princípios do contraditório e da ampla defesa.

8.3. Na hipótese de cancelamento do registro do fornecedor, o órgão ou a entidade gerenciadora poderá convocar os licitantes que compõem o cadastro de reserva, observada a ordem de classificação.

8.4. O cancelamento dos preços registrados poderá ser realizado pelo gerenciador, em determinada ata de registro de preços, total ou parcialmente, nas seguintes hipóteses, desde que devidamente comprovadas e justificadas:
8.4.1. Por razão de interesse público;
8.4.2. A pedido do fornecedor, decorrente de caso fortuito ou força maior; ou
8.4.3. Se não houver êxito nas negociações, nas hipóteses em que o preço de mercado tornar-se superior ou inferior ao preço registrado, nos termos do artigos 26, § 3º e 27, § 4º, ambos do Decreto Federal nº 11.462, de 2023 e artigo 22 do Decreto Estadual nº 3.371/2021.

9. DAS PENALIDADES

9.1. O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no edital ou no aviso de contratação direta.
9.1.1. As sanções também se aplicam aos integrantes do cadastro de reserva no registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente após terem assinado a ata.
9.2. É da competência do gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço (art. 7º, inc. XIV, do Decreto nº 11.462, de 2023), exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos ou entidade participante, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade (art. 8º, inc. IX, do Decreto nº 11.462, de 2023).
9.3. O órgão ou entidade participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no item 9.1, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.
9.4. CONDIÇÕES GERAIS
9.5. As condições gerais de execução do objeto, tais como os prazos para entrega e recebimento, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, ANEXO AO EDITAL.
9.6. No caso de adjudicação por preço global de grupo de itens, só será admitida a contratação de parte de itens do grupo se houver prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade.

10. DA VINCULAÇÃO

10.1. Integram esta Ata, o Edital do PREGÃO ELETRÔNICO SRP – 0XX/2024 - DPE e seus anexos, as propostas com os preços, o quadro com a ordem classificatória das empresas e preços apresentados no referido certame.

11. DOS CASOS OMISSOS

11.1. Os casos omissos serão resolvidos de acordo com a Lei Federal n.º 14.133/2021, Decreto Estadual Nº 3.371/2023 e alterações posteriores e demais normas aplicáveis.

A presente Ata, após lida e achada conforme, é assinada pelos representantes legais da Defensoria Pública do Estado do Pará e do Fornecedor Beneficiário.

Belém/PA, _____ de _____ de 2024.

_____
Defensoria Pública do Estado do Pará
MÔNICA PALHETA FURTADO BELÉM
Defensora Pública Geral

_____
-Razão Social da Empresa-
-Nome do Representante Legal-

TESTEMUNHAS:
1ª - NOME:
CPF:
2ª - NOME:
CPF:

ANEXO IV
MINUTA DE CONTRATO Nº XX/2024
PREGÃO ELETRÔNICO Nº 9010/2024-DPE
PROCESSO/PROTOCOLO Nº. 2024/2096228
ATA DE REGISTRO DE PREÇOS Nº 0XX/2024 – DPE

CONTRATO ADMINISTRATIVO Nº ...../...., QUE FAZEM ENTRE SI A DEFENSORIA PÚBLICA DO ESTADO DO PARÁ E A EMPRESA....., COMO MELHOR ABAIXO SE DECLARA.

Pelo presente instrumento de contrato, de um lado, a **DEFENSORIA PÚBLICA DO ESTADO DO PARÁ**, inscrita no CNPJ/MF sob o nº. 34.639.526/0001-38, estabelecida nesta cidade de Belém, Estado do Pará, na Rua Padre Prudêncio nº. 154, bairro Campina, doravante denominado CONTRATANTE, neste ato representada por sua Defensora Pública Geral, **Dra. MÔNICA PALHETA FURTADO BELÉM**, brasileira, portador da Carteira de Identidade 0.000.000 SSP/PA, CPF/MF nº 000.000.000-00, residente e domiciliado nesta cidade de Belém, e, de outro lado a empresa XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX , inscrita no CNPJ/MF sob o nº XXXXXXXXXXXXX, estabelecida no município de XXXXXXXXXXXX, Estado do XXXXXXXXXXXXX, a XXXXXXXXXXXX, Nº 0 0 0 0 0 0 , bairro XXXXXXXXX, daqui por diante designada CONTRATADA, neste ato representada pelo(a) Senhor(a) XXXXXXXXXXXXXXXXXXXXXXXXX, brasileiro, portador da Carteira de Identidade n.º XXXXXXXXX – SSP/XX e do CPF n.º XXXXXXXXXXXXXXX, residente e domiciliado na Rua _____,município de_____, Estado, conforme atos constitutivos da empresa **OU** procuração apresentada nos autos, tendo em vista o que consta no **Processo nº 2024/2096228** e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente **do Pregão Eletrônico nº 90010/2024,** mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – DO OBJETO:

1.1. O objeto do presente instrumento é a Contratação de solução de cibersegurança e gestão de rede com fornecimento de equipamentos, licenças de softwares e serviços, para solução de proteção e gerenciamento seguro da rede LAN/WLAN/WAN da Defensoria Pública do Estado do Pará – DPE/PA, para garantir a segurança da informação fim a fim e que possibilite a visibilidade e controle de tráfego e aplicações, prevenção contra ataques e ameaças avançadas e modernas, filtro de dados, VPN e controle granular de banda de rede, nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. O Edital da Licitação;

1.3.3. A Proposta do contratado;

1.3.4. Eventuais anexos dos documentos supracitados.

ITEM	DESCRIÇÃO DO OBJETO	QTD. ESTIMADA	Valor Unitário
1	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 01	2	
2	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 02	10	
3	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 03	20	
4	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 04	30	
5	FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) - TIPO 05	45	
6	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE CONFIGURAÇÃO (PACOTE 10 EQUIPAMENTOS)	10	
7	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DE LOGS E RELATORIA (PACOTE 5G/LOG DIA)	5	
8	SWITCH CONCENTRADOR (CORE)	4	
9	SWITCH DE ACESSO 24 PORTAS POE - TIPO 01	16	
10	SWITCH DE ACESSO 24 PORTAS POE - TIPO 02	100	
11	SWITCH DE ACESSO 48 PORTAS POE - TIPO 01	16	
12	SWITCH DE ACESSO 48 PORTAS POE - TIPO 02	20	
13	SWITCH DE ACESSO 8 PORTAS POE	77	
14	PONTO DE ACESSO - TIPO 01	155	
15	PONTO DE ACESSO - TIPO 02	80	
16	TRANSCEIVER SFP+ 10GBASE-T	50	
17	TRANSCEIVER SFP+ 10GBASE-SR	50	
18	TRANSCEIVER SFP+ 10GBASE-LR	50	
19	CONTROLE DE ACESSO A REDE (NAC)	1	
20	SERVIÇOS DE TREINAMENTO DAS SOLUÇÕES (POR SOLUÇÃO)	14	
21	SERVIÇO DE SUPORTE MENSAL PARA 36 MESES PARA CHAMADOS PREVENTIVOS, CORRETIVOS E PRÓ-ATIVOS (POR SOLUÇÃO)	36	
22	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPO 1	2	
23	SERVIÇOS DE INSTALAÇÃO FIREWALL TIPOS 2, 3, 4 e 5	105	
24	SERVIÇOS DE INSTALAÇÃO DE SWITCHES	229	
25	SERVIÇOS DE INSTALAÇÃO DE APs	235	

26	SERVIÇO DE INSTALAÇÃO DOS ITENS 6, 7 e 19	16	

CLÁUSULA SEGUNDA – DA VIGÊNCIA E DA PRORROGAÇÃO:

2.1. O prazo de vigência da contratação é de 36 (trinta e seis) meses. contados da data de sua assinatura, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

2.1.1. A prorrogação de que trata esse item é condicionada à avaliação, por parte do Gestor do Contrato, da vantajosidade da prorrogação, a qual deverá ser realizada motivadamente, com base no Histórico de Gestão do Contrato, nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação, e nos demais aspectos que forem julgados relevantes.

2.1.2. O contratado não tem direito subjetivo à prorrogação contratual.

2.1.3. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.1.4. Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

3. CLÁUSULA TERCEIRA – DOS MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS:

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

CLÁUSULA QUARTA – DA SUBCONTRATAÇÃO:

4.1. Não será admitida a subcontratação do objeto contratual.

CLÁUSULA QUINTA – DO PREÇO:

5.1. O valor total da contratação é de R$..... (.....)

5.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

5.3. O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos.

CLÁUSULA SEXTA – DO PAGAMENTO:

6.1. O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

CLÁUSULA SÉTIMA – DO REAJUSTE:

7.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em __/__/__ *(DD/MM/AAAA)*.

7.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

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

7.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).
7.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).
7.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.
7.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.
7.8. O reajuste será realizado por apostilamento.

CLÁUSULA OITAVA – DAS OBRIGAÇÕES DA CONTRATANTE:
8.1. São obrigações do Contratante, além das previstas no termo de referência:
8.2. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;
8.3. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;
8.4. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;
8.5. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;
8.6. Comunicar a empresa para emissão de Nota Fiscal no que pertinente à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021;
8.7. Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;
8.8. Aplicar ao Contratado as sanções previstas na lei e neste Contrato;
8.9. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;
8.10. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.
8.11. A Administração terá o prazo de *XXXXXXX*, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.
8.12. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de XXXXXX.
8.13. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.
8.14. Comunicar o Contratado na hipótese de posterior alteração do projeto pelo Contratante, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.
8.15. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

CLÁUSULA NONA – DAS OBRIGAÇÕES DO CONTRATADO:

9.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas, além das previstas no termo de referência:

9.2. Manter preposto aceito pela Administração no local ou do serviço para representá-lo na execução do contrato.

9.3. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

9.4. Aceitar, nas mesmas condições contratuais, os percentuais de acréscimos ou supressões limitados ao estabelecido no art. 125, da Lei Federal nº 14.133/21, tomando-se por base o valor contratual.

9.5. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

9.6. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II) e prestar todo esclarecimento ou informação por eles solicitados;

9.7. Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência;

9.8. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados;

9.9. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos;

9.10. Responsabilizar-se integralmente pela observância do dispositivo no título II, capítulo V, da CLT, e na Portaria n.º 3.460/77, do Ministério do Trabalho, relativos à segurança e higiene do trabalho, bem como a Legislação correlata em vigor a ser exigida.

9.11. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021;

9.12. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

9.13. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante;
9.14. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.
9.15. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.
9.16. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.
9.17. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.
9.18. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.
9.19. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.
9.20. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre;
9.21. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação;
9.22. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116);
9.23. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único);
9.24. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;
9.25. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021;
9.26. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante;

CLÁUSULA DÉCIMA – DAS OBRIGAÇÕES PERTINENTES À LGPD:

10.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.
10.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.
10.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.
10.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.
10.5. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.
10.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.
10.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.
10.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.
10.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.
10.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.
10.11. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.
10.12. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.
10.13. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

CLÁUSULA DÉCIMA PRIMEIRA – DA GARANTIA DE EXECUÇÃO:
11.1. Não haverá exigência de garantia contratual da execução.

CLÁUSULA DÉCIMA SEGUNDA – DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS:
12.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que:
a) der causa à inexecução parcial do contrato;
b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
f) praticar ato fraudulento na execução do contrato;
g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

12.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

i) **Advertência**, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

ii) **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas "b", "c" e "d" do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

iii) **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas "e", "f", "g" e "h" do subitem acima deste Contrato, bem como nas alíneas "b", "c" e "d", que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

iv) **Multa:**

(1) Moratória de 1,0 % (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

(2) Compensatória, para as infrações descritas nas alíneas "e" a "h" do subitem 12.1, de 20% a 30% do valor do Contrato.

(3) Compensatória, para a inexecução total do contrato prevista na alínea "c" do subitem 12.1, de 10,0% a 15% do valor do Contrato.

(4) Para infração descrita na alínea "b" do subitem 12.1, a multa será de 5,0% a 10% do valor do Contrato.

(5) Para infrações descritas na alínea "d" do subitem 12.1, a multa será de 1,0% a 30% do valor do Contrato.

(6) Para a infração descrita na alínea "a" do subitem 12.1, a multa será de 1,0% a 10% do valor do Contrato.

12.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021)

12.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

12.5. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021)

12.6. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

12.7. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

12.8. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no **caput** e parágrafos do

art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

12.9. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para o Contratante;

e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

12.10. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

12.11. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021);

12.12. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021)

12.13. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

12.14. Os débitos do contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

CLÁUSULA DÉCIMA TERCEIRA – DA EXTINÇÃO CONTRATUAL:

13.1. O contrato será extinto quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto.

13.2. Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que deverá a Administração providenciar a readequação do cronograma fixado para o contrato.

13.3. Quando a não conclusão do contrato referida no item anterior decorrer de culpa do contratado:

a) ficará ele constituído em mora, sendo-lhe aplicáveis as respectivas sanções administrativas; e

b) poderá a Administração optar pela extinção do contrato e, nesse caso, adotará as medidas admitidas em lei para a continuidade da execução contratual.

13.4. O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.
13.4.1. Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.
13.4.2. A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.
13.4.3. Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.
13.5. O termo de extinção, sempre que possível, será precedido:
13.5.1. Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;
13.5.2. Relação dos pagamentos já efetuados e ainda devidos;
13.5.3. Indenizações e multas.
13.6. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, *caput*, da Lei n.º 14.133, de 2021).
13.7. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

CLÁUSULA DÉCIMA QUARTA – DA DOTAÇÃO ORÇAMENTÁRIA:
14.1. As despesas decorrentes do presente instrumento correrão à conta da Dotação Orçamentária da CONTRATANTE vigente para o exercício de 2024, de acordo com a classificação a seguir:
Programa / Projeto /Atividade:
Fonte de Recursos:
Elemento:
Gp Pará:
14.2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS:
15.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SEXTA – DAS ALTERAÇÕES:
15.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.
15.2. O contratado é obrigado a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.
15.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria jurídica do contratante, salvo nos casos de justificada

necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês (art. 132 da Lei nº 14.133, de 2021).

15.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

CLÁUSULA DÉCIMA SÉTIMA – DA FISCALIZAÇÃO:

16.1. A execução das obrigações contratuais integrantes deste Contrato será acompanhada e fiscalizada pelo servidor XXXXXXXXXXXX, matricula n.º XXXXXXXXX e Suplente o Servidor **XXXXXXXXX**, matricula n.º XXXXXXXX, CONTRATANTE, com autoridade para exercer, como representante da Administração, toda e qualquer ação de orientação geral, com fins de atender o que determina os arts. 7 e 117 da Lei nº 14.133/2021.

CLÁUSULA DÉCIMA OITAVA – DA PUBLICAÇÃO:

17.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, *caput,* da Lei n.º 14.133, de 2021, e no Diário Oficial do Estado do Pará, no prazo de 10 (dez) dias a contar de sua assinatura, conforme a previsão da Constituição do Estado do Pará.

CLÁUSULA DÉCIMA NONA – DO FORO:

17.2. Fica eleito o Foro da Justiça Federal em , Seção Judiciária de ..... para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

E, por estarem de acordo, as partes assinam o presente instrumento, em 03 (três) vias de igual teor e forma, na presença das testemunhas abaixo.

Belém/PA, XX de XXXXXXXX de 2024.

Assinado Eletronicamente
MÔNICA PALHETA FURTADO BELÉM
DEFENSORIA PÚBLICA DO ESTADO DO PARÁ
CONTRATANTE

_____
CONTRATADA

Testemunhas:

1 - _____ 2 - _____

Nome e CPF: _____ Nome e CPF: _____

ASSINATURAS

Número do Protocolo: 2024/2096228

Anexo/Sequencial: 37

Este documento foi assinado eletronicamente na forma do Art. 6º do Decreto Estadual Nº 2.176, de 12/09/2018.

Assinatura(s) do Documento:

Assinado eletronicamente por: Monica Palheta Furtado Belem, **CPF:** ***.800.212-**

Em: 20/09/2024 12:41:38

Aut. Assinatura: 9f0e47cc725d53d1a26c35773536ba908719665553278e512ffe0a74b78afdbb

Identificador de autenticação: 38f03594-9fe2-4742-93a6-febfa1d7b771

Confira a autenticidade deste documento em https://www.sistemas.pa.gov.br/validacao-protocolo