Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP:60.130-240 - Fortaleza/CE
Fone: (85) 3108-0000
www.etice.ce.gov.br

Chamada de Oportunidade de Serviços de Nuvem Pública Nº. 011/2024 – Solução de wi-fi seguro, aderente ao Edital de Pré-qualificação Permanente de Serviços em Nuvem Nº 001/2019 - ETICE

Setembro/2024

Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP:60.130-240 - Fortaleza/CE
Fone: (85) 3108-0000
www.etice.ce.gov.br

1. OBJETO

Chamada de oportunidade para prestação de serviços compreendendo o provimento de recursos em nuvem, para eventuais e futuras contratações de serviços de oferta, sob demanda, de solução de wi-fi seguro.

2. OBJETIVOS

Contribuindo com o aprimoramento tecnológico dos entes da Administração Pública do Estado do Ceará e reforçando sua missão de ser referência nacional como empresa de Tecnologia da Informação e Comunicação – TIC, indutora da inovação e modernização para o desenvolvimento econômico-social no fornecimento de serviços de tecnologia de alta performance em nuvem, a **ETICE** deseja selecionar, dentre as empresas pré-qualificadas, **serviços técnicos especializados para provimento de solução em nuvem**, conforme detalhamento técnico constante neste documento.

Assim, considerando as premissas estabelecidas no Edital de Pré-qualificação 001/2019, a Empresa de Tecnologia da Informação do Ceará – ETICE convoca as empresas pré-qualificadas para que apresentem propostas para **fornecimento dos serviços em nuvem, seguindo as definições técnicas deste documento convocatório.**

Todos os recursos e serviços necessários deverão ser lançados na proposta na modalidade OPEX.

Outrossim, vale destacar que os itens de serviços vencedores de cada chamada de oportunidade já serão trazidos para a composição do Marketplace da ETICE, devendo o(s) contrato(s) serem realizados por demanda; ou seja, SEM comprometimento do Orçamento da ETICE, podendo haver a contratação parcelada do objeto da presente chamada de Oportunidade; tudo consoante ao disposto nos itens 13.11, 17.1.1, 17.1.2 e 17.1.3 do Edital de Pré-qualificação, *in verbis*:

> "13.11. **Os itens de serviços vencedores de cada chamada de oportunidade serão trazidos para a composição dos serviços do *marketplace* da Etice**, devendo seus preços finais serem mantidos como máximos por um prazo mínimo de 12 (doze) meses a contar da data da homologação do resultado da chamada de oportunidade.
>
> (...)
>
> 17.1.1. Consoante o disposto no art. 140, parágrafos 4º e 5º do Regulamento de Licitações e Contratos da Etice, **fica desde já a ETICE autorizada a celebração de contratos por demanda.**
>
> 17.1.2. A ETICE fixará um quantitativo ou valor máximo de fornecimento ou serviço a ser utilizado no prazo de vigência do referido contrato, **SEM comprometimento do Orçamento da Etice.**
>
> 17.1.2. Na hipótese do item anterior, a ETICE **demandará o objeto de forma PARCELADA e apenas quando necessitar, nos termos e prazos definidos no Edital e contrato**, remunerando o contratado apenas pelo que for efetivamente executado." *(grifou-se)*

Este documento descreve as **características funcionais, premissas técnicas e de serviços** que deverão ser consideradas pelas pré-qualificadas, para que, munidos de informações relevantes sobre as necessidades para atendimento ao escopo dos serviços, emitam propostas de acordo com as condições preestabelecidas no Edital de Pré-qualificação supracitado.

3. SOBRE O MODELO DE CONTRATAÇÃO

3.1. Esta chamada de oportunidade obedecerá ao disposto no **Edital de pré-qualificação de nuvem nº 001/2019 da ETICE e seus anexo**s, nos **Termos de Pré-Qualificação** e no **Regulamento de Licitações e Contratos da ETICE**; sendo regido, também, pela **Lei Federal 13.303/2016**, pelos **Princípios do Direito Civil** e, no que couber, pelos **Princípios da Administração Pública** e demais legislações correlatas.

3.2. A chamada será feita em lote único visto que os itens desta chamada são intrinsecamente interconectados o que impossibilitaria sua divisão.

3.3. Justificativa Lote Único

3.3.1. A decisão pela adoção de lote único para a contratação de serviços de Wi-Fi seguro em nuvem está fundamentada em critérios de economicidade, eficiência, uniformidade na prestação dos serviços e otimização de gestão contratual, conforme preconiza a Lei 13.303/2016, que rege as contratações das empresas estatais.

3.3.2. Uniformidade e Compatibilidade Técnica

3.3.2.1. A prestação de serviços de Wi-Fi seguro em nuvem requer uma infraestrutura integrada que garanta a compatibilidade técnica e a interoperabilidade de todos os componentes do sistema.

3.3.2.2. A divisão em múltiplos lotes poderia resultar na contratação de fornecedores diferentes para partes distintas do serviço, comprometendo a uniformidade e a integridade da solução. Isso pode gerar problemas de integração entre sistemas, gerando possíveis vulnerabilidades de segurança e falhas na comunicação.

3.3.3. Gestão Centralizada e Facilidade de Administração

3.3.3.1. Ao optar por um lote único, a administração pública facilita o gerenciamento contratual e operacional, reduzindo a complexidade na coordenação de múltiplos contratos. A gestão centralizada permite maior controle sobre os níveis de serviço (SLAs), maior rapidez na resolução de problemas e maior clareza na definição de responsabilidades, o que seria dificultado na presença de diversos fornecedores. Além disso, uma única empresa responsável pela prestação do serviço garante uma abordagem unificada de suporte técnico e manutenção.

3.3.4. Economia de Escala e Maior Competitividade

3.3.4.1. A contratação em lote único possibilita a obtenção de economia de escala, uma vez que o volume agregado de serviços permite aos fornecedores reduzirem custos unitários e oferecerem preços mais competitivos. A divisão em múltiplos lotes poderia elevar os custos totais do serviço, uma vez que fornecedores precisariam considerar custos adicionais de integração e coordenação, que não seriam necessários em um único lote.

3.3.5. Segurança e Confiabilidade

3.3.5.1. A segurança da informação é um fator crítico para serviços de Wi-Fi seguro em nuvem, que envolve o tráfego de dados sensíveis e o acesso à rede interna de órgãos públicos. A contratação em lote único minimiza os riscos associados à fragmentação

da segurança da informação, pois assegura que um único fornecedor siga um padrão único e consistente de segurança em toda a rede. A fragmentação de responsabilidades poderia acarretar falhas na política de segurança da informação e inconsistências na aplicação de soluções de proteção.

3.3.6. A Lei 13.303/2016, que estabelece o estatuto jurídico das empresas estatais, permite a adoção de lote único quando houver justificativa técnica e econômica que aponte vantagens para o interesse público. Neste caso, a decisão por um lote único se alinha com os princípios da eficiência, economicidade e continuidade do serviço público, uma vez que garante uma solução de conectividade robusta, segura, integrada e com melhor custo-benefício.

3.3.7. Diante do exposto, a escolha pelo lote único se mostra justificada e alinhada aos princípios legais e de gestão eficiente, proporcionando uma contratação mais segura, econômica e eficaz para a prestação de serviços de Wi-Fi seguro em nuvem.

4. CRITÉRIO DE JULGAMENTO

4.1. Menor Preço

5. ORIENTAÇÕES GERAIS

5.1. Prazos

Número do Evento	Evento	Prazo limite
1	Recebimento de propostas das empresas pré-qualificadas pela ETICE	Até 15 (quinze) dias úteis (*)
2	Pedidos de Esclarecimentos	**Até às 17h00** do 3º (terceiro) dia útil que antecede o prazo de entrega das propostas.
3	Resposta aos Pedidos de Esclarecimentos	Até 2 (dois) dias úteis, a contar do término do prazo de pedidos de esclarecimentos (**).
4	Pedidos de Impugnação	**Até às 17h00** do 3º (terceiro) dia útil que antecede o prazo de entrega das propostas.
5	Respostas à Impugnação Interposta	Até 2 (dois) dias úteis, a contar do término do prazo de pedidos de esclarecimento.
6	Avaliação, Negociação e definição da proposta vencedora pela ETICE	Até 5 (cinco) dias úteis, contados a partir do término do prazo de apresentação de propostas.
7	Interposição de Recurso	Até 5 (cinco) dias úteis, contados a partir da divulgação da proposta vencedora.

8	Apresentação de Contrarrazões ao Recurso	Até 5 (cinco) dias úteis, contados a partir do término do prazo de interposição de recurso.
9	Decisão **definitiva** da Comissão	Até 5 (cinco) dias úteis, contados a partir do término do prazo de apresentação de contrarrazões recursais, podendo variar em razão da complexidade da matéria. (***)
10	Homologação e Adjudicação	Até 5 (cinco) dias úteis, a contar da divulgação da decisão definitiva da Comissão.

(*) O prazo será contado a partir do primeiro dia útil seguinte à publicação deste documento no website da ETICE, no link https://www.etice.ce.gov.br/projeto/pre-qualificacao- permanente/.
(**) O prazo poderá ser alterado conforme disposto no item 6.4.
(***) Caso haja desistência expressa do Prazo Recursal (e consequente Contrarrazões), o Prazo para apresentação da Decisão Definitiva poderá ser reduzido conforme o caso.

5.1.1. Os Prazos dispostos no item acima poderão variar em conformidade com o caso concreto, **podendo inclusive serem mitigados**, em razão de não apresentação de recursos ou mesmo que as empresas Pré-qualificadas declinem, formalmente, do direito Recursal (e consequentemente das contrarrazões).

5.2. Sobre o envio da Proposta Técnica.

5.2.1. **A proposta deverá ser enviada de forma eletrônica e deverá ser CRIPTOGRAFADA utilizando uma chave privada (senha).**

5.2.2. A proponente é responsável por gerar uma chave aleatória e manter completo sigilo desta chave, sem revelá-la a terceiros, nem à Etice, até que se tenha passado o período de recebimento de propostas estabelecido na tabela do item 5.1.

5.2.3. Antes ou após criptografada, **a proposta deve ser assinada digitalmente**, conforme o modelo da Medida Provisória 2.200-2/2001.

5.2.4. Com o objetivo de facilitar a submissão de propostas e considerando que vários softwares possibilitam a assinatura digital de um documento antes de uma encriptação e não após ela, a ETICE aceitará também propostas que tenham sido assinadas digitalmente antes de terem sido encriptadas contanto que o nome do arquivo de proposta possibilite a identificação clara do proponente.

5.2.5. A proposta criptografada e assinada deve ser enviada para o e-mail avaliacao.nuvem@etice.ce.gov.br. **O HORÁRIO DE RECEBIMENTO DAS PROPOSTAS SERÁ ATÉ ÀS 17H (DEZESSETE HORAS) DO ÚLTIMO DIA ÚTIL PARA RECEBIMENTO DAS PROPOSTAS.**

5.2.6. Uma proposta só será considerada **entregue no prazo** caso a ETICE responda com um

e-mail para o proponente reconhecendo o recebimento dentro do prazo.

5.2.7. **Proposta enviada para e-mail não correto ou com erro de escrita ou que tenha sido recusada pelo servidor não será considerada entregue no prazo.**

5.2.8. A proponente deverá enviar a chave criptográfica usada para encriptar a proposta para a ETICE em até 01 (um) dia útil após encerrado o prazo de recebimento de propostas.

5.2.9. **Arquivos corrompidos ou chaves que não permitam descriptografar a proposta, tornarão a proposta nula.**

5.2.10. **Todos os recursos e serviços necessários deverão ser lançados nas propostas em modalidade OPEX e em moeda nacional (reais).**

5.2.11. Na proposta deverá constar as cotações de todos os itens de serviços especificados neste documento, expressas em reais e em valores mensais e anuais.

5.2.12. Para fins de elaboração de Proposta, as empresas participantes deverão considerar que **o prazo contratual será de 12 (doze) meses**, prorrogável na forma da lei.

5.2.13. A ETICE descriptografará todas as propostas válidas e ordenará tais propostas baseadas em seu valor global.

5.3. Processo de Seleção e Negociação

5.3.1. **A seleção e negociação da melhor proposta ocorrerá preferencialmente se existirem, no mínimo, 3 (três) propostas válidas para a chamada.**

5.3.2. Será considerada válida a proposta que atender aos requisitos elencados no item 5.2.

5.3.3. **Caso sejam apresentadas apenas 02 (duas) propostas válidas na chamada de oportunidade, para homologação do resultado da chamada, poderá ser realizada pesquisa de mercado para validação dos preços apresentados pelas PRÉ-QUALIFICADAS participantes da chamada, sendo vedada a contratação de empresa que não seja pré-qualificada. No caso de ser apresentada apenas 01 (uma) proposta, a Chamada será considerada fracassada.**

5.3.4. O processo de seleção e negociação respeitará as regras do edital de pré-qualificação e da presenta chamada com base na proposta mais vantajosa para a ETICE, de forma a não comprometer a economicidade.

5.3.5. **Será declarada vencedora a proposta que apresentar o menor preço.**

5.3.6. **Será Desclassificada a Proposta vencedora que:**

5.3.6.1. Contenham vícios insanáveis;

5.3.6.2. Descumpram especificações técnicas constantes desta Chamada de Oportunidade;

5.3.6.3. Apresentem preços cujo valor do item e/ou valor total seja superior ao valor estimado após a negociação para contratação, de acordo com § 1o Art. 57 da Lei nº 13.303.

5.3.6.3.1. Para declaração de sobrepreço a proposta vencedora necessariamente deve passar por negociação nos critérios do item 5.3.7, mantendo-se o segredo da estimativa.

5.3.6.3.2. A negociação deverá abordar a integralidade da proposta, não sendo restrita

aos itens específicos que apresentem sobrepreço.

5.3.6.3.3. A desclassificação será mantida caso, mesmo após o processo de negociação, os preços continuem superiores ao estimado.

5.3.6.4. Apresentem preços manifestamente inexequíveis;

5.3.6.4.1. Será considerada inexequível as propostas:

5.3.6.4.1.1. Cujo valor total seja igual ou inferior a 50% abaixo do valor estimado para contratação.

5.3.6.4.1.2. Cujo valor do item da proposta seja igual ou inferior a 50% abaixo do valor estimado para aquele item.

5.3.6.4.1.3. Para declaração de inexequibilidade a proposta vencedora necessariamente deve passar pelo processo de diligência, sendo mantida a desclassificação caso não seja demonstrada a sua viabilidade técnica/operacional.

5.3.6.5. Não tenham sua exequibilidade demonstrada, quando exigido pela ETICE;

5.3.6.5.1. A Etice comprovará a exequibilidade das propostas por meio dos itens abaixo:

5.3.6.5.1.1. Nota fiscais, faturas, relatórios e medições de serviços semelhantes prestados, atestados técnicos, contratos, dentre outros.

5.3.6.6. Apresentem desconformidade com outras exigências do instrumento convocatório, salvo se for possível a acomodação a seus termos antes da adjudicação do objeto e sem que se prejudique a atribuição de tratamento isonômico entre as licitantes;

5.3.6.7. A ETICE poderá realizar diligências para aferir a exequibilidade das propostas ou exigir das licitantes que ela seja demonstrada;

5.3.6.8. A desclassificação será sempre fundamentada.

5.3.7. A negociação com a empresa declarada vencedora será feita após a sua classificação, por meio de apresentação de nova proposta com descontos percentuais que esta possa oferecer.

5.3.7.1. Será mantido o caráter sigiloso da estimativa de preço, sendo este divulgado em concomitância com a abertura do prazo recursal.

5.3.7.2. A proposta negociada deverá apresentar os mesmos valores originalmente estipulados ou com redução, não sendo aceito qualquer tipo de aumento dos valores dos itens já orçados.

5.3.7.3. A apresentação de itens com valores maiores na proposta negociada, não se tratando de erro material, ensejará a sua desclassificação.

6. ESCLARECIMENTOS

6.1. As dúvidas na interpretação do presente documento e anexos, consultas ou pedido de esclarecimentos acerca das informações técnicas porventura existentes, poderão ser feitos via e-mail de forma **expressa, clara, concisa e objetiva**, constando no corpo do texto do e-mail a identificação completa da empresa pré-qualificada participante e do representante que questiona as informações ou solicita esclarecimentos.

6.2. Os pedidos de esclarecimentos deverão ser encaminhados **até às 17h00 do 3º (terceiro) dia útil que antecede o término do prazo de apresentação das propostas**.

6.3. O endereço de e-mail para os esclarecimentos é: **avaliacao.nuvem@etice.ce.gov.br**.

6.4. A ETICE terá um prazo de até 02 (dois) dias úteis para resposta, sendo possível estender esse prazo de acordo com a complexidade dos esclarecimentos e/ou a necessidade de utilização de recursos técnicos externos à ETICE.

6.5. Caso a(s) resposta(s) dos esclarecimentos provoquem alterações das definições técnicas do projeto e estas sejam consideradas relevantes pela ETICE, será reiniciada a contagem dos prazos estabelecidos no item 4.1 deste documento, cabendo comunicação prévia e única a todas as pré-qualificadas.

6.6. **As quantidades aqui mencionadas são previsões e NÃO implicam em obrigatoriedade de contratação de quaisquer quantidades pela Administração Pública, servindo apenas como referencial para a elaboração das propostas das empresas pré-qualificadas pela ETICE.**

7. DAS ESPECIFICAÇÕES TÉCNICAS DOS SERVIÇOS

ITEM	DESCRITIVO	UND	QTD
1	SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 1	SERV	200
2	SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 2	SERV	50
3	SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 3	SERV	30
4	SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 4	SERV	20
5	SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 5	SERV	12
6	SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 6	SERV	10
7	SERVIÇO DE ACESSO SEGURO DE DISPOSITIVOS A REDE COM GERENCIA EM NUVEM	SERV	10000
8	SERVIÇO DE VISIBILIDADE DE SEGURANÇA PARA REDE EM NUVEM	SERV	10000
9	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - TIPO 1	SERV	50
10	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - TIPO 2	SERV	200
11	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM -TIPO 3	SERV	200
12	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - TIPO 4	SERV	200
13	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - PONTO DE ACESSO DE REDE SEM FIO WIFI INTERNO - TIPO 1	SERV	5000
14	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - PONTO DE ACESSO DE REDE SEM FIO WIFI INTERNO - TIPO 2	SERV	2000
15	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - PONTO DE ACESSO DE REDE SEM FIO WIFI INTERNO - TIPO 3	SERV	1000

16	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - PONTO DE ACESSO DE REDE SEM FIO WIFI EXTERNO - TIPO 4	SERV	1000
17	INJETOR POE 802.3	INJETOR POE	1000
18	SOLUÇÃO DE POLÍTICA E AUTENTICAÇÃO DE USUÁRIOS DE REDE SEM FIO	SERV	50
19	SOLUÇÃO DE POLÍTICA E AUTENTICAÇÃO DE USUÁRIOS DE REDE SEM FIO COM VERIFICAÇÃO DE POSTURA DE DISPOSITIVO	SERV	10
20	SERVIÇO DE INSTALAÇÃO FÍSICA ATÉ 50 METROS	SERV	4000
21	SERVIÇO DE INSTALAÇÃO FÍSICA ATÉ 100 METROS	SERV	2000
22	SERVIÇO DE SITE SURVEY	SERV	300
23	SERVIÇOS DE GERENCIAMENTO, ORQUESTRAÇÃO DA NUVEM, SUSTENTAÇÃO EMERGENCIAL, ADMINISTRAÇÃO DOS PROJETOS.	UST	30.000

7.1. ESPECIFICAÇÃO DETALHADA

7.1.1. A especificação detalhada dos itens está descrita no **ANEXO A- CARACTERÍSTICAS E ESPECIFICAÇÕES DOS SERVIÇOS.**

8. DA VIGÊNCIA DO CONTRATO

8.1. Os prazos de vigência e de execução contratual serão de 12 (doze) meses, podendo ser prorrogado, a critério da Contratante, com concordância da contratada, por períodos iguais ou inferiores, conforme art. 71 da Lei Federal 13.303/2016 e do art. 148 do Regulamento de Licitações e Contratos da ETICE.

8.2. Referido contrato poderá ser alterado nos casos previstos no art. 81 da Lei Federal n°13.303/2016 e no art. 149 do Regulamento de Licitações e Contratos da ETICE.

9. DO MODELO DE PROPOSTA

9.1. O modelo de proposta encontra-se no **ANEXO J**.

10. ACORDO DE NÍVEIS DE SERVIÇOS – SLA

10.1. A gestão e fiscalização do contrato dar-se-ão mediante o estabelecimento e acompanhamento de indicadores de desempenho, disponibilidade e qualidade, que comporão o Acordo de Nível de Serviço (SLA) entre a Contratante e Contratada.

10.2. O Acordo de Nível de Serviço está especificado no **ANEXO I** da presente Chamada de Oportunidade.

11. CONFIDENCIALIDADE DOS TRABALHOS

11.1. A Contratada, seu preposto e qualquer profissional dela, envolvidos na realização dos trabalhos, obrigam-se a tratar todas as informações obtidas junto à ETICE e seu cliente final como informação sigilosa ou confidencial, devendo neste sentido mantê-las sob estrito sigilo, comprometendo-se ainda em não comunicar, divulgar ou

revelar as informações confidenciais a terceiros, mesmo após a finalização dos trabalhos a confidencialidade das informações permanece.

11.2. Para tal, serão consideradas como informações confidenciais todas e quaisquer informações ou dados, independentemente de estarem expressamente classificados como confidenciais, fornecidas verbalmente ou por escrito, ou de qualquer outra forma, corpórea ou não, cuja divulgação possa provocar prejuízos de qualquer natureza, abrangendo, mas não se limitando a, pormenores, estratégias de negócios, pesquisas, dados financeiros e estatísticos, informações sobre negociações em andamento, informações sobre softwares, informações cadastrais, documentos que venha a ter conhecimento ou acesso, ou que venha a receber da contratante, sejam de caráter técnico ou não.

11.3. Tais informações confidenciais deverão ser usadas exclusivamente para a condução dos trabalhos objeto da relação de serviços entre a ETICE, cliente final e a contratante, não podendo, sob nenhuma forma ou pretexto, serem divulgadas, reveladas, reproduzidas, utilizadas ou ser dado conhecimento a terceiros estranhos a esta contratação, exceto quando o dever de divulgar tais informações seja estritamente por força de exigência legal, devendo a parte obrigada a fornecer tais informações, avisar imediatamente a outra parte sobre tal exigência legal para, se for o caso, tomar as providências que achar necessárias.

11.4. A Contratada deverá apresentar "Termo de Responsabilidade e Sigilo", contendo a declaração de manutenção de sigilo e ciência das normas de segurança da ETICE, assinado por cada empregado seu que estiver diretamente envolvido na contratação, quando o serviço exigir.

11.5. A contratada deverá entregar à ETICE, no momento da rescisão do contrato, todo o material físico ou digital de propriedade da contratante e destruir qualquer cópia em posse da contratada.

12. DA FRAUDE E DA CORRUPÇÃO

12.1. As Pré-Qualificadas devem observar e a contratada deve observar e fazer observar, por seus fornecedores e subcontratados, se admitida subcontratação, o mais alto padrão de ética durante todo o processo de licitação de contratação e de execução do objeto contratual.

12.2. Para os propósitos deste item, definem-se as seguintes práticas:

12.2.6. "**prática corrupta**": oferecer, dar, receber ou solicitar, direta ou indiretamente, qualquer vantagem com o objetivo de influenciar a ação de servidor público no processo de licitação ou na execução de contrato;

12.2.7. "**prática fraudulenta**": a falsificação ou omissão dos fatos, com o objetivo de influenciar o processo de licitação ou de execução de contrato;

12.2.8. "**prática conluiada**": esquematizar ou estabelecer um acordo entre duas ou mais licitantes, com ou sem o conhecimento de representantes ou prepostos do órgão licitador, visando estabelecer preços em níveis artificiais e não- competitivos;

12.2.9. "**prática coercitiva**": causar dano ou ameaçar causar dano, direta ou indiretamente, às pessoas ou sua propriedade, visando a influenciar sua participação em um processo licitatório ou afetar a execução do contrato;

12.2.10. "**prática obstrutiva**":

12.2.10.5. destruir, falsificar, alterar ou ocultar provas em inspeções ou fazer declarações falsas aos representantes do organismo financeiro multilateral, com o objetivo de impedir materialmente a apuração de alegações de prática prevista neste subitem;

12.2.10.6. atos cuja intenção seja impedir materialmente o exercício do direito de o organismo financeiro multilateral promover inspeção.

12.3. Na hipótese de financiamento, parcial ou integral, por organismo financeiro multilateral, mediante adiantamento ou reembolso, este organismo imporá sanção sobre uma empresa ou pessoa física, para a outorga de contratos

financiados pelo organismo se, em qualquer momento, constatar o envolvimento da empresa, diretamente ou por meio de um agente, em práticas corruptas, fraudulentas, conluiadas, coercitivas ou obstrutivas ao participar da licitação ou da execução um contrato financiado pelo organismo.

12.4. Considerando os propósitos dos itens acima, a pré qualificada vencedora como condição para a contratação, deverá concordar e autorizar que, na hipótese de o contrato vir a ser financiado, em parte ou integralmente, por organismo financeiro multilateral, mediante adiantamento ou reembolso, permitirá que o organismo financeiro e/ou pessoas por ele formalmente indicadas possam inspecionar o local de execução do contrato e todos os documentos e registros relacionados à licitação e à execução do contrato.

12.5. A contratante, garantida a prévia defesa, aplicará as sanções administrativas pertinentes, previstas na Lei, se comprovar o envolvimento de representante da empresa ou da pessoa física contratada em práticas corruptas, fraudulentas, conluiadas ou coercitivas, no decorrer da licitação ou na execução do contrato financiado por organismo financeiro multilateral, sem prejuízo das demais medidas administrativas, criminais e cíveis.

13. DA SUBCONTRATAÇÃO

13.1. Será admitida a subcontratação no limite de até 30% (trinta por cento) do objeto, conforme disposto no art. 78 da Lei nº 13.303/2016 e nos arts. 143 a 147 do Regulamento de Licitações e Contratos da ETICE, desde que não constitua o escopo principal da contratação, e, se previamente aprovada pela ETICE.

13.2. A subcontratação de que trata esta cláusula, **não exclui a responsabilidade da contratada perante a ETICE quanto à qualidade do objeto contratado**, não constituindo, portanto, **qualquer vínculo contratual ou legal da ETICE com a subcontratada**.

13.3. A empresa subcontratada deverá atender, em relação ao objeto da subcontratação, as exigências de qualificação técnica impostas a pré qualificada vencedora.

13.4. É **vedada** a subcontratação de empresa ou consórcio que tenha participado:

13.4.6. Do procedimento licitatório do qual se originou a contratação.

13.4.7. Direta ou indiretamente, da elaboração de projeto básico ou executivo.

14. DAS OBRIGAÇÕES DA CONTRATADA

14.1. Prestar os serviços de forma alinhada aos termos especificados no presente documento, no Contrato e na Proposta Comercial, responsabilizando-se integralmente pela exploração e execução do serviço perante a Contratante.

14.2. Manter durante toda a execução contratual, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

14.3. Aceitar, nas mesmas condições contratuais, os percentuais de acréscimos ou supressões limitados ao estabelecido no §1º, do art. 81, da Lei Federal nº 13.303/2016, tomando-se por base o valor contratual.

14.4. 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.

14.5. 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 para execução contratual, não transferindo a responsabilidade à ETICE para nenhum fim de direito.

14.6. Prestar imediatamente as informações e os esclarecimentos que venham a ser solicitados pela ETICE, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidas no prazo de 24 (vinte e quatro) horas.

14.7. Refazer o objeto contratual que comprovadamente apresente condições de defeito ou em desconformidade com as especificações deste termo, contado da sua notificação.

14.8. Cumprir, quando for o caso, as condições de garantia do objeto, responsabilizando-se pelo período oferecido em sua proposta, observando o prazo mínimo exigido pela Administração.

14.9. Providenciar a substituição de qualquer profissional envolvido na execução do objeto contratual, cuja conduta seja considerada indesejável pela fiscalização da ETICE.

14.10. Responsabilizar-se por todos os direitos e obrigações contratados, mesmo que transfira para autorizadas técnicas parte dos serviços contratados.

14.11. Comunicar ao gestor do contrato, por escrito, qualquer fato relacionado ao uso indevido do equipamento, para providências por parte da CONTRATANTE.

14.12. Comunicar antecipadamente a realização de intervenções nos ambientes técnicos da Contratante entre datacenters, no caso de qualquer possibilidade de impacto na prestação dos serviços.

14.13. Assinar Termo de Confidencialidade e Sigilo, resguardando que os recursos, dados e informações de propriedade da Contratante, e quaisquer outros, repassados por força do objeto do contrato, constituem informação privilegiada e possuem caráter de confidencialidade e sigilo.

14.14. Manter, sob as penas da Lei, o mais completo e absoluto sigilo sobre quaisquer dados, informações, documentos, especificações técnicas e comerciais dos bens da Contratante, de que venha a tomar conhecimento ou ter acesso, ou que venham a ser confiados, sejam relacionados ou não com a prestação de serviços objeto do contrato.

14.15. Respeitar a legislação relativa à disposição final ambientalmente adequada dos resíduos gerados, mitigação dos danos ambientais por meio de medidas condicionantes e de compensação ambiental e outros, conforme § 1º do art. 32 da Lei 13.303/2016.

15. DAS OBRIGAÇÕES DA CONTRATANTE

15.1. Solicitar a execução do objeto à contratada através da emissão de Ordem de Serviço/Fornecimento.

15.2. Proporcionar à contratada todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual, consoante estabelece a Lei Federal no 13.303/2016 e, subsidiariamente, a Lei Federal nº 8.666/1993.

15.3. Fiscalizar a execução do objeto contratual através de sua unidade competente, podendo, em decorrência, solicitar providências da contratada, que atenderá ou justificará de imediato.

15.4. Notificar a contratada de qualquer irregularidade decorrente da execução do objeto contratual.

15.5. Efetuar os pagamentos devidos à contratada nas condições estabelecidas neste contrato.

15.6. Aplicar as penalidades previstas em lei e neste instrumento.

15.7. Não obstante a Contratada seja a única e exclusiva responsável pela execução dos serviços especificados, a Contratante reserva-se o direito de exercer a mais ampla, irrestrita, permanente e completa fiscalização, diretamente ou por outros prepostos designados, podendo, em decorrência, solicitar providências da Contratada, que atenderá ou justificará de imediato.

15.8. Permitir o acesso dos empregados da Contratada, quando necessário, para execução dos serviços e prestar as informações e os esclarecimentos que venham a ser solicitados pela Contratada.

Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP:60.130-240 - Fortaleza/CE
Fone: (85) 3108-0000
www.etice.ce.gov.br

16. DAS DISPOSIÇÕES GERAIS

16.1. Esta chamada de oportunidade **não implica necessariamente em contratação**, nos moldes já dispostos Edital de Pré-Qualificação 001/2019, podendo a autoridade competente revogá-la por razões de interesse público, anulá-la por ilegalidade de ofício ou por provocação de terceiros, mediante decisão devidamente fundamentada, sem quaisquer reclamações ou direitos à indenização ou reembolso.

16.2. É facultada à Comissão de Avaliação ou à autoridade competente, em qualquer fase da licitação, a promoção de diligência destinada a esclarecer ou a complementar a instrução do processo licitatório, **vedada a inclusão posterior de documentos** que deveriam constar originariamente na proposta e na documentação.

16.3. Toda a documentação fará parte dos autos e não será devolvida à pré qualificada, ainda que se trate de originais.

16.4. Na contagem dos prazos estabelecidos nesta Chamada de Oportunidade, excluir-se-ão os dias de início e incluir-se-ão os dias de vencimento. **Os prazos estabelecidos neste edital para a fase externa se iniciam e se vencem somente em dias úteis de expediente da ETICE.**

16.5. Os representantes legais das Pré-Qualificadas são responsáveis pela fidelidade e legitimidade das informações e dos documentos apresentados em qualquer fase da licitação.

16.6. O desatendimento de exigências meramente formais, não essenciais, não implicará no afastamento da Pré-Qualificada, desde que seja possível a aferição da sua qualificação e a exata compreensão da sua proposta.

16.7. A Comissão de Avaliação poderá sanar erros formais que **NÃO** acarretem prejuízos para o objeto da Chamada de Oportunidade, a Administração e as Pré-Qualificadas, dentre estes, os decorrentes de operações aritméticas.

16.8. Desde já fica estabelecido que caso a Pré-Qualificada **NÃO APRESENTE PROPOSTA** para a presente Chamada de Oportunidade, já está renunciando, assim, expressamente ao direito de recurso e respectiva contrarrazões, concordando com o curso desta Chamada de Oportunidade de Serviços de Nuvem Pública, aderente ao Edital de Pré-Qualificação Permanente de Serviços em Nuvem NO 001/ 2019 - ETICE.

16.9. Os casos omissos serão resolvidos pela Comissão de Avaliação, nos termos da legislação pertinente.

16.10. As normas que disciplinam esta Chamada de Oportunidade serão sempre interpretadas em favor da ampliação da disputa.

16.11. Os documentos referentes aos orçamentos, bem como o valor estimado da contratação, possuem caráter sigiloso e serão disponibilizados em concomitância com a abertura do prazo recursal, em conformidade com o Regulamento de Licitações e Contratos da ETICE.

16.12. O foro designado para julgamento de quaisquer questões judiciais resultantes deste edital será o da **Comarca de Fortaleza**, Capital do Estado do Ceará.

Fortaleza,

De Acordo:	**Aprovo:**
Márcio Adriano Castro Lima *Diretor* *Diretoria de Tecnologia e Inovação (DITEC)*	**Francisco Antônio Martins Barbosa** *Presidente da Etice*

Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP:60.130-240 - Fortaleza/CE
Fone: (85) 3108-0000
www.etice.ce.gov.br

ROL DE ANEXOS:

ANEXO A - CARACTERÍSTICAS E ESPECIFICAÇÕES DOS SERVIÇOS
ANEXO B – CARACTERÍSTICAS E ESPECIFICAÇÕES DOS SERVIÇOS DE GERENCIAMENTO, ORQUESTRAÇÃO DA NUVEM, SUSTENTAÇÃO EMERGENCIAL, ADMINISTRAÇÃO DOS PROJETOS
ANEXO C - CARACTERÍSTICAS E ESPECIFICAÇÕES DA SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DOS ITENS 1 A 6 E CARACTERÍSTICAS E ESPECIFICAÇÕES DA SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DOS ITENS 9 A 16
ANEXO D - CARACTERÍSTICAS E ESPECIFICAÇÕES DOS SERVIÇOS DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE SEGURA, INSTALAÇÃO CONFIGURAÇÃO E TESTES (ITENS 1 A 6) E CARACTERÍSTICAS E ESPECIFICAÇÕES DA SERVIÇOS DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE LAN E SOFTWARE, INSTALAÇÃO CONFIGURAÇÃO E TESTES (ITENS 7 A 10)
ANEXO E - CARACTERÍSTICAS E ESPECIFICAÇÕES DOS SERVIÇOS DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE WLAN E SOFTWARE, INSTALAÇÃO CONFIGURAÇÃO E TESTES (ITENS 5 A 7)
ANEXO F - MANUTENÇÃO E SUPORTE TÉCNICO
ANEXO G - CATÁLOGO DE SERVIÇOS
ANEXO H - LISTA DE PERFIS TÉCNICOS
ANEXO I - DO ACORDO DE NÍVEIS DE SERVIÇOS – SLA
ANEXO J - MODELO DE PROPOSTA

Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP:60.130-240 - Fortaleza/CE
Fone: (85) 3108-0000
www.etice.ce.gov.br

ANEXO A - CARACTERÍSTICAS E ESPECIFICAÇÕES DOS SERVIÇOS

1. ESPECIFICAÇÃO DETALHADA

1.1.1. SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 1

1.1.1.1. SERVIÇO DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM

1.1.1.1.1. A solução deve ser fornecida incluindo disponibilização de equipamento e software, instalação, configuração e testes conforme características e especificações descritas no ANEXO D;

1.1.1.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.1.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO F;

1.1.1.3. CARACTERÍSTICAS GERAIS

1.1.1.3.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.1.3.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

1.1.1.3.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;

1.1.1.3.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

1.1.1.3.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.1.3.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.1.3.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.1.4. CAPACIDADE E QUANTIDADES

1.1.1.4.1. Throughput de, no mínimo, 330 Mbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

1.1.1.4.2. Suporte a, no mínimo, 490.000 (quatrocentas e noventa mil) conexões ou sessões simultâneas;

1.1.1.4.3. Suporte a, no mínimo, 10.300 (dez mil e trezentas) novas conexões ou sessões por segundo;

1.1.1.4.4. Throughput de, no mínimo, 950 Mbps para conexões VPN;

1.1.1.4.5. Licenciado ou permitir, pelo menos, 100 conexões ou sessões simultâneas de

VPN client-to-site;

1.1.1.4.6. Possuir, pelo menos, 6 (seis) interfaces de rede 1Gbps UTP;

1.1.1.4.7. Possuir 1 (uma) interface do tipo console ou similar;

1.1.1.4.8. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces. Caso um mesmo Throughput seja apresentado mais de uma vez em diferentes métricas, será considerado o de maior valor;

1.1.1.5. FUNCIONALIDADES DE FIREWALL

1.1.1.5.1. Deve suportar autenticação para o serviço NTP.

1.1.1.5.2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador.

1.1.1.5.3. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e Rede.

1.1.1.5.4. Deve suportar SNMP v2 e v3.

1.1.1.5.5. Deve ser possível realizar captura de pacotes diretamente na gerência do equipamento.

1.1.1.5.6. Deve ser possível monitorar a utilização de CPU e memória diretamente na gerência do equipamento.

1.1.1.5.7. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento.

1.1.1.5.8. Deve ser possível conectar a serviços de DDNS;

1.1.1.5.9. Deve ser possível configurar o timeout da sessão do administrador na interface web.

1.1.1.5.10. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.

1.1.1.5.11. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.

1.1.1.5.12. A solução deve possibilitar ao administrador realizar a integração com o AD (Active Directory) através de um assistente de configuração na própria interface gráfica do produto;

1.1.1.5.13. A solução deve identificar usuários das seguintes fontes pelo menos:

1.1.1.5.14. Active Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

1.1.1.5.15. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

1.1.1.5.16. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

1.1.1.5.17. Na integração com o AD, a operação de cadastro deve ser realizada na própria gerência do equipamento, de maneira simples e sem utilização de scripts de comando;

1.1.1.6. FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS

1.1.1.6.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio equipamento sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

1.1.1.6.2. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento;

1.1.1.6.3. Deve ser possível realizar a atualização manualmente sem necessidade de internet através da importação do pacote de atualização.

1.1.1.6.4. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo, pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta, scanning de portas, CIFS Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS SQL Server, IKE aggressive Exchange;

1.1.1.6.5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

1.1.1.6.6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;

1.1.1.6.7. A solução deve proteger contra-ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

1.1.1.6.8. A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

1.1.1.6.9. Em cada proteção de segurança, devem estar inclusas informações como: categoria, tipo de impacto na ferramenta, severidade, e tipo de ação que a solução irá executar;

1.1.1.6.10. A solução de IPS deve possuir um modo de solução de problemas, que define o uso de perfil de detecção sem modificar as proteções individuais já criadas e customizadas;

1.1.1.6.11. Deve ser possível criar regras de exceção no IPS para que a solução não faça a inspeção de um tráfego específico por pelo menos proteção, origem, destino, serviço ou porta.

1.1.1.6.12. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.

1.1.1.6.13. A solução deve incluir ferramenta própria ou solução de terceiros para mitigar/bloquear a comunicação entre os hosts infectados com bot e operador remoto (command & control).

1.1.1.6.14. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.

1.1.1.6.15. A solução de proteção contra malware e bot deve compartilhar a mesma política para facilitar o gerenciamento.

1.1.1.6.16. A solução de proteção contra malware e bot deve possuir um modo de solução de problemas, que define o uso de perfil de detecção, sem modificar as proteções individuais já criadas e customizadas;

1.1.1.6.17. As proteções devem ser ativadas baseadas em, pelo menos, critério de nível de confiança, ações da proteção e impacto de performance.

1.1.1.6.18. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou

gerar um alerta;

1.1.1.6.19. Deve ser possível criar regras de exceção para que a solução não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

1.1.1.6.20. A solução de anti-malware deve suportar protocolos SMTP e P OP 3, FTP, HT TP em qualquer porta;

1.1.1.6.21. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:

1.1.1.6.22. Inspecionar tipos de arquivos conhecidos que contenham malware;

1.1.1.6.23. Inspecionar todos os tipos de arquivos;

1.1.1.6.24. Inspecionar tipos de arquivos de famílias específicas;

1.1.1.6.25. Deve bloquear acesso a URLs com malware;

1.1.1.6.26. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado;

1.1.1.7. FILTRO DE CONTEÚDO WEB

1.1.1.7.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações web e filtro URL integrada no próprio appliance de segurança que permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações web e URL;

1.1.1.7.2. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;

1.1.1.7.3. Deve ser possível configurar com apenas um clique o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking.

1.1.1.7.4. Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.

1.1.1.7.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:

1.1.1.7.6. Usuário do Active Directory

1.1.1.7.7. IP

1.1.1.7.8. Rede

1.1.1.7.9. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.

1.1.1.7.10. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

1.1.1.7.11. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

1.1.1.7.12. Deve ser possível limitar o consumo de banda de aplicações.

1.1.1.7.13. A base de aplicações deve ser superior a 2900 aplicações, reconhecendo, pelo menos, as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp, etc;

1.1.1.7.14. Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.

1.1.1.7.15. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

1.1.1.7.15.1. Aceitar
1.1.1.7.15.2. Bloquear e informar

1.1.1.8. IDENTIFICAÇÃO DE USUÁRIOS

1.1.1.8.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.
1.1.1.8.2. A solução deve possibilitar ao administrador realizar a integração com o AD através de um assistente de configuração na própria interface gráfica do produto;
1.1.1.8.3. A solução deve identificar usuários das seguintes fontes:
1.1.1.8.4. Active Directory o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;
1.1.1.8.5. Autenticação via navegador para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;
1.1.1.8.6. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;
1.1.1.8.7. Na integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scripts de comando;

1.1.1.9. FUNCIONALIDADES DE ACESSO REMOTO

1.1.1.9.1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;
1.1.1.9.2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).
1.1.1.9.3. Deve suportar pelo menos os seguintes métodos de conexão:
1.1.1.9.4. Conexão através de cliente instalado no laptop ou desktop do usuário.
1.1.1.9.5. Conexão através de cliente instalado no smartphone e tablets.
1.1.1.9.6. Conexão através de navegador com SSL.
1.1.1.9.7. Conexão através de cliente nativo Windows L2TP.
1.1.1.9.8. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.
1.1.1.9.9. A solução deve permitir conexão VPN aos seguintes usuários:
1.1.1.9.10. Usuários locais na própria base do appliance.
1.1.1.9.11. Grupos de usuários locais na própria base do appliance.
1.1.1.9.12. Grupos de usuários do Active Directory.
1.1.1.9.13. Grupos de usuários Radius.
1.1.1.9.14. A solução deve permitir atribuir um endereço específico para o usuário remoto.

1.1.1.10. FUNCIONALIDADE DE VPN SITE-TO-SITE

1.1.1.10.1. A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;
1.1.1.10.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de

terceiros;

1.1.1.10.3. A solução deve suportar autenticação com senha ou certificado;

1.1.1.10.4. Deve suportar, pelo menos, criptografia AES 128 e 256;

1.1.1.10.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;

1.1.1.11. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

1.1.1.11.1. Suportar a criação de políticas de QoS por:

1.1.1.11.1.1. Endereço de origem, endereço de destino e por porta;

1.1.1.11.2. O QoS deve possibilitar a definição de classes por:

1.1.1.11.2.1. Banda garantida, banda máxima e fila de prioridade;

1.1.1.11.3. Disponibilizar estatísticas em tempo real para classes de QoS;

1.1.1.11.4. A solução deve permitir, por aplicação, o encaminhamento do tráfego para diferentes links de Internet, sejam eles locais ou remotos, deve suportar múltiplos links de acesso como MPLS, Internet Banda Larga, LTE e Satélite.

1.1.1.11.5. Deve possibilitar a utilização de configuração inteligente de acessos WAN IP ativos-ativos sem a necessidade de switch para agregação WAN, ou seja, distribuir o tráfego simultaneamente pelos N acessos conectados e não apenas na configuração dos acessos principal e backup.

1.1.1.11.6. Medir parâmetros de rede jitter, perda de pacotes e latência em tempo real.

1.1.1.11.7. Se houver necessidade de saída internet do ponto remoto, deve ser possível selecionar por tipo de aplicativo;

1.1.1.11.8. Deve permitir a comunicação indireta entre localidades por meio de uma topologia “hub and spoke”;

1.1.1.11.9. Deve balancear o tráfego de aplicativos em vários links simultaneamente;

1.1.1.11.10. Redistribuição do tráfego balanceado, de forma inteligente, tendo em conta o congestionamento da largura de banda, entre os links utilizados, em caso de falhas nestes links, ou de acordo com as políticas de qualidade pré-definidas;

1.1.1.11.11. Habilitar a criação de políticas de negócios para controlar o padrão de redirecionamento de tráfego e aplicar qualidade de serviço;

1.1.1.11.12. Suportar o redirecionamento do tráfego de internet de pontos remotos para um ponto de internet centralizado, usando políticas por aplicativo;

1.1.1.11.13. Redirecionamento condicionado do tráfego de internet em caso de falha do link de internet local ou do link remoto centralizado, utilizando políticas por aplicativo;

1.1.1.11.14. Suporte simultâneo ao redirecionamento do tráfego da Web de alguns aplicativos para a Internet centralizada, outros aplicativos para a Internet local e outros aplicativos para inspeção avançada de segurança na nuvem.

1.1.1.11.15. Deve ser capaz de criar um túnel otimizado que proteja os aplicativos TCP e UDP contra jitter e perda de pacotes para garantir desempenho de ponta a ponta para áudio, vídeo e tráfego transacional;

1.1.1.11.16. Usar probes artificiais baseadas em ICMP, UDP ou TCP para medir a qualidade da rede percebida pelo tráfego do usuário, medindo no minimo jitter, latencia e perda de pacotes.

1.1.1.11.17. Capacidade de realizar agregação de largura de banda automaticamente entre links de diferentes velocidades, levando em consideração o uso total da largura de banda de cada link sem causar congestionamento em links de baixa

velocidade.

1.1.1.11.18. Habilitar a configuração de backup do link, ou seja, um link de backup só deve ser ativado quando o link principal falhar.

1.1.1.11.19. Implementar um mecanismo de proteção de variação de latência (jitter) mesmo que a degradação esteja em todos os links, para proteger o tráfego em tempo real (voz e vídeo).

1.1.1.11.20. Garantir o desempenho de aplicativos em um cenário de link de transporte duplo quando ambos os links estão degradados simultaneamente

1.1.1.11.21. Possuir um mecanismo de priorização (QoS) para proteger o tráfego de aplicativos clientes prioritários quando houver congestionamento em pontos remotos

1.1.1.11.22. Deve automatizar o reconhecimento dos melhores níveis de SLA de rede com base no tipo de tráfego seja áudio, vídeo ou transacional.

1.1.1.11.23. O console de gerenciamento deve informar o status operacional (UP/DOWN/SPEED) das interfaces LAN e WAN

1.1.1.11.24. O console de gerenciamento deve informar o status operacional de cada dispositivo que faz parte da rede para operacionalidade

1.1.1.11.25. Realizar medições de “Latência”/”Jitter”/”Queda de pacotes” em cada um dos túneis SDWAN independentemente, na direção de transmissão ou recepção

1.1.1.11.26. O orquestrador pode estar na nuvem do fabricante ou até mesmo ser instalado em um servidor dedicado ou virtualizado, utilizando uma máquina virtual

1.1.1.11.27. No caso do orquestrador estar na nuvem, a administração de atualizações, gerenciamento de alta disponibilidade e hardening do plano de gerenciamento deve ser realizada pelo fabricante da solução;

1.1.1.12. PREVENÇÃO DE AMEAÇAS AVANÇADAS

1.1.1.12.1. A solução deve incluir ferramenta própria ou solução de terceiros para proteção de redes contra ameaças desconhecidas em arquivos que são baixados da Internet ou anexados a e-mails.

1.1.1.12.2. A solução deve compartilhar a mesma política da proteção contra vírus e bot para facilitar o gerenciamento.

1.1.1.12.3. A solução deve trabalhar em modo de prevenção e não apenas detecção.

1.1.1.12.4. Deve permitir criar uma lista de exceção de e-mails que não devem ter seus anexos inspecionados.

1.1.1.12.5. Deve permitir criar uma lista de exceção para arquivos que não devem ser inspecionados.

1.1.1.12.6. A solução deve suportar protocolos SMTP, HTTP em qualquer porta;

1.1.1.12.7. Deve permitir configurar por tipo de arquivo as ações de inspeção ou bypass. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas

1.1.1.12.8. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF com tamanho até 15 Mb.

1.1.1.12.9. Deve permitir configurar como uma emulação em conexão http será tratada,

sendo permitida até que a emulação seja concluída ou bloqueada até a emulação ser completa.

1.1.1.13. SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO

1.1.1.13.1. A solução deve ser fornecida incluindo solução de gerenciamento centralizado conforme características e especificações descritas no ANEXO C;

1.1.2. SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 2

1.1.2.1. SERVIÇO DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM

1.1.2.1.1. A solução deve ser fornecida incluindo disponibilização de equipamento e software, instalação, configuração e testes conforme características e especificações descritas no ANEXO D;

1.1.2.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.2.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO F;

1.1.2.3. CARACTERÍSTICAS GERAIS

1.1.2.3.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.2.3.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

1.1.2.3.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;

1.1.2.3.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

1.1.2.3.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.2.3.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.2.3.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.2.4. CAPACIDADE E QUANTIDADES

1.1.2.4.1. Throughput de, no mínimo, 1.8 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

1.1.2.4.2. Suporte a, no mínimo, 2.200.000 (duas milhões e duzentas mil) conexões ou sessões simultâneas;

1.1.2.4.3. Suporte a, no mínimo, 64.000 (sessenta e quatro mil) novas conexões ou sessões por segundo;

1.1.2.4.4. Throughput de, no mínimo, 3.8 Gbps para conexões VPN;

1.1.2.4.5. Licenciado ou permitir, pelo menos, 500 conexões ou sessões simultâneas de VPN client-to-site;

1.1.2.4.6. Possuir, pelo menos, 16 (dezesseis) interfaces de rede 1Gbps UTP;

1.1.2.4.7. Possuir 1 (uma) interface do tipo console ou similar;

1.1.2.4.8. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces. Caso um mesmo Throughput seja apresentado mais de uma vez em diferentes métricas, será considerado o de maior valor;

1.1.2.5. FUNCIONALIDADES DE FIREWALL

1.1.2.5.1. Deve suportar autenticação para o serviço NTP.

1.1.2.5.2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador.

1.1.2.5.3. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e Rede.

1.1.2.5.4. Deve suportar SNMP v2 e v3.

1.1.2.5.5. Deve ser possível realizar captura de pacotes diretamente na gerência do equipamento.

1.1.2.5.6. Deve ser possível monitorar a utilização de CPU e memória diretamente na gerência do equipamento.

1.1.2.5.7. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento.

1.1.2.5.8. Deve ser possível conectar a serviços de DDNS;

1.1.2.5.9. Deve ser possível configurar o timeout da sessão do administrador na interface web.

1.1.2.5.10. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.

1.1.2.5.11. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.

1.1.2.5.12. A solução deve possibilitar ao administrador realizar a integração com o AD (Active Directory) através de um assistente de configuração na própria interface gráfica do produto;

1.1.2.5.13. A solução deve identificar usuários das seguintes fontes pelo menos:

1.1.2.5.14. Active Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

1.1.2.5.15. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

1.1.2.5.16. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

1.1.2.5.17. Na integração com o AD, a operação de cadastro deve ser realizada na própria gerência do equipamento, de maneira simples e sem utilização de scripts de comando;

1.1.2.6. FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS

1.1.2.6.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio equipamento sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

1.1.2.6.2. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento;

1.1.2.6.3. Deve ser possível realizar a atualização manualmente sem necessidade de internet através da importação do pacote de atualização.

1.1.2.6.4. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo, pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta, scanning de portas, CIFS Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS SQL Server, IKE aggressive Exchange;

1.1.2.6.5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

1.1.2.6.6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;

1.1.2.6.7. A solução deve proteger contra-ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

1.1.2.6.8. A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

1.1.2.6.9. Em cada proteção de segurança, devem estar inclusas informações como: categoria, tipo de impacto na ferramenta, severidade, e tipo de ação que a solução irá executar;

1.1.2.6.10. A solução de IPS deve possuir um modo de solução de problemas, que define o uso de perfil de detecção sem modificar as proteções individuais já criadas e

customizadas;

1.1.2.6.11. Deve ser possível criar regras de exceção no IPS para que a solução não faça a inspeção de um tráfego específico por pelo menos proteção, origem, destino, serviço ou porta.

1.1.2.6.12. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.

1.1.2.6.13. A solução deve incluir ferramenta própria ou solução de terceiros para mitigar/bloquear a comunicação entre os hosts infectados com bot e operador remoto (command & control).

1.1.2.6.14. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.

1.1.2.6.15. A solução de proteção contra malware e bot deve compartilhar a mesma política para facilitar o gerenciamento.

1.1.2.6.16. A solução de proteção contra malware e bot deve possuir um modo de solução de problemas, que define o uso de perfil de detecção, sem modificar as proteções individuais já criadas e customizadas;

1.1.2.6.17. As proteções devem ser ativadas baseadas em, pelo menos, critério de nível de confiança, ações da proteção e impacto de performance.

1.1.2.6.18. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;

1.1.2.6.19. Deve ser possível criar regras de exceção para que a solução não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

1.1.2.6.20. A solução de anti-malware deve suportar protocolos SMTP e P OP 3, FTP, HT TP em qualquer porta;

1.1.2.6.21. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:

1.1.2.6.22. Inspecionar tipos de arquivos conhecidos que contenham malware;

1.1.2.6.23. Inspecionar todos os tipos de arquivos;

1.1.2.6.24. Inspecionar tipos de arquivos de famílias específicas;

1.1.2.6.25. Deve bloquear acesso a URLs com malware;

1.1.2.6.26. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado;

1.1.2.7. FILTRO DE CONTEÚDO WEB

1.1.2.7.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações web e filtro URL integrada no próprio appliance de segurança que permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações web e URL;

1.1.2.7.2. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;

1.1.2.7.3. Deve ser possível configurar com apenas um clique o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking.

1.1.2.7.4. Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.

1.1.2.7.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:

1.1.2.7.5.1. Usuário do Active Directory

1.1.2.7.5.2. IP

1.1.2.7.5.3. Rede

1.1.2.7.6. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.

1.1.2.7.7. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

1.1.2.7.8. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

1.1.2.7.9. Deve ser possível limitar o consumo de banda de aplicações.

1.1.2.7.10. A base de aplicações deve ser superior a 2900 aplicações, reconhecendo, pelo menos, as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp, etc;

1.1.2.7.11. Deve ser possível realizar a recategorização de uma URL através da gerência do equipamento.

1.1.2.7.12. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

1.1.2.7.12.1. Aceitar

1.1.2.7.12.2. Bloquear e informar

1.1.2.8. IDENTIFICAÇÃO DE USUÁRIOS

1.1.2.8.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.

1.1.2.8.2. A solução deve possibilitar ao administrador realizar a integração com o AD através de um assistente de configuração na própria interface gráfica do produto;

1.1.2.8.3. A solução deve identificar usuários das seguintes fontes:

1.1.2.8.4. Active Directory o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

1.1.2.8.5. Autenticação via navegador para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

1.1.2.8.6. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

1.1.2.8.7. Na integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scripts de comando;

1.1.2.9. FUNCIONALIDADES DE ACESSO REMOTO

1.1.2.9.1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;

1.1.2.9.2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).

1.1.2.9.3. Deve suportar pelo menos os seguintes métodos de conexão:

1.1.2.9.4. Conexão através de cliente instalado no laptop ou desktop do usuário.

1.1.2.9.5. Conexão através de cliente instalado no smartphone e tablets.

1.1.2.9.6. Conexão através de navegador com SSL.

1.1.2.9.7. Conexão através de cliente nativo Windows L2TP.

1.1.2.9.8. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.

1.1.2.9.9. A solução deve permitir conexão VPN aos seguintes usuários:

1.1.2.9.10. Usuários locais na própria base do appliance.

1.1.2.9.11. Grupos de usuários locais na própria base do appliance.

1.1.2.9.12. Grupos de usuários do Active Directory.

1.1.2.9.13. Grupos de usuários Radius.

1.1.2.9.14. A solução deve permitir atribuir um endereço específico para o usuário remoto.

1.1.2.10. FUNCIONALIDADE DE VPN SITE-TO-SITE

1.1.2.10.1. A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;

1.1.2.10.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;

1.1.2.10.3. A solução deve suportar autenticação com senha ou certificado;

1.1.2.10.4. Deve suportar, pelo menos, criptografia AES 128 e 256;

1.1.2.10.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;

1.1.2.11. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

1.1.2.11.1. Suportar a criação de políticas de QoS por:

1.1.2.11.2. Endereço de origem, endereço de destino e por porta;

1.1.2.11.3. O QoS deve possibilitar a definição de classes por:

1.1.2.11.4. Banda garantida, banda máxima e fila de prioridade;

1.1.2.11.5. Disponibilizar estatísticas em tempo real para classes de QoS;

1.1.2.11.6. A solução deve permitir, por aplicação, o encaminhamento do tráfego para diferentes links de Internet, sejam eles locais ou remotos, deve suportar múltiplos links de acesso como MPLS, Internet Banda Larga, LTE e Satélite.

1.1.2.11.7. Deve possibilitar a utilização de configuração inteligente de acessos WAN IP ativos-ativos sem a necessidade de switch para agregação WAN, ou seja, distribuir o tráfego simultaneamente pelos N acessos conectados e não apenas na configuração dos acessos principal e backup.

1.1.2.11.8. Medir parâmetros de rede jitter, perda de pacotes e latência em tempo real.

1.1.2.11.9. Se houver necessidade de saída internet do ponto remoto, deve ser possível selecionar por tipo de aplicativo;

1.1.2.11.10. Deve permitir a comunicação indireta entre localidades por meio de uma topologia “hub and spoke”;

1.1.2.11.11. Deve balancear o tráfego de aplicativos em vários links simultaneamente;

1.1.2.11.12. Redistribuição do tráfego balanceado, de forma inteligente, tendo em conta o congestionamento da largura de banda, entre os links utilizados, em caso de falhas nestes links, ou de acordo com as políticas de qualidade pré-definidas;

1.1.2.11.13. Habilitar a criação de políticas de negócios para controlar o padrão de redirecionamento de tráfego e aplicar qualidade de serviço;

1.1.2.11.14. Suportar o redirecionamento do tráfego de internet de pontos remotos para um ponto de internet centralizado, usando políticas por aplicativo;

1.1.2.11.15. Redirecionamento condicionado do tráfego de internet em caso de falha do link de internet local ou do link remoto centralizado, utilizando políticas por aplicativo;

1.1.2.11.16. Suporte simultâneo ao redirecionamento do tráfego da Web de alguns aplicativos para a Internet centralizada, outros aplicativos para a Internet local e outros aplicativos para inspeção avançada de segurança na nuvem.

1.1.2.11.17. Deve ser capaz de criar um túnel otimizado que proteja os aplicativos TCP e UDP contra jitter e perda de pacotes para garantir desempenho de ponta a ponta para áudio, vídeo e tráfego transacional;

1.1.2.11.18. Usar probes artificiais baseadas em ICMP, UDP ou TCP para medir a qualidade da rede percebida pelo tráfego do usuário, medindo no minimo jitter, latencia e

perda de pacotes.

1.1.2.11.19. Capacidade de realizar agregação de largura de banda automaticamente entre links de diferentes velocidades, levando em consideração o uso total da largura de banda de cada link sem causar congestionamento em links de baixa velocidade.

1.1.2.11.20. Habilitar a configuração de backup do link, ou seja, um link de backup só deve ser ativado quando o link principal falhar.

1.1.2.11.21. Implementar um mecanismo de proteção de variação de latência (jitter) mesmo que a degradação esteja em todos os links, para proteger o tráfego em tempo real (voz e vídeo).

1.1.2.11.22. Garantir o desempenho de aplicativos em um cenário de link de transporte duplo quando ambos os links estão degradados simultaneamente

1.1.2.11.23. Possuir um mecanismo de priorização (QoS) para proteger o tráfego de aplicativos clientes prioritários quando houver congestionamento em pontos remotos

1.1.2.11.24. Deve automatizar o reconhecimento dos melhores níveis de SLA de rede com base no tipo de tráfego seja áudio, vídeo ou transacional.

1.1.2.11.25. O console de gerenciamento deve informar o status operacional (UP/DOWN/SPEED) das interfaces LAN e WAN

1.1.2.11.26. O console de gerenciamento deve informar o status operacional de cada dispositivo que faz parte da rede para operacionalidade

1.1.2.11.27. Realizar medições de “Latência”/”Jitter”/”Queda de pacotes” em cada um dos túneis SDWAN independentemente, na direção de transmissão ou recepção

1.1.2.11.28. O orquestrador pode estar na nuvem do fabricante ou até mesmo ser instalado em um servidor dedicado ou virtualizado, utilizando uma máquina virtual

1.1.2.11.29. No caso do orquestrador estar na nuvem, a administração de atualizações, gerenciamento de alta disponibilidade e hardening do plano de gerenciamento deve ser realizada pelo fabricante da solução;

1.1.2.12. PREVENÇÃO DE AMEAÇAS AVANÇADAS

1.1.2.12.1. A solução deve incluir ferramenta própria ou solução de terceiros para proteção de redes contra ameaças desconhecidas em arquivos que são baixados da Internet ou anexados a e-mails.

1.1.2.12.2. A solução deve compartilhar a mesma política da proteção contra vírus e bot para facilitar o gerenciamento.

1.1.2.12.3. A solução deve trabalhar em modo de prevenção e não apenas detecção.

1.1.2.12.4. Deve permitir criar uma lista de exceção de e-mails que não devem ter seus anexos inspecionados.

1.1.2.12.5. Deve permitir criar uma lista de exceção para arquivos que não devem ser

inspecionados.

1.1.2.12.6. A solução deve suportar protocolos SMTP, HTTP em qualquer porta;

1.1.2.12.7. Deve permitir configurar por tipo de arquivo as ações de inspeção ou bypass.

1.1.2.12.8. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas

1.1.2.12.9. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF com tamanho até 15 Mb.

1.1.2.12.10. Deve permitir configurar como uma emulação em conexão http será tratada, sendo permitida até que a emulação seja concluída ou bloqueada até a emulação ser completa.

1.1.2.13. SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO

1.1.2.13.1. A solução deve ser fornecida incluindo solução de gerenciamento centralizado conforme características e especificações descritas no ANEXO C;

1.1.3. SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 3

1.1.3.1. SERVIÇO DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM

1.1.3.1.1. A solução deve ser fornecida incluindo disponibilização de equipamento e software, instalação, configuração e testes conforme características e especificações descritas no ANEXO D;

1.1.3.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.3.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO F;

1.1.3.3. CARACTERÍSTICAS GERAIS

1.1.3.3.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.3.3.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

1.1.3.3.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;

1.1.3.3.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

1.1.3.3.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.3.3.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.3.3.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.3.4. CAPACIDADE E QUANTIDADES

1.1.3.4.1. Throughput de, no mínimo, 4.8 Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, anti-malware e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente;

1.1.3.4.2. Suporte a, no mínimo, 4.100.000 (quatro milhões e cem mil) conexões ou sessões simultâneas;

1.1.3.4.3. Suporte a, no mínimo, 98.000 (noventa e oito mil) novas conexões ou sessões por segundo;

1.1.3.4.4. Throughput de, no mínimo, 5.6 Gbps para conexões VPN;

1.1.3.4.5. Licenciado ou permitir, pelo menos, 500 conexões ou sessões simultâneas de VPN client-to-site;

1.1.3.4.6. Possuir, pelo menos, 16 (dezesseis) interfaces de rede 1Gbps UTP;

1.1.3.4.7. Possuir, pelo menos, 4 (quatro) interfaces de rede 10Gbps SFP+;

1.1.3.4.8. Possuir 1 (uma) interface do tipo console ou similar;

1.1.3.4.9. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces. Caso um mesmo Throughput seja apresentado mais de uma vez em diferentes métricas, será considerado o de maior valor;

1.1.3.5. FUNCIONALIDADES DE FIREWALL

1.1.3.5.1. Deve suportar autenticação para o serviço NTP.

1.1.3.5.2. Deve ser possível definir por quais origens de rede são permitidas as conexões do administrador.

1.1.3.5.3. Deve ser possível restringir o acesso à gerência do equipamento por, pelo menos, endereço IP e Rede.

1.1.3.5.4. Deve suportar SNMP v2 e v3.

1.1.3.5.5. Deve ser possível realizar captura de pacotes diretamente na gerência do equipamento.

1.1.3.5.6. Deve ser possível monitorar a utilização de CPU e memória diretamente na

gerência do equipamento.

1.1.3.5.7. Deve ser possível realizar a configuração do cluster diretamente na gerência do equipamento.

1.1.3.5.8. Deve ser possível conectar a serviços de DDNS;

1.1.3.5.9. Deve ser possível configurar o timeout da sessão do administrador na interface web.

1.1.3.5.10. Deve ser possível configurar a complexidade da senha do administrador e dias para expirar.

1.1.3.5.11. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logs.

1.1.3.5.12. A solução deve possibilitar ao administrador realizar a integração com o AD (Active Directory) através de um assistente de configuração na própria interface gráfica do produto;

1.1.3.5.13. A solução deve identificar usuários das seguintes fontes pelo menos:

1.1.3.5.14. Active Directory: o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

1.1.3.5.15. Autenticação via navegador: para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

1.1.3.5.16. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

1.1.3.5.17. Na integração com o AD, a operação de cadastro deve ser realizada na própria gerência do equipamento, de maneira simples e sem utilização de scripts de comando;

1.1.3.6. FUNCIONALIDADE DE PREVENÇÃO DE AMEAÇAS

1.1.3.6.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS integrados no próprio equipamento sem a necessidade de uso de quaisquer interfaces ou dispositivos externos.

1.1.3.6.2. Deve ser possível agendar para que o mecanismo de inspeção receba e implemente atualizações para os ataques emergentes sem a necessidade de reiniciar o equipamento;

1.1.3.6.3. Deve ser possível realizar a atualização manualmente sem necessidade de internet através da importação do pacote de atualização.

1.1.3.6.4. Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo, pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, força bruta, scanning de portas, CIFS Port overflow, Non Compliant DNS, Non Compliant SMTP, Non Compliant CIFS, Non Compliant MS

SQL Server, IKE aggressive Exchange;

1.1.3.6.5. Deve ser capaz de bloquear tráfego SSH em DNS tunneling;

1.1.3.6.6. A solução deverá ser capaz de inspecionar e proteger apenas hosts internos ou inspecionar todo o tráfego;

1.1.3.6.7. A solução deve proteger contra-ataques do tipo envenenamento de cache DNS (DNS Cache Poisoning);

1.1.3.6.8. A solução deverá possuir pelo menos dois perfis pré-configurados de fábrica para uso imediato e permitir a customização de um perfil;

1.1.3.6.9. Em cada proteção de segurança, devem estar inclusas informações como: categoria, tipo de impacto na ferramenta, severidade, e tipo de ação que a solução irá executar;

1.1.3.6.10. A solução de IPS deve possuir um modo de solução de problemas, que define o uso de perfil de detecção sem modificar as proteções individuais já criadas e customizadas;

1.1.3.6.11. Deve ser possível criar regras de exceção no IPS para que a solução não faça a inspeção de um tráfego específico por pelo menos proteção, origem, destino, serviço ou porta.

1.1.3.6.12. Deve ser possível visualizar a lista de proteções disponíveis no equipamento com os detalhes.

1.1.3.6.13. A solução deve incluir ferramenta própria ou solução de terceiros para mitigar/bloquear a comunicação entre os hosts infectados com bot e operador remoto (command & control).

1.1.3.6.14. A solução deve bloquear arquivos potencialmente maliciosos infectados com malware.

1.1.3.6.15. A solução de proteção contra malware e bot deve compartilhar a mesma política para facilitar o gerenciamento.

1.1.3.6.16. A solução de proteção contra malware e bot deve possuir um modo de solução de problemas, que define o uso de perfil de detecção, sem modificar as proteções individuais já criadas e customizadas;

1.1.3.6.17. As proteções devem ser ativadas baseadas em, pelo menos, critério de nível de confiança, ações da proteção e impacto de performance.

1.1.3.6.18. Deve ser possível habilitar a trilha das proteções para não logar, criar um log ou gerar um alerta;

1.1.3.6.19. Deve ser possível criar regras de exceção para que a solução não faça a inspeção de um tráfego específico por escopo, proteção e definir a ação e log para cada uma delas.

1.1.3.6.20. A solução de anti-malware deve suportar protocolos SMTP e P OP 3, FTP, HT TP em qualquer porta;

1.1.3.6.21. Deve ser possível definir uma política de inspeção para os tipos de arquivos por:

1.1.3.6.22. Inspecionar tipos de arquivos conhecidos que contenham malware;

1.1.3.6.23. Inspecionar todos os tipos de arquivos;

1.1.3.6.24. Inspecionar tipos de arquivos de famílias específicas;

1.1.3.6.25. Deve bloquear acesso a URLs com malware;

1.1.3.6.26. Deve ser possível customizar a página exibida para o usuário quando a URL contiver um malware e o acesso for bloqueado;

1.1.3.7. FILTRO DE CONTEÚDO WEB

1.1.3.7.1. A solução deverá contar com ferramentas de visibilidade e controle de aplicações web e filtro URL integrada no próprio appliance de segurança que permita a criação de políticas de liberação ou bloqueio baseando-se em aplicações web e URL;

1.1.3.7.2. A gerência das políticas de segurança de controle de aplicação e controle de URL's deverá ser realizada na mesma interface web de gerenciamento;

1.1.3.7.3. Deve ser possível configurar com apenas um clique o bloqueio a sites e aplicações que representem um risco de segurança e estão categorizadas como spyware, phishing, botnet, spam, anonymizer ou hacking.

1.1.3.7.4. Deve ser possível configurar com apenas um clique o bloqueio a sites com conteúdo inapropriado como sexo, violência, armas, jogos e álcool.

1.1.3.7.5. Deve configurar regras para permitir ou bloquear aplicações ou páginas da Internet por pelo menos:

1.1.3.7.5.1. Usuário do Active Directory

1.1.3.7.5.2. IP

1.1.3.7.5.3. Rede

1.1.3.7.6. Deve ser possível configurar o bloqueio de compartilhamento de arquivos com origem usualmente ilegais como aplicações torrents e peer-to-peer.

1.1.3.7.7. Deve ser possível configurar manualmente o bloqueio de aplicações ou categorias de sites de aplicações indesejadas.

1.1.3.7.8. Deve ainda ser possível adicionar uma URL ou aplicação que não está na base de dados.

1.1.3.7.9. Deve ser possível limitar o consumo de banda de aplicações.

1.1.3.7.10. A base de aplicações deve ser superior a 2900 aplicações, reconhecendo, pelo menos, as seguintes aplicações: bittorrent, gnutella, skype, facebook, linkedin, twitter, gmail, dropbox, whatsapp, etc;

1.1.3.7.11. Deve ser possível realizar a recategorização de uma URL através da gerência

do equipamento.

1.1.3.7.12. Deve ser possível customizar e definir a frequência com que serão exibidas as mensagens para os usuários nas seguintes ações:

1.1.3.7.12.1. Aceitar

1.1.3.7.12.2. Bloquear e informar

1.1.3.8. IDENTIFICAÇÃO DE USUÁRIOS

1.1.3.8.1. A solução deve ser capaz de trabalhar com identidades de usuários para propósitos de configurações e logging.

1.1.3.8.2. A solução deve possibilitar ao administrador realizar a integração com o AD através de um assistente de configuração na própria interface gráfica do produto;

1.1.3.8.3. A solução deve identificar usuários das seguintes fontes:

1.1.3.8.4. Active Directory o gateway de segurança deve realizar consulta aos servidores AD para obter informação dos usuários;

1.1.3.8.5. Autenticação via navegador para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador;

1.1.3.8.6. A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

1.1.3.8.7. Na integração com o AD, a operação de cadastro deve ser realizada na própria interface web de gerência, de maneira simples e sem utilização de scripts de comando;

1.1.3.9. FUNCIONALIDADES DE ACESSO REMOTO

1.1.3.9.1. A solução deve prover acesso seguro encriptado aos usuários remotos através da Internet;

1.1.3.9.2. A solução deve prover conectividade através de um cliente instalado no computador do usuário e através do navegador do usuário com conexão segura (HTTPS).

1.1.3.9.3. Deve suportar pelo menos os seguintes métodos de conexão:

1.1.3.9.4. Conexão através de cliente instalado no laptop ou desktop do usuário.

1.1.3.9.5. Conexão através de cliente instalado no smartphone e tablets.

1.1.3.9.6. Conexão através de navegador com SSL.

1.1.3.9.7. Conexão através de cliente nativo Windows L2TP.

1.1.3.9.8. Solução deve suportar alterar a porta padrão 443 para estabelecimento de VPN SSL.

1.1.3.9.9. A solução deve permitir conexão VPN aos seguintes usuários:

1.1.3.9.10. Usuários locais na própria base do appliance.

1.1.3.9.11. Grupos de usuários locais na própria base do appliance.

1.1.3.9.12. Grupos de usuários do Active Directory.

1.1.3.9.13. Grupos de usuários Radius.

1.1.3.9.14. A solução deve permitir atribuir um endereço específico para o usuário remoto.

1.1.3.10. FUNCIONALIDADE DE VPN SITE-TO-SITE

1.1.3.10.1. A solução deve prover acesso seguro criptografado entre duas localidades através da Internet;

1.1.3.10.2. A solução deve estabelecer VPN com o site remoto do próprio fabricante ou de terceiros;

1.1.3.10.3. A solução deve suportar autenticação com senha ou certificado;

1.1.3.10.4. Deve suportar, pelo menos, criptografia AES 128 e 256;

1.1.3.10.5. Deve possuir mecanismo para monitorar a saúde do túnel remoto;

1.1.3.11. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

1.1.3.11.1. Suportar a criação de políticas de QoS por:

1.1.3.11.2. Endereço de origem, endereço de destino e por porta;

1.1.3.11.3. O QoS deve possibilitar a definição de classes por:

1.1.3.11.4. Banda garantida, banda máxima e fila de prioridade;

1.1.3.11.5. Disponibilizar estatísticas em tempo real para classes de QoS;

1.1.3.11.6. A solução deve permitir, por aplicação, o encaminhamento do tráfego para diferentes links de Internet, sejam eles locais ou remotos, deve suportar múltiplos links de acesso como MPLS, Internet Banda Larga, LTE e Satélite.

1.1.3.11.7. Deve possibilitar a utilização de configuração inteligente de acessos WAN IP ativos-ativos sem a necessidade de switch para agregação WAN, ou seja, distribuir o tráfego simultaneamente pelos N acessos conectados e não apenas na configuração dos acessos principal e backup.

1.1.3.11.8. Medir parâmetros de rede jitter, perda de pacotes e latência em tempo real.

1.1.3.11.9. Se houver necessidade de saída internet do ponto remoto, deve ser possível selecionar por tipo de aplicativo;

1.1.3.11.10. Deve permitir a comunicação indireta entre localidades por meio de uma topologia “hub and spoke”;

1.1.3.11.11. Deve balancear o tráfego de aplicativos em vários links simultaneamente;

1.1.3.11.12. Redistribuição do tráfego balanceado, de forma inteligente, tendo em conta o congestionamento da largura de banda, entre os links utilizados, em caso de falhas nestes links, ou de acordo com as políticas de qualidade pré-definidas;

1.1.3.11.13. Habilitar a criação de políticas de negócios para controlar o padrão de redirecionamento de tráfego e aplicar qualidade de serviço;

1.1.3.11.14. Suportar o redirecionamento do tráfego de internet de pontos remotos para um ponto de internet centralizado, usando políticas por aplicativo;

1.1.3.11.15. Redirecionamento condicionado do tráfego de internet em caso de falha do link de internet local ou do link remoto centralizado, utilizando políticas por aplicativo;

1.1.3.11.16. Suporte simultâneo ao redirecionamento do tráfego da Web de alguns aplicativos para a Internet centralizada, outros aplicativos para a Internet local e outros aplicativos para inspeção avançada de segurança na nuvem.

1.1.3.11.17. Deve ser capaz de criar um túnel otimizado que proteja os aplicativos TCP e UDP contra jitter e perda de pacotes para garantir desempenho de ponta a ponta para áudio, vídeo e tráfego transacional;

1.1.3.11.18. Usar probes artificiais baseadas em ICMP, UDP ou TCP para medir a qualidade da rede percebida pelo tráfego do usuário, medindo no minimo jitter, latencia e perda de pacotes.

1.1.3.11.19. Capacidade de realizar agregação de largura de banda automaticamente entre links de diferentes velocidades, levando em consideração o uso total da largura de banda de cada link sem causar congestionamento em links de baixa velocidade.

1.1.3.11.20. Habilitar a configuração de backup do link, ou seja, um link de backup só deve ser ativado quando o link principal falhar.

1.1.3.11.21. Implementar um mecanismo de proteção de variação de latência (jitter) mesmo que a degradação esteja em todos os links, para proteger o tráfego em tempo real (voz e vídeo).

1.1.3.11.22. Garantir o desempenho de aplicativos em um cenário de link de transporte duplo quando ambos os links estão degradados simultaneamente

1.1.3.11.23. Possuir um mecanismo de priorização (QoS) para proteger o tráfego de aplicativos clientes prioritários quando houver congestionamento em pontos remotos

1.1.3.11.24. Deve automatizar o reconhecimento dos melhores níveis de SLA de rede com base no tipo de tráfego seja áudio, vídeo ou transacional.

1.1.3.11.25. O console de gerenciamento deve informar o status operacional (UP/DOWN/SPEED) das interfaces LAN e WAN

1.1.3.11.26. O console de gerenciamento deve informar o status operacional de cada dispositivo que faz parte da rede para operacionalidade

1.1.3.11.27. Realizar medições de “Latência” /”Jitter”/”Queda de pacotes” em cada um dos túneis SDWAN independentemente, na direção de transmissão ou recepção

1.1.3.11.28. O orquestrador pode estar na nuvem do fabricante ou até mesmo ser instalado em um servidor dedicado ou virtualizado, utilizando uma máquina virtual

1.1.3.11.29. No caso de o orquestrador estar na nuvem, a administração de atualizações, gerenciamento de alta disponibilidade e hardening do plano de gerenciamento deve ser realizada pelo fabricante da solução;

1.1.3.12. PREVENÇÃO DE AMEAÇAS AVANÇADAS

1.1.3.12.1. A solução deve incluir ferramenta própria ou solução de terceiros para proteção de redes contra ameaças desconhecidas em arquivos que são baixados da Internet ou anexados a e-mails.

1.1.3.12.2. A solução deve compartilhar a mesma política da proteção contra vírus e bot para facilitar o gerenciamento.

1.1.3.12.3. A solução deve trabalhar em modo de prevenção e não apenas detecção.

1.1.3.12.4. Deve permitir criar uma lista de exceção de e-mails que não devem ter seus anexos inspecionados.

1.1.3.12.5. Deve permitir criar uma lista de exceção para arquivos que não devem ser inspecionados.

1.1.3.12.6. A solução deve suportar protocolos SMTP, HTTP em qualquer porta;

1.1.3.12.7. Deve permitir configurar por tipo de arquivo as ações de inspeção ou bypass.

1.1.3.12.8. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliance através de assinaturas

1.1.3.12.9. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF com tamanho até 15 Mb.

1.1.3.12.10. Deve permitir configurar como uma emulação em conexão http será tratada, sendo permitida até que a emulação seja concluída ou bloqueada até a emulação ser completa.

1.1.3.13. SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO

1.1.3.13.1. A solução deve ser fornecida incluindo solução de gerenciamento centralizado conforme características e especificações descritas no ANEXO C;

1.1.4. SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 4

1.1.4.1. SERVIÇO DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM

1.1.4.1.1. A solução deve ser fornecida incluindo disponibilização de equipamento e software, instalação, configuração e testes conforme características e especificações descritas no ANEXO D;

1.1.4.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.4.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO F;

1.1.4.3. CARACTERÍSTICAS GERAIS

1.1.4.3.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.4.3.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

1.1.4.3.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;

1.1.4.3.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

1.1.4.3.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.4.3.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.4.3.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.4.4. CAPACIDADES E QUANTIDADES

1.1.4.4.1. Throughput de no mínimo 6.4 (seis ponto quatro) Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, anti-bot/anti-spyware e prevenção de ameaças avançadas de dia zero;

1.1.4.4.2. Suporte a, no mínimo, 15.000.000 (quinze milhões) de conexões ou sessões simultâneas;

1.1.4.4.3. Suporte a, no mínimo, 235.000 (duzentas e trinta e cinco mil) novas conexões ou sessões por segundo;

1.1.4.4.4. Throughput de, no mínimo, 18 (dezoito) Gbps, no mínimo, para conexões VPN;

1.1.4.4.5. Deve possuir fonte de alimentação redundante;

1.1.4.4.6. Deve suportar futuramente, pelo menos, 11 contextos virtuais;

1.1.4.4.7. Caso a solução permita expansão de memória RAM, deve vir com o máximo de memória possível;

1.1.4.4.8. Deve possuir, no mínimo, 08 (oito) interfaces de rede 1/10Gbps SFP+;

1.1.4.4.9. Deve possuir, no mínimo, 08 (oito) interfaces de rede 1Gbps RJ-45;

1.1.4.4.10. Possuir 1 (uma) interface de rede dedicada para sincronismo;

1.1.4.4.11. Possuir 1 (uma) interface de rede dedicada ao gerenciamento, não sendo

permitido utilizar qualquer outra interface para exercer a função de gerenciamento do equipamento;

1.1.4.4.12. Possuir 1 (uma) interface do tipo console ou similar;

1.1.4.4.13. Possuir interface dedicada e física para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo não responde. Caso o equipamento não possua essa interface física/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração via software ou uso da interface dedicada de gerenciamento.

1.1.4.4.14. Deve possuir armazenamento interno SSD de, no mínimo, 480GB;

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

1.1.4.4.16. Suporte a RFC 4291 de arquitetura de endereçamento IPv6;

1.1.4.4.17. Suportar configurar IPv6 em Dual Stack em uma interface bond/agregação. Essa configuração também poderá ser realizada em uma subinterface de bond/agregação;

1.1.4.4.18. Deve suportar NAT64 e NAT46;

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

1.1.4.4.20. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IPv4 e IPv6 sem duplicação da base de objetos e regras;

1.1.4.4.21. Deve suportar operar em cluster ativo-passivo ou ativo-ativo sem a necessidade de licenças adicionais;

1.1.4.4.22. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

1.1.4.5. FUNCIONALIDADES DE FIREWALL

1.1.4.5.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

1.1.4.5.2. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;

1.1.4.5.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.1.4.5.4. A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

1.1.4.5.5. Realizar upgrade via SCP, SFTP e https via interface WEB;

1.1.4.5.6. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.1.4.5.6.1. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;

1.1.4.5.6.2. Deverá suportar VXLAN;

1.1.4.5.7. Deve suportar os seguintes tipos de NAT:

1.1.4.5.7.1. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

1.1.4.5.8. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

1.1.4.5.9. As regras de NAT devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra;

1.1.4.5.10. Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizavéis de forma dinâmica, por exemplo: Office 365, AWS, Azure e outros. Ou seja, objetos dinâmicos que não se caracterizam como FQDN;

1.1.4.5.11. Enviar logs para sistemas de monitoração externos, simultaneamente;

1.1.4.5.12. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

1.1.4.5.13. Deve realizar roteamentos unicast e multicast simultaneamente em uma única instância (contexto) de firewall.

1.1.4.5.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

1.1.4.5.15. Suportar OSPF graceful restart;

1.1.4.5.16. Deve suportar roteamento ECMP (equal cost multi-path);

1.1.4.5.17. Para o ECMP, a solução deve suportar o balanceamento do roteamento de forma simultanea usando os seguintes parametros Origem, Destino, Porta de Origem, Porta de Destino e Protocolo;

1.1.4.5.18. Autenticação integrada via Kerberos.

1.1.4.5.19. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções/ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação

de política para solução solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, FTP, acesso WEB, alterações de política, comunicação SNMP.

1.1.4.5.20. As regras de firewall devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra;

1.1.4.5.21. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;

1.1.4.5.22. A solução deve ter a capacidade de operar através de uma unica instância de firewall de forma simultânea mediante o uso das suas interfaces fisicas nos seguintes modos: transparente, modo sniffer (monitoramento e análise o trafego de rede), camada 2 (L2) e camada 3 (L3);

1.1.4.5.23. A solução deve permitir salvar as configurações das políticas para serem aplicadas em horarios pré-definidos;

1.1.4.5.24. Deve possuir mecanismo de ativação de validada da regra com período customizado;

1.1.4.5.25. Deverá suportar redundância e balancemento de links, tendo capacidade para no mínimo 3 links de internet;

1.1.4.5.26. Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento;

1.1.4.5.27. Deve permitir a configuração do tempo de checagem para cada um dos links.

1.1.4.6. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

1.1.4.6.1. Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

1.1.4.6.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

1.1.4.6.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3

1.1.4.6.4. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.1.4.6.5. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

1.1.4.6.5.1. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

1.1.4.6.5.2. Reconhecer pelo menos 3.000 (três 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;

1.1.4.6.6. A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

1.1.4.6.7. Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE)

1.1.4.6.8. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

1.1.4.6.9. 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;

1.1.4.6.10. A fim de otimização de tempo operacional dos administrdores, a solução deverá possuir pelo menos 150 categorias de aplicações WEB pré-definidas pelo fabricante;

1.1.4.6.11. Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer.);

1.1.4.6.12. A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

1.1.4.6.13. Atualizar a base de assinaturas de aplicações automaticamente;

1.1.4.6.14. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

1.1.4.6.15. Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas entre elas usuários, IP, grupos de usuários do sistema do Active Directory;

1.1.4.6.16. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

1.1.4.6.17. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

1.1.4.6.18. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

1.1.4.6.19. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

1.1.4.6.19.1. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da

semana e hora);

1.1.4.6.19.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

1.1.4.6.19.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

1.1.4.6.19.4. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

1.1.4.6.19.5. Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;

1.1.4.6.19.6. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;

1.1.4.6.19.7. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

1.1.4.6.19.8. Suportar a criação de categorias de URLs customizadas;

1.1.4.6.19.9. Suportar a exclusão de URLs do bloqueio, por categoria;

1.1.4.6.19.10. Permitir a customização de página de bloqueio;

1.1.4.6.20. 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, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

1.1.4.6.21. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou API’s ou Syslog, para a identificação de endereços IP e usuários;

1.1.4.6.22. Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

1.1.4.7. FUNCIONALIDADE DE FILTRO DE DADOS

1.1.4.7.1. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos e expressões reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de arquivos:

1.1.4.7.1.1. Número de cartão de crédito;

1.1.4.7.1.2. Código fonte JAVA;

1.1.4.7.1.3. Arquivo PDF;

1.1.4.7.1.4. Arquivo executável;

1.1.4.7.1.5. Arquivo de banco de dados;

1.1.4.7.2. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload".

1.1.4.7.3. A solução de controle de dados deve permir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima seja feito.

1.1.4.7.4. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

1.1.4.8. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

1.1.4.8.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

1.1.4.8.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

1.1.4.8.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/passivo;

1.1.4.8.4. Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

1.1.4.8.5. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

1.1.4.8.6. Deverá possuir os seguintes mecanismos de inspeção de IPS:

1.1.4.8.6.1. Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

1.1.4.8.7. Detectar e bloquear a origem de portscans;

1.1.4.8.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

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

1.1.4.8.10. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

1.1.4.8.11. Suportar bloqueio de arquivos por tipo;

1.1.4.8.12. Identificar e bloquear comunicação com botnets;

1.1.4.8.13. Deve suportar referência cruzada com CVE;

1.1.4.8.14. Em cada proteção de segurança, deve estar incluso informações como:

1.1.4.8.14.1. Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro codigo de referência;

1.1.4.8.14.2. Severidade;

1.1.4.8.14.3. Tipo de ação a ser executada.

1.1.4.8.15. O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.

1.1.4.8.16. O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.

1.1.4.8.17. O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.

1.1.4.8.18. O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor)

1.1.4.8.19. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.1.4.8.19.1. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

1.1.4.8.20. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

1.1.4.8.21. Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual;

1.1.4.8.22. A solução de IPS, deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas que estão em modo detecção devem ser alterada para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.

1.1.4.8.23. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;

1.1.4.8.24. A solução deverá possuir pelo menos dois perfis pré-configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;

1.1.4.8.25. A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.

1.1.4.8.26. Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

1.1.4.8.27. Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados;

1.1.4.8.28. O gerenciamento centralizado via interface gráfica, deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento;

1.1.4.8.29. A solução de IPS deve possuir mecanismo onde irá determinar de forma automática, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual;

1.1.4.8.30. O anti-vírus ou outra funcionalidade deve oferecer suporte à verificação de links dentro de e-mails;

1.1.4.8.31. A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso

1.1.4.8.32. A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;

1.1.4.8.33. Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;

1.1.4.8.34. A solução deve permitir a criação de allow-list baseado no MD5 do arquivo;

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

1.1.4.8.36. Suportar rastreamento de vírus em arquivos pdf;

1.1.4.8.37. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

1.1.4.8.38. Possuir a capacidade de prevenção de ameaças não conhecidas;

1.1.4.8.39. Em caso de falha no mecanismo de inspeção do anti-vírus/anti-malware, deve ser possível configurar se as conexões serão permitidas ou bloqueada

1.1.4.8.40. A solução de anti-vírus/anti-malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);

1.1.4.8.41. A solução deverá suportar análise de arquivos que tráfegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede;

1.1.4.8.42. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

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

acessos;

1.1.4.8.44. A solução deverá possuir mecanismo de “machine learning” para prevenção de ataques de DNS do tipo DGA (Domain Generation Algorithm), não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

1.1.4.8.45. A solução deverá possuir mecanismo de “machine learning” para prevenção de ataques de DNS Tunneling, não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

1.1.4.8.46. Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

1.1.4.8.47. A solução de anti-malware/anti-vírus deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

1.1.4.8.48. A solução deve possuir funcionalidade de identificação de bloqueio de tráfego malicioso comunicando com C&C (command & control);

1.1.4.9. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

1.1.4.9.1. Suportar a criação de políticas de QoS por:

1.1.4.9.1.1. Endereço de origem, endereço de destino e por porta;

1.1.4.9.2. O QoS deve possibilitar a definição de classes por:

1.1.4.9.2.1. Banda garantida, banda máxima e fila de prioridade;

1.1.4.9.3. Disponibilizar estatísticas em tempo real para classes de QoS;

1.1.4.10. FUNCIONALIDADES DE VPN

1.1.4.10.1. Suportar VPN site-to-site e client-to-site;

1.1.4.10.2. Suportar IPSec VPN;

1.1.4.10.3. A solução deve suportar Autoridade Certificadora Interna e Externa (de terceiros);

1.1.4.10.4. Suportar SSL VPN;

1.1.4.10.5. A VPN IPSEc deve suportar:

1.1.4.10.5.1. 3DES, Autenticação MD5, SHA-1, SHA-384, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard), SHA-512 e Autenticação via certificado IKE PKI;

1.1.4.10.6. A VPN SSL deve suportar:

1.1.4.10.6.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB ;

1.1.4.10.6.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

1.1.4.10.6.3. Suportar configuração de comformidade para acesso do usuário via portal SSL ou cliente na máquina do usuário;

1.1.4.10.6.4. Atribuição de endereço IP nos clientes remotos de VPN;

1.1.4.10.6.5. Atribuição de DNS nos clientes remotos de VPN;

1.1.4.10.6.6. Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

1.1.4.10.7. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

1.1.4.11. SOLUÇÃO PARA PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS – ZERO DAY

1.1.4.11.1. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

1.1.4.11.2. A solução deverá ser composta por hardware e software específicos (appliance) com sistema operacional especializado em sua versão mais atualizada ou nuvem do próprio fabricante que possua o conceito de sandboxing para prevenção de ataques zero-day.

1.1.4.11.3. Não serão aceitas soluções que dependam da estrutura de hypervisor do contratante para a análise de ameaças de dia zero, como Vmware ESXi, Microsoft HyperV, entre outros;

1.1.4.11.4. A solução deverá operar em modo MTA (Mail Transfer Agent) para proteção de malware desconhecido de dia zero.

1.1.4.11.5. Inspecionar de forma efetiva o malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS), FTP e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandboxing;

1.1.4.11.6. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

1.1.4.11.7. Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URLs conhecidas;

1.1.4.11.8. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP, Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

1.1.4.11.9. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente;

1.1.4.11.10. O conteúdo enviado para a solução de sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador

para que o processo de análise seja realizado;

1.1.4.11.11. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

1.1.4.11.12. A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;

1.1.4.11.13. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF acima de 10 Mb;

1.1.4.11.14. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e criptografados em SSL;

1.1.4.11.15. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos java (.jar e class);

1.1.4.11.16. A solução deve suportar inspeção para o protocolo SMBv3;

1.1.4.11.17. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

1.1.4.11.18. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

1.1.4.11.19. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm e gz;

1.1.4.11.20. A solução deve permitir a criação de allow-lists baseado no MD5 do arquivo;

1.1.4.11.21. A solução deve possuir mecanismo para identificar sites conhecidos e desconhecidos como phishing, analisando em tempo real a URL acessada.

1.1.4.11.22. A solução deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas informações em sites classificados como phishing;

1.1.4.11.23. O Mecanismo de classificação de anti-phising deve atuar sem a necessidade de instalação de agente na máquina do usuário;

1.1.4.11.24. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

1.1.4.11.24.1. Número de arquivos emulados;

1.1.4.11.24.2. Numero de arquivos com malware.

1.1.4.11.25. A solução deve prover informação, seja por meio de relatório ou log, sobre as

seguintes situações:

1.1.4.11.25.1. O tamanho máximo do arquivo emulado seja excedido;

1.1.4.11.25.2. O tempo máximo de emulação seja excedido.

1.1.5. SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 5

1.1.5.1. SERVIÇO DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM

1.1.5.1.1. A solução deve ser fornecida incluindo disponibilização de equipamento e software, instalação, configuração e testes conforme características e especificações descritas no ANEXO D;

1.1.5.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.5.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO F;

1.1.5.3. CARACTERÍSTICAS GERAIS

1.1.5.3.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.5.3.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

1.1.5.3.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;

1.1.5.3.4. A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

1.1.5.3.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.5.3.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.5.3.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.5.4. CAPACIDADES E QUANTIDADES

1.1.5.4.1. Throughput de no mínimo 10.5 (dez ponto cinco) Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, anti-bot/anti-spyware e prevenção de ameaças avançadas de dia zero;

1.1.5.4.2. Suporte a, no mínimo, 15.000.000 (quinze milhões) de conexões ou sessões simultâneas;

1.1.5.4.3. Suporte a, no mínimo, 340.000 (trezentas e quarenta mil) novas conexões ou sessões por segundo;

1.1.5.4.4. Throughput de, no mínimo, 25 (vinte e cinco) Gbps, no mínimo, para conexões VPN;

1.1.5.4.5. Deve possuir fonte de alimentação redundante;

1.1.5.4.6. Deve suportar futuramente, pelo menos, 11 contextos virtuais;

1.1.5.4.7. Caso a solução permita expansão de memória RAM, deve vir com o máximo de memória possível;

1.1.5.4.8. Deve possuir, no mínimo, 10 (dez) interfaces de rede 1/10Gbps SFP+;

1.1.5.4.9. Deve possuir, no mínimo, 08 (oito) interfaces de rede 1Gbps RJ-45;

1.1.5.4.10. Possuir 1 (uma) interface de rede dedicada para sincronismo;

1.1.5.4.11. Possuir 1 (uma) interface de rede dedicada ao gerenciamento, não sendo permitido utilizar qualquer outra interface para exercer a função de gerenciamento do equipamento;

1.1.5.4.12. Possuir 1 (uma) interface do tipo console ou similar;

1.1.5.4.13. Possuir interface dedicada e fisica para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo não responde. Caso o equipamento não possua essa interface fisica/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração via software ou uso da interface dedicada de gerenciamento.

1.1.5.4.14. Deve possuir armazenamento interno SSD de, no mínimo, 960GB;

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

1.1.5.4.16. Suporte a RFC 4291 de arquitetura de endereçamento IPv6;

1.1.5.4.17. Suportar configurar IPv6 em Dual Stack em uma interface bond/agregação. Essa configuração também poderá ser realizada em uma subinterface de bond/agregação;

1.1.5.4.18. Deve suportar NAT64 e NAT46;

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

1.1.5.4.20. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IPv4 e IPv6 sem duplicação da base de objetos e regras;

1.1.5.4.21. Deve suportar operar em cluster ativo-passivo ou ativo-ativo sem a necessidade de licenças adicionais;

1.1.5.4.22. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

1.1.5.5. FUNCIONALIDADES DE FIREWALL

1.1.5.5.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

1.1.5.5.2. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;

1.1.5.5.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.1.5.5.4. A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

1.1.5.5.5. Realizar upgrade via SCP, SFTP e https via interface WEB;

1.1.5.5.6. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.1.5.5.6.1. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;

1.1.5.5.6.2. Deverá suportar VXLAN;

1.1.5.5.7. Deve suportar os seguintes tipos de NAT:

1.1.5.5.7.1. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

1.1.5.5.8. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

1.1.5.5.9. As regras de NAT devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra;

1.1.5.5.10. Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizavéis de forma dinâmica, por exemplo: Office 365, AWS, Azure e outros. Ou seja, objetos dinâmicos que não se caracterizam como FQDN;

1.1.5.5.11. Enviar logs para sistemas de monitoração externos, simultaneamente;

1.1.5.5.12. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

1.1.5.5.13. Deve realizar roteamentos unicast e multicast simultaneamente em uma única

instância (contexto) de firewall.

1.1.5.5.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

1.1.5.5.15. Suportar OSPF graceful restart;

1.1.5.5.16. Deve suportar roteamento ECMP (equal cost multi-path);

1.1.5.5.17. Para o ECMP, a solução deve suportar o balanceamento do roteamento de forma simultanea usando os seguintes parametros Origem, Destino, Porta de Origem, Porta de Destino e Protocolo;

1.1.5.5.18. Autenticação integrada via Kerberos.

1.1.5.5.19. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções/ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, FTP, acesso WEB, alterações de política, comunicação SNMP.

1.1.5.5.20. As regras de firewall devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra;

1.1.5.5.21. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;

1.1.5.5.22. A solução deve ter a capacidade de operar através de uma unica instância de firewall de forma simultânea mediante o uso das suas interfaces fisicas nos seguintes modos: transparente, modo sniffer (monitoramento e análise o trafego de rede), camada 2 (L2) e camada 3 (L3);

1.1.5.5.23. A solução deve permitir salvar as configurações das políticas para serem aplicadas em horarios pré-definidos;

1.1.5.5.24. Deve possuir mecanismo de ativação de validada da regra com período customizado;

1.1.5.5.25. Deverá suportar redundância e balancemento de links, tendo capacidade para no mínimo 3 links de internet;

1.1.5.5.26. Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento;

1.1.5.5.27. Deve permitir a configuração do tempo de checagem para cada um dos links.

1.1.5.6. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

1.1.5.6.1. Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

1.1.5.6.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

1.1.5.6.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3

1.1.5.6.4. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.1.5.6.5. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

1.1.5.6.5.1. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

1.1.5.6.5.2. Reconhecer pelo menos 3.000 (três 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;

1.1.5.6.6. A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

1.1.5.6.7. Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE)

1.1.5.6.8. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

1.1.5.6.8.1. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

1.1.5.6.9. 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;

1.1.5.6.10. A fim de otimização de tempo operacional dos administrdores, a solução deverá possuir pelo menos 150 categorias de aplicações WEB pré-definidas pelo fabricante;

1.1.5.6.11. Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer.);

1.1.5.6.12. A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

1.1.5.6.13. Atualizar a base de assinaturas de aplicações automaticamente;

1.1.5.6.14. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

1.1.5.6.15. Os dispositivos de proteção de rede devem possuir a capacidade de identificar

de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas entre elas usuários, IP, grupos de usuários do sistema do Active Directory;

1.1.5.6.16. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

1.1.5.6.17. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

1.1.5.6.18. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

1.1.5.6.19. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

1.1.5.6.19.1. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.1.5.6.19.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

1.1.5.6.19.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

1.1.5.6.19.4. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

1.1.5.6.19.5. Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;

1.1.5.6.19.6. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;

1.1.5.6.19.7. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

1.1.5.6.19.8. Suportar a criação de categorias de URLs customizadas;

1.1.5.6.19.9. Suportar a exclusão de URLs do bloqueio, por categoria;

1.1.5.6.19.10. Permitir a customização de página de bloqueio;

1.1.5.6.20. 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, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

1.1.5.6.21. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou API's ou Syslog, para a identificação de endereços IP e usuários;

1.1.5.6.22. Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

1.1.5.7. FUNCIONALIDADE DE FILTRO DE DADOS

1.1.5.7.1. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos e expressões reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de arquivos:

1.1.5.7.1.1. Número de cartão de crédito;

1.1.5.7.1.2. Código fonte JAVA;

1.1.5.7.1.3. Arquivo PDF;

1.1.5.7.1.4. Arquivo executável;

1.1.5.7.1.5. Arquivo de banco de dados;

1.1.5.7.2. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload".

1.1.5.7.3. A solução de controle de dados deve permir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima seja feito.

1.1.5.7.4. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

1.1.5.8. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

1.1.5.8.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

1.1.5.8.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

1.1.5.8.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/passivo;

1.1.5.8.4. Deve suportar granularidade nas políticas de Antivírus e Anti-malware,

possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

1.1.5.8.5. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

1.1.5.8.6. Deverá possuir os seguintes mecanismos de inspeção de IPS:

1.1.5.8.6.1. Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

1.1.5.8.7. Detectar e bloquear a origem de portscans;

1.1.5.8.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

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

1.1.5.8.10. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

1.1.5.8.11. Suportar bloqueio de arquivos por tipo;

1.1.5.8.12. Identificar e bloquear comunicação com botnets;

1.1.5.8.13. Deve suportar referência cruzada com CVE;

1.1.5.8.14. Em cada proteção de segurança, deve estar incluso informações como:

1.1.5.8.14.1. Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro codigo de referência;

1.1.5.8.14.2. Severidade;

1.1.5.8.14.3. Tipo de ação a ser executada.

1.1.5.8.15. O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.

1.1.5.8.16. O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.

1.1.5.8.17. O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.

1.1.5.8.18. O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor)

1.1.5.8.19. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.1.5.8.19.1. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

1.1.5.8.20. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-

Malware, através da console de gerência centralizada;

1.1.5.8.21. Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual;

1.1.5.8.22. A solução de IPS, deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas que estão em modo detecção devem ser alterada para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.

1.1.5.8.23. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;

1.1.5.8.24. A solução deverá possuir pelo menos dois perfis pré-configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;

1.1.5.8.25. A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.

1.1.5.8.26. Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

1.1.5.8.27. Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados;

1.1.5.8.28. O gerenciamento centralizado via interface gráfica, deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento;

1.1.5.8.29. A solução de IPS deve possuir mecanismo onde irá determinar de forma automática, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual;

1.1.5.8.30. O anti-vírus ou outra funcionalidade deve oferecer suporte à verificação de links dentro de e-mails;

1.1.5.8.31. A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso

1.1.5.8.32. A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;

1.1.5.8.33. Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;

1.1.5.8.34. A solução deve permitir a criação de allow-list baseado no MD5 do arquivo;

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

1.1.5.8.36. Suportar rastreamento de vírus em arquivos pdf;

1.1.5.8.37. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

1.1.5.8.38. Possuir a capacidade de prevenção de ameaças não conhecidas;

1.1.5.8.39. Em caso de falha no mecanismo de inspeção do anti-vírus/anti-malware, deve ser possível configurar se as conexões serão permitidas ou bloqueada

1.1.5.8.40. A solução de anti-vírus/anti-malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);

1.1.5.8.41. A solução deverá suportar análise de arquivos que tráfegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede;

1.1.5.8.42. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

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

1.1.5.8.44. A solução deverá possuir mecanismo de “machine learning” para prevenção de ataques de DNS do tipo DGA (Domain Generation Algorithm), não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

1.1.5.8.45. A solução deverá possuir mecanismo de “machine learning” para prevenção de ataques de DNS Tunneling, não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

1.1.5.8.46. Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

1.1.5.8.47. A solução de anti-malware/anti-vírus deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

1.1.5.8.48. A solução deve possuir funcionalidade de identificação de bloqueio de tráfego malicioso comunicando com C&C (command & control);

1.1.5.9. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

1.1.5.9.1. Suportar a criação de políticas de QoS por:

1.1.5.9.1.1. Endereço de origem, endereço de destino e por porta;

1.1.5.9.2. O QoS deve possibilitar a definição de classes por:

1.1.5.9.2.1. Banda garantida, banda máxima e fila de prioridade;

1.1.5.9.3. Disponibilizar estatísticas em tempo real para classes de QoS;

1.1.5.10. FUNCIONALIDADES DE VPN

1.1.5.10.1. Suportar VPN site-to-site e client-to-site;

1.1.5.10.2. Suportar IPSec VPN;

1.1.5.10.3. A solução deve suportar Autoridade Certificadora Interna e Externa (de terceiros);

1.1.5.10.4. Suportar SSL VPN;

1.1.5.10.5. A VPN IPSEc deve suportar:

1.1.5.10.5.1. 3DES, Autenticação MD5, SHA-1, SHA-384, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard), SHA-512 e Autenticação via certificado IKE PKI;

1.1.5.10.6. A VPN SSL deve suportar:

1.1.5.10.6.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB ;

1.1.5.10.6.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

1.1.5.10.6.3. Suportar configuração de comformidade para acesso do usuário via portal SSL ou cliente na máquina do usuário;

1.1.5.10.6.4. Atribuição de endereço IP nos clientes remotos de VPN;

1.1.5.10.6.5. Atribuição de DNS nos clientes remotos de VPN;

1.1.5.10.6.6. Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

1.1.5.10.7. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

1.1.5.11. SOLUÇÃO PARA PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS – ZERO DAY

1.1.5.11.1. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

1.1.5.11.2. A solução deverá ser composta por hardware e software específicos (appliance) com sistema operacional especializado em sua versão mais atualizada ou nuvem do próprio fabricante que possua o conceito de sandboxing para prevenção de ataques zero-day.

1.1.5.11.3. Não serão aceitas soluções que dependam da estrutura de hypervisor do contratante para a análise de ameaças de dia zero, como Vmware ESXi, Microsoft HyperV, entre outros;

1.1.5.11.4. A solução deverá operar em modo MTA (Mail Transfer Agent) para proteção de malware desconhecido de dia zero.

1.1.5.11.5. Inspecionar de forma efetiva o malware desconhecido (Dia Zero), oriundo da

comunicação Web (HTTP e HTTPS), FTP e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandboxing;

1.1.5.11.6. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

1.1.5.11.7. Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URLs conhecidas;

1.1.5.11.8. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP, Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

1.1.5.11.9. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente;

1.1.5.11.10. O conteúdo enviado para a solução de sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado;

1.1.5.11.11. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

1.1.5.11.12. A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;

1.1.5.11.13. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF acima de 10 Mb;

1.1.5.11.14. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e criptografados em SSL;

1.1.5.11.15. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos java (.jar e class);

1.1.5.11.16. A solução deve suportar inspeção para o protocolo SMBv3;

1.1.5.11.17. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

1.1.5.11.18. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

1.1.5.11.19. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb,

xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm e gz;

1.1.5.11.20. A solução deve permitir a criação de allow-lists baseado no MD5 do arquivo;

1.1.5.11.21. A solução deve possuir mecanismo para identificar sites conhecidos e desconhecidos como phishing, analisando em tempo real a URL acessada.

1.1.5.11.22. A solução deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas informações em sites classificados como phishing;

1.1.5.11.23. O Mecanismo de classificação de anti-phising deve atuar sem a necessidade de instalação de agente na máquina do usuário;

1.1.5.11.24. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

1.1.5.11.24.1. Número de arquivos emulados;

1.1.5.11.24.2. Número de arquivos com malware.

1.1.5.11.25. A solução deve prover informação, seja por meio de relatório ou log, sobre as seguintes situações:

1.1.5.11.25.1. O tamanho máximo do arquivo emulado seja excedido;

1.1.5.11.25.2. O tempo máximo de emulação seja excedido.

1.1.6. SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 6

1.1.6.1. SERVIÇO DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM

1.1.6.1.1. A solução deve ser fornecida incluindo disponibilização de equipamento e software, instalação, configuração e testes conforme características e especificações descritas no ANEXO D;

1.1.6.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.6.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO F;

1.1.6.3. CARACTERÍSTICAS GERAIS

1.1.6.3.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.6.3.2. A solução deverá ser compatível com SNMPv2 e SNMPv3;

1.1.6.3.3. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos equipamentos desde que obedeçam a todos os requisitos desta especificação;

1.1.6.3.4. A comunicação entre os appliances de segurança e o módulo de gerência deve

ser através de meio criptografado;

1.1.6.3.5. Os appliances de segurança devem suportar operar em cluster ativo-ativo e ativo-passivo sem a necessidade de licenças adicionais;

1.1.6.3.6. Não serão aceitos modelos em listas de end-of-sale, cuja data do fim de vendas seja anterior à data da proposta.

1.1.6.3.7. Não serão aceitos modelos em lista de end-of-support, cuja data do fim do suporte seja anterior ao fim da vigência do contrato e/ou do fim do período de garantia e suporte exigido no edital.

1.1.6.4. CAPACIDADES E QUANTIDADES

1.1.6.4.1. Throughput de no mínimo 16 (dezesseis) Gbps, com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, filtro de URL, antivírus, anti-bot/anti-spyware e prevenção de ameaças avançadas de dia zero;

1.1.6.4.2. Suporte a, no mínimo, 25.000.000 (vinte e cinco milhões) de conexões ou sessões simultâneas;

1.1.6.4.3. Suporte a, no mínimo, 500.000 (quinhentas mil) novas conexões ou sessões por segundo;

1.1.6.4.4. Throughput de, no mínimo, 25 (vinte e cinco) Gbps, no mínimo, para conexões VPN;

1.1.6.4.5. Deve possuir fonte de alimentação redundante;

1.1.6.4.6. Deve suportar futuramente, pelo menos, 15 contextos virtuais;

1.1.6.4.7. Caso a solução permita expansão de memória RAM, deve vir com o máximo de memória possível;

1.1.6.4.8. Deve possuir, no mínimo, 10 (dez) interfaces de rede 1/10Gbps SFP+;

1.1.6.4.9. Deve possuir, no mínimo, 06 (seis) interfaces de rede 1Gbps RJ-45;

1.1.6.4.10. Possuir 1 (uma) interface de rede dedicada para sincronismo;

1.1.6.4.11. Possuir 1 (uma) interface de rede dedicada ao gerenciamento, não sendo permitido utilizar qualquer outra interface para exercer a função de gerenciamento do equipamento;

1.1.6.4.12. Possuir 1 (uma) interface do tipo console ou similar;

1.1.6.4.13. Possuir interface dedicada e fisica para gerenciamento do equipamento fora de banda. Essa interface deve ser um canal de gerenciamento que funcione mesmo quando o dispositivo não responde. Caso o equipamento não possua essa interface fisica/dedicada, deverá ser composta com outro equipamento de terceiro onde faça essa função. Não sendo permitido qualquer tipo de configuração via software ou uso da interface dedicada de gerenciamento.

1.1.6.4.14. Deve possuir armazenamento interno SSD de, no mínimo, 960GB;

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

1.1.6.4.16. Suporte a RFC 4291 de arquitetura de endereçamento IPv6;

1.1.6.4.17. Suportar configurar IPv6 em Dual Stack em uma interface bond/agregação. Essa configuração também poderá ser realizada em uma subinterface de bond/agregação;

1.1.6.4.18. Deve suportar NAT64 e NAT46;

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

1.1.6.4.20. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IPv4 e IPv6 sem duplicação da base de objetos e regras;

1.1.6.4.21. Deve suportar operar em cluster ativo-passivo ou ativo-ativo sem a necessidade de licenças adicionais;

1.1.6.4.22. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

1.1.6.5. FUNCIONALIDADES DE FIREWALL

1.1.6.5.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

1.1.6.5.2. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;

1.1.6.5.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

1.1.6.5.4. A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

1.1.6.5.5. Realizar upgrade via SCP, SFTP e https via interface WEB;

1.1.6.5.6. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

1.1.6.5.6.1. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;

1.1.6.5.6.2. Deverá suportar VXLAN;

1.1.6.5.7. Deve suportar os seguintes tipos de NAT:

1.1.6.5.7.1. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

1.1.6.5.8. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

1.1.6.5.9. As regras de NAT devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra;

1.1.6.5.10. Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços online atualizavéis de forma dinâmica, por exemplo: Office 365, AWS, Azure e outros. Ou seja, objetos dinâmicos que não se caracterizam como FQDN;

1.1.6.5.11. Enviar logs para sistemas de monitoração externos, simultaneamente;

1.1.6.5.12. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar baseado na topologia. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

1.1.6.5.13. Deve realizar roteamentos unicast e multicast simultaneamente em uma única instância (contexto) de firewall.

1.1.6.5.14. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

1.1.6.5.15. Suportar OSPF graceful restart;

1.1.6.5.16. Deve suportar roteamento ECMP (equal cost multi-path);

1.1.6.5.17. Para o ECMP, a solução deve suportar o balanceamento do roteamento de forma simultanea usando os seguintes parametros Origem, Destino, Porta de Origem, Porta de Destino e Protocolo;

1.1.6.5.18. Autenticação integrada via Kerberos.

1.1.6.5.19. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções/ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, FTP, acesso WEB, alterações de política, comunicação SNMP.

1.1.6.5.20. As regras de firewall devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada regra;

1.1.6.5.21. Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas ou obrigatoriamente listadas;

1.1.6.5.22. A solução deve ter a capacidade de operar através de uma unica instância de firewall de forma simultânea mediante o uso das suas interfaces fisicas nos seguintes modos: transparente, modo sniffer (monitoramento e análise o trafego de rede), camada 2 (L2) e camada 3 (L3);

1.1.6.5.23. A solução deve permitir salvar as configurações das políticas para serem

aplicadas em horários pré-definidos;

1.1.6.5.24. Deve possuir mecanismo de ativação de validada da regra com período customizado;

1.1.6.5.25. Deverá suportar redundância e balanceamento de links, tendo capacidade para no mínimo 3 links de internet;

1.1.6.5.26. Deverá suportar configurar um valor de threshold baseando-se em critérios mínimos como fator de decisão nas regras de balanceamento;

1.1.6.5.27. Deve permitir a configuração do tempo de checagem para cada um dos links.

1.1.6.6. FUNCIONALIDADE DE FILTRO DE CONTEÚDO WEB

1.1.6.6.1. Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

1.1.6.6.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

1.1.6.6.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2 e TLS 1.3

1.1.6.6.4. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

1.1.6.6.5. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

1.1.6.6.5.1. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

1.1.6.6.5.2. Reconhecer pelo menos 3.000 (três 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;

1.1.6.6.6. A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

1.1.6.6.7. Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE)

1.1.6.6.8. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

1.1.6.6.8.1. Será aceito soluções de outros fabricantes diferentes do firewall ofertado pela licitante desde que atendido todos os requisitos desta especificação;

1.1.6.6.9. 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;

1.1.6.6.10. A fim de otimização de tempo operacional dos administrdores, a solução deverá possuir pelo menos 150 categorias de aplicações WEB pré-definidas pelo fabricante;

1.1.6.6.11. Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer.);

1.1.6.6.12. A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

1.1.6.6.13. Atualizar a base de assinaturas de aplicações automaticamente;

1.1.6.6.14. Limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

1.1.6.6.15. Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de políticas de segurança baseadas nas informações coletadas entre elas usuários, IP, grupos de usuários do sistema do Active Directory;

1.1.6.6.16. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

1.1.6.6.17. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

1.1.6.6.18. Deve possibilitar que o controle de portas seja aplicado para todas as aplicações;

1.1.6.6.19. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

1.1.6.6.19.1. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

1.1.6.6.19.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

1.1.6.6.19.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

1.1.6.6.19.4. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

1.1.6.6.19.5. Suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;

1.1.6.6.19.6. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;

1.1.6.6.19.7. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

1.1.6.6.19.8. Suportar a criação de categorias de URLs customizadas;

1.1.6.6.19.9. Suportar a exclusão de URLs do bloqueio, por categoria;

1.1.6.6.19.10. Permitir a customização de página de bloqueio;

1.1.6.6.20. 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, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

1.1.6.6.21. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via Radius ou API’s ou Syslog, para a identificação de endereços IP e usuários;

1.1.6.6.22. Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no Firewall (Captive Portal);

1.1.6.7. FUNCIONALIDADE DE FILTRO DE DADOS

1.1.6.7.1. A solução de controle de dados deve trazer de fábrica vários tipos de arquivos e expressões reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de arquivos:

1.1.6.7.1.1. Número de cartão de crédito;

1.1.6.7.1.2. Código fonte JAVA;

1.1.6.7.1.3. Arquivo PDF;

1.1.6.7.1.4. Arquivo executável;

1.1.6.7.1.5. Arquivo de banco de dados;

1.1.6.7.2. A solução de controle de dados deve permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da política, tais como: "Upload", "Download" e "Download e Upload".

1.1.6.7.3. A solução de controle de dados deve permir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima seja feito.

1.1.6.7.4. A solução de controle de dados deve permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

1.1.6.8. FUNCIONALIDADES DE PREVENÇÃO DE AMEAÇAS

1.1.6.8.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

1.1.6.8.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

1.1.6.8.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware quando implementado em alta disponibilidade ativo/passivo;

1.1.6.8.4. Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

1.1.6.8.5. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-open baseado em software, configurável baseado em thresholds de CPU e memória do dispositivo;

1.1.6.8.6. Deverá possuir os seguintes mecanismos de inspeção de IPS:

1.1.6.8.6.1. Análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

1.1.6.8.7. Detectar e bloquear a origem de portscans;

1.1.6.8.8. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

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

1.1.6.8.10. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS e SMTP;

1.1.6.8.11. Suportar bloqueio de arquivos por tipo;

1.1.6.8.12. Identificar e bloquear comunicação com botnets;

1.1.6.8.13. Deve suportar referência cruzada com CVE;

1.1.6.8.14. Em cada proteção de segurança, deve estar incluso informações como:

1.1.6.8.14.1. Código CVE (Common Vulnerabilities and Exposures), não sendo aceito outro codigo de referência;

1.1.6.8.14.2. Severidade;

1.1.6.8.14.3. Tipo de ação a ser executada.

1.1.6.8.15. O IPS deve fornecer um mecanismo automatizado para ativar ou gerenciar novas assinaturas vindas de atualizações.

1.1.6.8.16. O IPS deve suportar exceções de rede com base na origem, destino, serviço ou uma combinação dos três.

1.1.6.8.17. O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar as proteções individuais.

1.1.6.8.18. O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impacto no desempenho, gravidade da ameaça, nível de confiança, proteção do cliente, proteção do servidor)

1.1.6.8.19. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

1.1.6.8.19.1. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

1.1.6.8.20. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

1.1.6.8.21. Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão sendo gerenciados, assim como, qual o tipo de perfil assinalado, de forma individual;

1.1.6.8.22. A solução de IPS, deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações, que aponta quais assinaturas que estão em modo detecção devem ser alterada para modo prevenção, assim evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.

1.1.6.8.23. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalidade de IPS;

1.1.6.8.24. A solução deverá possuir pelo menos dois perfis pré-configurados pelo fabricante que permitam sua utilização assim que o equipamento for configurado;

1.1.6.8.25. A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.

1.1.6.8.26. Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

1.1.6.8.27. Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços de domínios bloqueados;

1.1.6.8.28. O gerenciamento centralizado via interface gráfica, deve possibilitar a configuração de captura dos pacotes por regras individuais, visando aperfeiçoar o desempenho do equipamento;

1.1.6.8.29. A solução de IPS deve possuir mecanismo onde irá determinar de forma automática, onde qualquer nova assinatura que for baixada na base local deverá atuar em modo de prevenção ou detecção, assim evitará qualquer tipo de alteração na base de assinatura atual;

1.1.6.8.30. O anti-vírus ou outra funcionalidade deve oferecer suporte à verificação de links

dentro de e-mails;

1.1.6.8.31. A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quando usuário estiver conectado com ambiente externo malicioso

1.1.6.8.32. A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface gráfica da gerência centralizada;

1.1.6.8.33. Para melhor administração a solução deve possuir a granularidade na classificação das proteções de IPS através de: severidade, nível de confiança da proteção, impacto da performance, referência de indústria terceira e status de download recente;

1.1.6.8.34. A solução deve permitir a criação de allow-list baseado no MD5 do arquivo;

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

1.1.6.8.36. Suportar rastreamento de vírus em arquivos pdf;

1.1.6.8.37. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc);

1.1.6.8.38. Possuir a capacidade de prevenção de ameaças não conhecidas;

1.1.6.8.39. Em caso de falha no mecanismo de inspeção do anti-vírus/anti-malware, deve ser possível configurar se as conexões serão permitidas ou bloqueada

1.1.6.8.40. A solução de anti-vírus/anti-malware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas não podem causar a interrupção de outras funcionalidades de segurança como prevenção de ameaças avançadas (zero-day);

1.1.6.8.41. A solução deverá suportar análise de arquivos que tráfegam dentro do protocolo CIFS/SMB, de forma a conter malwares se espalhando horizontalmente pela rede;

1.1.6.8.42. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

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

1.1.6.8.44. A solução deverá possuir mecanismo de “machine learning” para prevenção de ataques de DNS do tipo DGA (Domain Generation Algorithm), não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

1.1.6.8.45. A solução deverá possuir mecanismo de “machine learning” para prevenção de ataques de DNS Tunneling, não sendo aceito soluções que usem apenas mecanismo baseado em assinaturas.

1.1.6.8.46. Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, sejam resolvidas pelo firewall com endereços previamente definidos, para interceptar a comunicação e bloquear o acesso do usuário.

1.1.6.8.47. A solução de anti-malware/anti-vírus deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

1.1.6.8.48. A solução deve possuir funcionalidade de identificação de bloqueio de tráfego malicioso comunicando com C&C (command & control);

1.1.6.9. FUNCIONALIDADES DE CONTROLE DE QUALIDADE DE SERVIÇO

1.1.6.9.1. Suportar a criação de políticas de QoS por:

1.1.6.9.1.1. Endereço de origem, endereço de destino e por porta;

1.1.6.9.2. O QoS deve possibilitar a definição de classes por:

1.1.6.9.2.1. Banda garantida, banda máxima e fila de prioridade;

1.1.6.9.3. Disponibilizar estatísticas em tempo real para classes de QoS;

1.1.6.10. FUNCIONALIDADES DE VPN

1.1.6.10.1. Suportar VPN site-to-site e client-to-site;

1.1.6.10.2. Suportar IPSec VPN;

1.1.6.10.3. A solução deve suportar Autoridade Certificadora Interna e Externa (de terceiros);

1.1.6.10.4. Suportar SSL VPN;

1.1.6.10.5. A VPN IPSEc deve suportar:

1.1.6.10.5.1. 3DES, Autenticação MD5, SHA-1, SHA-384, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES 128 e 256 (Advanced Encryption Standard), SHA-512 e Autenticação via certificado IKE PKI;

1.1.6.10.6. A VPN SSL deve suportar:

1.1.6.10.6.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB ;

1.1.6.10.6.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

1.1.6.10.6.3. Suportar configuração de comformidade para acesso do usuário via portal SSL ou cliente na máquina do usuário;

1.1.6.10.6.4. Atribuição de endereço IP nos clientes remotos de VPN;

1.1.6.10.6.5. Atribuição de DNS nos clientes remotos de VPN;

1.1.6.10.6.6. Dever permitir criar políticas para tráfego dos clientes remotos conectados na VPN SSL;

1.1.6.10.7. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

1.1.6.11. SOLUÇÃO PARA PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS – ZERO DAY

1.1.6.11.1. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

1.1.6.11.2. A solução deverá ser composta por hardware e software específicos (appliance) com sistema operacional especializado em sua versão mais atualizada ou nuvem do próprio fabricante que possua o conceito de sandboxing para prevenção de ataques zero-day.

1.1.6.11.3. Não serão aceitas soluções que dependam da estrutura de hypervisor do contratante para a análise de ameaças de dia zero, como Vmware ESXi, Microsoft HyperV, entre outros;

1.1.6.11.4. A solução deverá operar em modo MTA (Mail Transfer Agent) para proteção de malware desconhecido de dia zero.

1.1.6.11.5. Inspecionar de forma efetiva o malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS), FTP e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandboxing;

1.1.6.11.6. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

1.1.6.11.7. Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URLs conhecidas;

1.1.6.11.8. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows XP, Windows 7, Windows 8.1 e Windows 10, assim como Office 2003, 2010, 2013 e 2016;

1.1.6.11.9. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente;

1.1.6.11.10. O conteúdo enviado para a solução de sandboxing deverá ser feito automaticamente, sem a necessidade da interação do usuário/administrador para que o processo de análise seja realizado;

1.1.6.11.11. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

1.1.6.11.12. A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;

1.1.6.11.13. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF acima de 10 Mb;

1.1.6.11.14. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e criptografados em SSL;

1.1.6.11.15. Deve implementar análise em sandbox, detecção e bloqueio de malwares em

arquivos java (.jar e class);

1.1.6.11.16. A solução deve suportar inspeção para o protocolo SMBv3;

1.1.6.11.17. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

1.1.6.11.18. Implementar mecanismo de exceção, permitindo a criação de regras por VLAN, subrede e endereço IP;

1.1.6.11.19. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido: pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm e gz;

1.1.6.11.20. A solução deve permitir a criação de allow-lists baseado no MD5 do arquivo;

1.1.6.11.21. A solução deve possuir mecanismo para identificar sites conhecidos e desconhecidos como phishing, analisando em tempo real a URL acessada.

1.1.6.11.22. A solução deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas informações em sites classificados como phishing;

1.1.6.11.23. O Mecanismo de classificação de anti-phising deve atuar sem a necessidade de instalação de agente na máquina do usuário;

1.1.6.11.24. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

1.1.6.11.24.1. Número de arquivos emulados;

1.1.6.11.24.2. Número de arquivos com malware.

1.1.6.11.25. A solução deve prover informação, seja por meio de relatório ou log, sobre as seguintes situações:

1.1.6.11.25.1. O tamanho máximo do arquivo emulado seja excedido;

1.1.6.11.25.2. O tempo máximo de emulação seja excedido.

1.1.7. SERVIÇO DE ACESSO SEGURO DE DISPOSITIVOS A REDE COM GERENCIA EM NUVEM

1.1.7.1. A solução deve ser fornecida incluindo disponibilização de software, instalação, configuração e testes conforme características e especificações descritas no ANEXO D;

1.1.7.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.7.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações

descritas no ANEXO F;

1.1.7.3. Características Gerais

1.1.7.3.1. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

1.1.7.3.2. A solução de proteção avançada para notebooks, desktops e servidores deve consistir em um agente de segurança que será responsável pela análise de arquivos e comportamentos no sistema operacional do computador do usuário final ou servidor a fim de bloquear qualquer tipo de ameaça conhecida e desconhecida.

1.1.7.3.3. Deve escanear arquivos e identificar infecções baseado em características comportamentais dos vírus;

1.1.7.3.4. Deve escanear arquivos quando eles forem acessados, executados, permitindo detecção imediata e tratamento por qualquer ameaça;

1.1.7.3.5. Deve permitir executar uma análise detalhada de cada arquivo conforme selecionado pelo usuário;

1.1.7.3.6. Deve permitir especificar diretórios e extensões de arquivos para que sejam excluídos da análise de vírus;

1.1.7.3.7. Deve checar as áreas mais comuns do sistema de arquivos e o registro do sistema operacional em busca de ameaças avançadas;

1.1.7.3.8. Deve possuir as seguintes opções de remediação:

1.1.7.3.8.1. Reparar;

1.1.7.3.8.2. Quarentenar;

1.1.7.3.8.3. Apagar;

1.1.7.3.9. Deve permitir ser gerenciado através de console unificada para gerenciamento centralizado de políticas e logs.

1.1.7.3.10. Deve identificar automaticamente o ponto de entrada do malware e o seu impacto para a organização;

1.1.7.3.11. A solução deve suportar os seguintes sistemas operacionais:

1.1.7.3.11.1. Windows 7 SP1, 8.1, 10 e 11;

1.1.7.3.11.2. Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 e 2022;

1.1.7.3.12. Deve gerar automaticamente relatório completo da execução do malware utilizando técnicas contidas no MITRE Framework;

1.1.7.3.13. Deve bloquear ataques independentemente se o vetor de distribuição é baseado na web, email ou mídia removível;

1.1.7.3.14. Deve detectar e bloquear comunicações com servidores de comando e controle (C&C) para impedir vazamento de dados mesmo quando conectado/trabalhando remotamente.

1.1.7.3.15. Deve permitir a quarentena de sistemas infectados para evitar que o malware se espalhe;

1.1.7.3.16. Deve possuir funcionalidade de análise forense de incidente, provendo uma visão completa do fluxo do ataque, causa raiz, impacto no negócio e o ponto de entrada do malware para agilizar as ações de remediação;

1.1.7.3.17. O endpoint deve ser integrado ao anti-vírus (agente único e gerenciamento), que fornece uma forte proteção de primeira linha estática e dinâmica usando assinaturas e análise comportamental.

1.1.7.3.18. O endpoint deve fornecer a capacidade de ativar/desativar granularmente cada funcionalidade, que serve como um meio para isolar qualquer interferência com outros aplicativos. Além das ferramentas de solução de problemas padrão, as informações de forense podem ajudar na identificação de tais interferências;

1.1.7.3.19. Deve ser capaz de efetuar roll-back de mudanças no registro do Windows e alterações no sistema de arquivos em caso de alteração a arquivos infectados;

1.1.7.3.20. Deve proteger os dados forenses armazenados na estação de trabalho (endpoint) contra acessos não autorizados ou outro tipo de tentativa de manipulação através da estrutura segura de logs da solução;

1.1.7.3.21. Os clientes devem se comunicar apenas com servidores autorizados (ou seja, apenas IPs específicos fornecidos por um servidor autenticado) e realizar a validação do certificado do servidor (usando informações internas) para verificar se o servidor é confiável;

1.1.7.3.22. Deve possuir análise de campos de login e senha em caso de acesso a páginas de internet como e-mail e formulários na detecção e prevenção de sites de phishing;

1.1.7.3.23. Deve possuir mecanismo de proteção para evitar que o usuário use credenciais corporativas em sites não corporativos;

1.1.7.3.24. A solução deve ser capaz de fazer remediação de forma automatizada, sem a necessidade da intervenção do usuário;

1.1.7.3.25. A solução deverá detectar e bloquear tem tempo real qualquer ação maliciosa ao sistema operacional que venha através de download de arquivos na web, cópia através de um drive externo, sites de phishing e até mesmo mecanismos de criptografia de arquivos como o ransomware.

1.1.7.3.26. A solução deve possuir mecanismos de restauração dos arquivos no momento em que é detectado e bloqueado o ransomware, ou seja, não permitindo o sequestro de informações.

1.1.7.3.27. A solução deverá detectar e bloquear ameaças em download ou através de movimento lateral (cópia de arquivos) em qualquer extensão Microsoft Office, sendo ela capaz de detectar qualquer tipo de executável que tente criptografar os arquivos do computador do usuário.

1.1.7.3.28. A solução deverá detectar e bloquear malwares de dia zero no momento do download e cópia através de drive externo. Deve prevenir e remediar de forma automática ataques evasivos de ransomware, baseado em análise comportamental;

1.1.7.3.29. Deve reverter as ações do ransomware, restaurando os dados corporativos automaticamente, garantindo proteção contra criptografia dos dados;

1.1.7.3.30. Possuir tecnologia que não seja baseada em assinaturas, garantindo seu funcionamento tanto de forma online quanto offline;

1.1.7.3.31. Deve permitir que os agentes obtenham atualizações de assinaturas através de um ponto local, sem uma conexão com o serviço de gerenciamento.

1.1.7.3.32. Deve implementar, através de análise dinâmica e heurística, proteção em tempo real contra sites conhecidos e desconhecidos de phishing;

1.1.7.3.33. Deve detectar, através de análise estática e heurística, elementos suspeitos em sites que solicitem credenciais dos usuários;

1.1.7.3.34. Deve detectar e prevenir a reutilização de credenciais corporativas em sites externos;

1.1.7.3.35. Deve suportar o monitoramento do Log de Eventos do Windows para analisar eventos de malware de fornecedores de antivírus de terceiros.

1.1.7.3.36. Deve ser capaz de realizar ações com base no Log de Eventos do Windows, como:

1.1.7.3.36.1. Analisar ataques;

1.1.7.3.36.2. Encerrar processos;

1.1.7.3.36.3. Excluir ou colocar arquivos em quarentena

1.1.7.3.37. Deve possuir processo de análise forense automático de incidentes, disponibilizando as seguintes informações sobre o ataque:

1.1.7.3.37.1. Eventos maliciosos;

1.1.7.3.37.2. Ponto de entrada do malware;

1.1.7.3.37.3. Escopo dos danos causados;

1.1.7.3.37.4. Máquinas infectadas;

1.1.7.3.38. Deverá ser capaz de realizar importação customizada de Indicadores de Comprometimentos (IOC) externos;

1.1.7.4. Características de Gerenciamento Centralizado de Políticas de Segurança, Logs e Relatórios:

1.1.7.4.1. O software de gerência deve ser capaz de gerenciar todos os endpoints de segurança de forma centralizada, possibilitando a concentração dos logs e emissão de relatórios;

1.1.7.4.2. A gerência dos endpoints deve ser realizada através de console própria ou através de interface web (HTTPS).

1.1.7.4.3. Permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras em todos os equipamentos.

1.1.7.4.4. A solução deve possuir mecanismo de indexação de logs para permitir uma busca acelerada dos eventos sem a necessidade de abertura de arquivos de logs mais antigos.

1.1.7.4.5. A solução deve ter integração com o Microsoft Active Directory para identificação de usuários e importação da estrutura de máquinas;

1.1.7.4.6. A solução deve incluir a opção de pesquisar dentro da lista de eventos, drill down em detalhes para a investigação e análise dos eventos;

1.1.7.4.7. A solução de gerenciamento deverá ser entregue em nuvem do próprio fabricante;

1.1.7.4.8. A solução deve apresentar sumário apontando os agentes que estão instalados, em progresso ou que ainda estão pendentes;

1.1.7.4.9. Todos os logs deverão ser referenciados com o nome do usuário caso haja a integração com o Active Directory;

1.1.7.4.10. Deve disponibilizar informações gráficas na linha do tempo que informe o número de eventos ocorridos;

1.1.7.4.11. Disponibilizar recursos interativos de navegação nos eventos informados;

1.1.7.4.12. A solução deve possuir relatórios customizáveis onde seja possível pegar diferentes informações para montagem do relatório;

1.1.7.4.13. Correlacionar eventos capaz de utilizar como base informações o número de conexões em determinado tempo seguido pelo menos das ações: bloqueio da origem, envio de SNMP e envio de e-mail;

1.1.7.4.14. A solução deve exportar relatórios via HTML e CSV;

1.1.7.4.15. A solução deve possibilitar a visualização geográfica dos eventos de segurança correlacionados;

1.1.7.4.16. A solução deve permitir ao administrador ser capaz de atribuir filtros para diferentes linhas do gráfico que são atualizadas em intervalos regulares, mostrando todos os eventos que corresponda a esse filtro. Permitindo ao operador a concentrar-se sobre os eventos mais importantes.

1.1.7.4.17. A solução deve prover no mínimo as seguintes funcionalidades para análise avançada dos incidentes:

1.1.7.4.17.1. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

1.1.7.4.17.2. Estatísticas com comparativo de período (hora, dia e mês);

1.1.7.4.18. Deve permitir a geração de relatórios com horários predefinidos, diários, semanais e mensais, incluindo principais eventos, principais origens, principais destinos, principais serviços, principais origens e os seus principais eventos, principais destinos e seus principais eventos e principais serviços e seus principais eventos;

1.1.7.4.19. A solução deve incluir a opção de pesquisar dentro da lista de eventos, drill down em detalhes para a investigação e analise dos eventos;

1.1.7.4.20. Deve mostrar a distribuição dos diferentes eventos filtrados por país em um mapa, onde deve estar incluso principais eventos de origem ou destino por pais.

1.1.7.4.21. Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

1.1.7.4.22. Deve estar inclusa na lista de eventos a opção de gerar automaticamente gráficos ou tabelas com o evento, a origem e distribuição de destino.

1.1.7.4.23. Deve estar incluso no dashboard com horários predefinidos, diários, semanais e relatórios mensais. Incluindo:

1.1.7.4.23.1. Principais eventos,

1.1.7.4.23.2. Principais origens,

1.1.7.4.23.3. Principais destinos,

1.1.7.4.23.4. Principais serviços,

1.1.7.4.23.5. Principais origens e os seus principais eventos,

1.1.7.4.23.6. Principais destinos e seus principais eventos;

1.1.7.4.24. A solução deve incluir relatórios de horários, diários, semanais e mensais pré-definidos. Incluindo pelo menos eventos de principais origens, principais destinos, principais eventos, principais usuários, principais localidades de origens e os principais eventos relacionados em cada filtro;

1.1.7.4.25. Deve suportar a programação de relatórios automáticos, para as informações básicas que precisa extrair de forma diária, semanal e mensal. Também deve permitir ao administrador definir a data e a hora que o sistema de informação começa a gerar o relatório agendado.

1.1.7.4.26. A solução deve possuir pesquisa através de todos os endpoints instalados para buscar informações relacionadas a nome de processo, MD5 do arquivo, IP da rede origem, IP da rede de destino, URL, nome do arquivo, tipo do arquivo para identificação de possiveis atividades anômalas no ambiente corporativo.

1.1.7.4.27. A solução deve possuir pequisa das principais atividades maliciosas, através de pesquisas baseadas em processos, palavras chaves ou usuário. Quando encontrado, deve ser possiveis incluir outras informações no campo de busca que podem ser combinadas no período determinado pelo administrador. Assim, terá ampla visibilidade da informação que foi colocado na busca em todos os endponits instalados no ambiente de produção;

1.1.7.4.28. A ferramenta deve apresentar linha do tempo com as principais atividade de rede e ameaças permitindo o administrador ter mais informações entre elas:

1.1.7.4.28.1. Detalhes da rede

1.1.7.4.28.2. Detalhe do dispositivo identificando contendo informações do usuário, computador, sistema operacional e sua versão e nome de domínio;

1.1.7.4.29. Detalhes do processo que foi identificado através da busca realizada.

1.1.7.4.30. Horário da atividade que foi identificada.

1.1.7.4.31. Quando identificar qualquer atividade de rede ou ameaça através da ferramenta,

a solução deve permitir o administrador a realizar ações como:

1.1.7.4.31.1. Terminar processo;

1.1.7.4.31.2. Quarentenar arquivo;

1.1.7.4.31.3. Ter acesso à análise forense.

1.1.7.4.32. Deverá permitir consultas predefinidas de vulnerabilidades reais, permitindo também uma visualização do painel MITRE ATT&CK, ajudando na identificação das técnicas de evasão baseado neste framework;

1.1.8. SERVIÇO DE VISIBILIDADE DE SEGURANÇA PARA REDE EM NUVEM

1.1.8.1. A solução deve ser fornecida incluindo disponibilização de software, instalação, configuração e testes conforme características e especificações descritas no ANEXO D;

1.1.8.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.8.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO F;

1.1.8.3. Características Gerais

1.1.8.3.1. A solução de XDR deverá se integrar com outras ferramentas de segurança do mesmo fabricante e de terceiros para fornecer uma visão unificada de todas as operações de segurança a fim de ajudar a detectar, responder e prevenir ataques cibernéticos;

1.1.8.3.2. A console de administração, bem como todos os elementos da ferramenta descritas nesse termo, deverão ser entregues em nuvem, ou seja, sem a necessidade de fornecimento de hardware ou máquina virtual;

1.1.8.3.3. A solução deverá se integrar com pelo menos as seguintes ferramentas do mesmo fabricante:

1.1.8.3.3.1. Gateway/Firewall;

1.1.8.3.3.2. Anti-vírus/EDR;

1.1.8.3.4. A solução deverá se integrar com, pelo menos, as seguintes ferramentas de mercado:

1.1.8.3.4.1. Fortinet FortiGate;

1.1.8.3.4.2. Palo Alto Next Generation Firewall;

1.1.8.3.4.3. Check Point Quantum Security Gateway;

1.1.8.3.4.4. Cisco Firepower;

1.1.8.3.4.5. CrowdStrike Falcon;

1.1.8.3.4.6. SentinelOne Singularity;

1.1.8.3.4.7. Harmony Endpoint;

1.1.8.3.4.8. Trend Vision One;

1.1.8.3.4.9. Microsoft 365 Defender for Endpoint;

1.1.8.3.5. A solução deve mostrar o status de conectividade das soluções integradas, mudando o status caso haja desconexão das integrações;

1.1.8.3.6. A solução deve demonstrar a quantidade de detecções ou prevenções por origem;

1.1.8.3.7. Deve ser capaz de demonstrar uma linha do tempo com a quantidade de incidentes e suas severidades;

1.1.8.3.8. Para cada incidente detectado, deverá demonstrar o nível de confiança da detecção em pelo menos os seguintes níveis:

1.1.8.3.8.1. Alto;

1.1.8.3.8.2. Médio;

1.1.8.3.8.3. Baixo;

1.1.8.3.9. Na indicação do incidente, deverá informar a origem dos eventos correlacionados;

1.1.8.3.10. Cada incidente gerado pela ferramenta deve possuir, pelo menos, as seguintes características:

1.1.8.3.10.1. ID único de identificação;

1.1.8.3.10.2. Data de criação e data da última atualização;

1.1.8.3.10.3. Nível de prioridade, severidade e confiança;

1.1.8.3.10.4. Capacidade de adicionar um comentário ao incidente para que sirva de orientação para outros analistas que verificarem o incidente posteriormente;

1.1.8.3.10.5. Apresentar todos os ativos e indicadores afetados envolvidos no incidente;

1.1.8.3.10.6. Os indicadores do incidente devem ser automaticamente adicionados ao gerenciamento de IOCs, garantindo que outros elementos do ambiente não tenham comunicação com esse indicador;

1.1.8.3.10.7. Deverá apresentar um breve descritivo sobre o incidente para servir como orientação para o analista responsável;

1.1.8.3.11. A solução deve informar as táticas e técnicas envolvidas no incidente conforme o MITRE ATT&CK;

1.1.8.3.12. Deve ser possível criar exclusões a partir de um incidente para casos de, por exemplo, falso positivo e atividade reconhecida;

1.1.8.3.13. Deve ser possível aplicar a exclusão criada de forma retroativa à partir de uma data pré-definida;

1.1.8.3.14. A ferramenta deve possibilitar a criação de exclusões para que não seja gerado um incidente para um Host, IP ou e-mail específico;

1.1.8.3.15. O XDR deverá utilizar inteligência artificial (IA) e o aprendizado de máquina (ML) para analisar eventos de segurança em todos os produtos integrados e identificar riscos de segurança no ambiente;

1.1.8.3.16. Após correlacionar os logs dos produtos, se um risco de segurança for detectado, a solução deverá gerar um incidente (alerta) com uma prioridade apropriada com base na gravidade e no nível de confiança da detecção, e fornecer mitigação ao incidente;

1.1.8.3.17. Os incidentes devem ser mapeados de acordo com o framework do MITRE ATT&CK;

1.1.8.3.18. Deverá permitir que o incidente seja assinalado para a análise de um analista do SOC;

1.1.8.3.19. Permitir que os administradores sejam notificados quando um novo incidente for gerado;

1.1.8.3.20. A console de administração deve permitir filtrar por um período de até 30 dias, painéis com, no mínimo, as seguintes informações:

1.1.8.3.20.1. Produtos conectados ao XDR;

1.1.8.3.20.2. Número total de eventos de segurança analisados por fonte e a respectiva ação tomada;

1.1.8.3.20.3. Incidentes gerados, bem como o status de cada incidente. Os status devem ser, no mínimo:

1.1.8.3.20.3.1. Novo;

1.1.8.3.20.3.2. Novo e atribuído;

1.1.8.3.20.3.3. Em progresso;

1.1.8.3.20.3.4. Fechado;

1.1.8.3.20.4. O dashboard deve permitir filtrar os incidentes por prioridade;

1.1.8.3.20.5. Deve prover uma visão de incidentes abertos e atribuídos por analista;

1.1.8.3.21. A ferramenta deve alertar os administradores através das seguintes ferramentas:

1.1.8.3.21.1. E-mail;

1.1.8.3.21.2. Slack;

1.1.8.3.21.3. Teams;

1.1.8.3.22. Deverá possuir ferramenta de consulta de indicadores em uma base de inteligência do próprio fabricante;

1.1.8.3.23. A consulta deve permitir no mínimo os seguintes indicadores:

1.1.8.3.23.1. URL;

1.1.8.3.23.2. Domínio;

1.1.8.3.23.3. Hash do arquivo (MD5, SHA1 ou SHA256);

1.1.8.3.23.4. Endereço IP;

1.1.8.3.24. Deve ser possível enviar um arquivo através da console de administração ou já analisar de forma automática os arquivos em ambiente de sandboxing do fabricante, retornando o veredito da emulação;

1.1.8.3.25. A console administrativa deve fornecer uma ferramenta investigativa que permite consultas avançadas sobre todos os eventos forenses (maliciosos e benignos) coletados;

1.1.8.3.26. A ferramenta de investigação deve possuir filtros de consultas pré-definidas para auxiliar na análise;

1.1.8.3.27. A ferramenta deverá ser capaz de reter logs por até 1 ano;

1.1.8.3.28. A solução deverá fornecer um local central para gerenciar indicadores de

compromisso (IoCs) de todos os produtos integrados;

1.1.8.3.29. O gerenciador de IoCs pode integrar com feeds personalizados de várias fontes e combiná-los em um único feed de fácil acesso;

1.1.8.3.30. O gerenciador de IoCs também deve permitir com que o administrador crie ou importe sua própria lista de indicadores de compromisso.

1.1.8.3.31. Para a solução de EDR do mesmo fabricante integrada, deverá permitir automatizar operações de segurança com pelo menos as seguintes ações:

1.1.8.3.31.1. Isolar um endpoint infectado;

1.1.8.3.31.2. Deletar um arquivo da máquina;

1.1.8.3.31.3. Terminar um processo da máquina;

1.1.8.3.31.4. Alertar no caso de uma possível exploração;

1.1.8.3.31.5. Alertar no caso de tentativas repetidas de logins em dispositivos Windows;

1.1.8.3.32. A solução deve gerar logs de auditoria para registrar mudanças de configurações do produto para, pelo menos:

1.1.8.3.32.1. Mudanças de políticas;

1.1.8.3.32.2. Notificações enviadas;

1.1.8.3.32.3. Criação de exclusões;

1.1.8.3.33. Deve ser possível exportar logs de auditoria em pelo menos um dos seguintes formatos:

1.1.8.3.33.1. CSV

1.1.8.3.33.2. XLS

1.1.8.3.33.3. HTML

1.1.8.3.33.4. PDF

1.1.8.3.34. Deve permitir gerar relatórios, com capacidade para agendar envios de forma diária, semanal ou mensal;

1.1.8.3.35. A solução deve dispor de REST API para consulta de incidentes e dados forenses;

1.1.8.3.36. Deve permitir a integração com ferramentas para abertura de tickets de forma

automática, sendo elas, no mínimo:

1.1.8.3.36.1. Jira

1.1.8.3.36.2. ServiceNow

1.1.8.3.37. Deve permitir a visualização das automações executadas, bem como dia e hora da execução;

1.1.9. SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM – TIPO 1

1.1.9.1. SERVIÇOS DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE DE LAN

1.1.9.1.1. A solução deve ser fornecida incluindo disponibilização de equipamento e software, instalação, configuração e testes conforme características e especificações descritas no ANEXO D;

1.1.9.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.9.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO F;

1.1.9.3. REQUISITOS TÉCNICOS

1.1.9.3.1. Deve possuir no mínimo 48 portas 10/100/1000BaseT Gigabit Ethernet BaseT;

1.1.9.3.2. Deve possuir 4 portas adicionais com velocidade de 1/10G SFP+;

1.1.9.3.3. Deve possuir 1 interface RJ-45, USB-C ou serial para acesso console local;

1.1.9.3.4. Deve possuir memória RAM de no mínimo 1GB;

1.1.9.3.5. Deve possuir buffer de pacotes de no mínimo 1MB;

1.1.9.3.6. Deve possuir capacidade de encaminhamento de no mínimo 97 Mpps;

1.1.9.3.7. Deve possuir capacidade de comutação de no mínimo 175 Gbps;

1.1.9.3.8. O switch deve ser do tipo empilhável, com altura máxima de 1RU e instalação em rack (19”). Deve acompanhar todos os componentes necessários para sua fixação no rack;

1.1.9.3.9. Deve possuir fonte de alimentação interna 100/240VAC

1.1.9.3.10. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;

1.1.9.3.11. FUNCIONALIDADES DE CAMADA 2

1.1.9.3.11.1. Deve implementar VLAN 802.1Q

1.1.9.3.11.2. Deve implementar suporte a Jumbo Packets de pelo menos 9000 bytes

1.1.9.3.11.3. Deve implementar Port Mirroring com no mínimo 4 grupos de espelhamento

1.1.9.3.11.4. Deve implementar 4094 VLAN IDs

1.1.9.3.11.5. Deve suportar 256 VLANS configuradas simultâneamente

1.1.9.3.11.6. Deve implementar MVRP (IEEE 802.1Ak);
1.1.9.3.11.7. Deve implementar LLDP (IEEE 802.1ab);
1.1.9.3.11.8. Deve implementar LLDP-MED (ANSI/TIA-1057);
1.1.9.3.11.9. Deve implementar MSTP (IEEE 802.1s);
1.1.9.3.11.10. Deve possuir tabela ARP de pelo menos 1024 entradas
1.1.9.3.11.11. Deve possuir capacidade mínima da tabela MAC de 8 mil entradas

1.1.9.3.12. FUNCIONALIDADES DE CAMADA 3

1.1.9.3.12.1. Deve implementar roteamento estático;
1.1.9.3.12.2. Deve suportar dual stack
1.1.9.3.12.3. Deve suportar DHCP Client para IPv4 e IPv6
1.1.9.3.12.4. Deve suportar no mínimo 512 rotas IPV4 e 512 rotas IPv6

1.1.9.4. MULTICAST

1.1.9.4.1. Deve implementar MLD snooping (RFC 4604);
1.1.9.4.2. Deve implementar IGMP v2 e v3 (RFC 2236 e RFC 3376);

1.1.9.5. QOS E ACL

1.1.9.5.1. Deve implementar a função de rate limit configurado por porta;
1.1.9.5.2. Deve implementar Strict priority (SP) queuing (RFC 7640);
1.1.9.5.3. Deve implementar priorização de tráfego em tempo real;
1.1.9.5.4. Deve implementar priorização de tráfego com no mínimo os seguintes parâmetros: endereço IP, Tipo de Serviço, Número da porta TCP/UDP, porta de origem e Diffserv.
1.1.9.5.5. Deve suporta no mínimo oito filas por porta;
1.1.9.5.6. Deve suportar ACL para IPv4 e IPv6;
1.1.9.5.7. Deve implementar ACL com base no IP de origem e destino, porta TCP e UDP de origem e destino baseada em VLAN ou por Porta;

1.1.9.6. SEGURANÇA

1.1.9.6.1. Deve implementar TACACS+ e/ou RADIUS;
1.1.9.6.2. Deve implementar IEEE 802.1x;
1.1.9.6.3. Deve implementar autenticação baseada em web;
1.1.9.6.4. Deve implementar autenticação baseada em endereço MAC;
1.1.9.6.5. Deve implementar proteção contra-ataques na CPU do switch para prevenção de desligamento do equipamento;
1.1.9.6.6. Deve implementar SSHv2;;

1.1.9.7. GERENCIAMENTO

1.1.9.7.1. Deve implementar NTP;
1.1.9.7.2. Deve suportar duas imagens de software na flash;
1.1.9.7.3. Deve suportar múltiplos arquivos de configuração na flash (mais de um arquivo);
1.1.9.7.4. deve suportar detecção de falha e link entre switches;
1.1.9.7.5. Deve implementar sFlow;
1.1.9.7.6. Deve possuir interface web e/ou via linha de comando para configuração;

1.1.9.7.7. Deve implementar Syslog;
1.1.9.7.8. Deve implementar TFTP e/ou SFTP;
1.1.9.7.9. Deve suportar RMON
1.1.9.7.10. Deve suportar Ping e/ou Traceroute para IPv4 e IPv6
1.1.9.7.11. Deve implementar SNMP v1/v2/v3

1.1.9.8. LICENCIAMENTO

1.1.9.8.1. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;
1.1.9.8.2. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades disponíveis para o equipamento;

1.1.9.9. SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO

1.1.9.9.1. A solução deve ser fornecida incluindo solução de gerenciamento centralizado conforme características e especificações descritas no ANEXO C;

1.1.10. SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM – TIPO 2

1.1.10.1. SERVIÇOS DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE LAN

1.1.10.1.1. A solução deve ser fornecida incluindo disponibilização de equipamento e software, instalação, configuração e testes conforme características e especificações descritas no ANEXO D;

1.1.10.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.10.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO F;

1.1.10.3. REQUISITOS TÉCNICOS

1.1.10.3.1. Deve possuir no mínimo 24 portas 10/100/1000BaseT Gigabit Ethernet BaseT
1.1.10.3.2. Deve possuir 4 portas com velocidade de 1/10G SFP+;
1.1.10.3.3. Deve implementar PoE e PoE+ (Power over Ethernet) de acordo com o padrão IEEE 803.3af e IEEE 802.3at;
1.1.10.3.4. Deve possuir no mínimo 370 watts destinados as portas com PoE+ ativo;
1.1.10.3.5. Deve possuir 1 interface RJ-45, USB-C ou serial para acesso console local
1.1.10.3.6. Deve possuir memória RAM de no mínimo 1GB;
1.1.10.3.7. Deve possuir buffer de pacotes de no mínimo 1MB;
1.1.10.3.8. Deve possuir capacidade de encaminhamento de no mínimo 94 Mpps;
1.1.10.3.9. Deve possuir capacidade de comutação de no mínimo 127 Gbps;
1.1.10.3.10. O switch deve ser do tipo empilhável, com altura máxima de 1RU e instalação em rack (19”). Deve acompanhar todos os componentes necessários

para sua fixação no rack;

1.1.10.3.11. Deve possuir fonte de alimentação interna 100/240VAC;

1.1.10.3.12. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;

1.1.10.3.13. FUNCIONALIDADES DE CAMADA 2

1.1.10.3.13.1. Deve implementar VLAN 802.1Q

1.1.10.3.13.2. Deve implementar suporte a Jumbo Packets de pelo menos 9000 bytes

1.1.10.3.13.3. Deve implementar Port Mirroring com no mínimo 4 grupos de espelhamento

1.1.10.3.13.4. Deve implementar funcionalidade que permita a detecção de links unidirecionais;

1.1.10.3.13.5. Deve implementar 4094 VLAN IDs

1.1.10.3.13.6. Deve suportar 256 VLANS Configuradas simultaneamente

1.1.10.3.13.7. Deve implementar MVRP (IEEE 802.1Ak);

1.1.10.3.13.8. Deve implementar LLDP (IEEE 802.1ab);

1.1.10.3.13.9. Deve implementar LLDP-MED;

1.1.10.3.13.10. Deve implementar MSTP (IEEE 802.1s);

1.1.10.3.13.11. Deve possuir tabela ARP de pelo menos 1024 entradas

1.1.10.3.13.12. Deve possuir capacidade mínima da tabela MAC de 8 mil entradas

1.1.10.3.14. FUNCIONALIDADES DE CAMADA 3

1.1.10.3.14.1. Deve implementar roteamento estático;

1.1.10.3.14.2. Deve suportar dual stack

1.1.10.3.14.3. Deve suportar DHCP Client para IPv4 e IPv6

1.1.10.3.14.4. Deve suportar no mínimo 512 rotas IPV4 e 512 rotas IPv6

1.1.10.4. MULTICAST

1.1.10.4.1. Deve implementar MLD snooping;

1.1.10.4.2. Deve implementar IGMP v2 e v3 (RFC 2236 e RFC 3376);

1.1.10.5. QOS E ACL

1.1.10.5.1. Deve implementar a função de rate limit configurado por porta;

1.1.10.5.2. Deve implementar Strict priority (SP) queuing

1.1.10.5.3. Deve implementar priorização de tráfego em tempo real

1.1.10.5.4. Deve implementar priorização de tráfego com no mínimo os seguintes parâmetros: endereço IP, Tipo de Serviço, Número da porta TCP/UDP, porta de origem e Diffserv.

1.1.10.5.5. Deve suporta no mínimo oito filas por porta

1.1.10.5.6. Deve suportar ACL para IPv4 e IPv6

1.1.10.5.7. Deve implementar ACL com base no IP de origem e destino, porta TCP e UDP de origem e destino baseada em VLAN ou por Porta.

1.1.10.6. SEGURANÇA

1.1.10.6.1. Deve implementar TACACS+ e/ou RADIUS;

1.1.10.6.2. Deve implementar IEEE 802.1x;

1.1.10.6.3. Deve implementar autenticação baseada em web;

1.1.10.6.4. Deve implementar autenticação baseada em endereço MAC;

1.1.10.6.5. Deve implementar proteção contra ataques na CPU do switch para prevenção de desligamento do equipamento

1.1.10.6.6. Deve implementar SSHv2;

1.1.10.7. GERENCIAMENTO

1.1.10.7.1. Deve implementar NTP;

1.1.10.7.2. Deve suportar duas imagens de software na flash;

1.1.10.7.3. Deve suportar múltiplos arquivos de configuração na flash (mais de um arquivo);

1.1.10.7.4. deve suportar detecção de falha e link entre switches;

1.1.10.7.5. Deve implementar sFlow;

1.1.10.7.6. Deve possuir interface web e/ou via linha de comando para configuração;

1.1.10.7.7. Deve implementar Syslog;

1.1.10.7.8. Deve implementar TFTP e/ou SFTP;

1.1.10.7.9. Deve suportar RMON

1.1.10.7.10. Deve suportar Ping e/ou Traceroute para IPv4 e IPv6

1.1.10.7.11. Deve implementar SNMP v1/v2/v3

1.1.10.8. LICENCIAMENTO

1.1.10.8.1. Deve ser fornecido com a versão de software mais atualizada disponível para o equipamento;

1.1.10.8.2. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades especificadas;

1.1.10.9. SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO

1.1.10.9.1. A solução deve ser fornecida incluindo solução de gerenciamento centralizado conforme características e especificações descritas no ANEXO C;

1.1.11. SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM – TIPO 3

1.1.11.1. SERVIÇOS DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE LAN.

1.1.11.1.1. A solução deve ser fornecida incluindo disponibilização de equipamentos e software, instalação, configuração e testes conforme características e especificações descritas no ANEXO D;

1.1.11.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.11.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO F;

1.1.11.3. REQUISITOS TÉCNICOS

1.1.11.3.1. CAPACIDADES E QUANTIDADES

1.1.11.3.1.1. Deve possuir no mínimo 24 portas 10/100/1000BaseT Gigabit Ethernet BaseT

1.1.11.3.1.2. Deve possuir 4 portas adicionais com velocidade de 1/10G SFP+;

1.1.11.3.1.3. Deve possuir 1 interface RJ-45, USB-C ou serial para acesso console local

1.1.11.3.1.4. Deve possuir memória RAM de no mínimo 1GB;

1.1.11.3.1.5. Deve possuir buffer de pacotes de no mínimo 1MB;

1.1.11.3.1.6. Deve possuir capacidade de encaminhamento de no mínimo 94 Mpps;

1.1.11.3.1.7. Deve possuir capacidade de comutação de no mínimo 127 Gbps;

1.1.11.3.1.8. O switch deve ser do tipo empilhável, com altura máxima de 1RU e instalação em rack (19”). Deve acompanhar todos os componentes necessários para sua fixação no rack;

1.1.11.3.1.9. Deve possuir fonte de alimentação interna 100/240VAC

1.1.11.3.1.10. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;

1.1.11.3.2. FUNCIONALIDADES DE CAMADA 2

1.1.11.3.2.1. Deve implementar VLAN 802.1Q;

1.1.11.3.2.2. Deve implementar suporte a Jumbo Packets de pelo menos 9000 bytes;

1.1.11.3.2.3. Deve implementar Port Mirroring com no mínimo 4 grupos de espelhamento

1.1.11.3.2.4. Deve implementar funcionalidade que permita a detecção de links unidirecionais;

1.1.11.3.2.5. Deve implementar 4094 VLAN IDs

1.1.11.3.2.6. Deve suportar 256 VLANS Configuradas simultaneamente

1.1.11.3.2.7. Deve implementar MVRP (IEEE 802.1Ak);

1.1.11.3.2.8. Deve implementar LLDP (IEEE 802.1ab);

1.1.11.3.2.9. Deve implementar LLDP-MED;

1.1.11.3.2.10. Deve implementar MSTP (IEEE 802.1s);

1.1.11.3.2.11. Possuir tabela ARP de pelo menos 1024 entradas

1.1.11.3.2.12. Deve possuir capacidade mínima da tabela MAC de 8 mil entradas

1.1.11.3.3. FUNCIONALIDADES DE CAMADA 3

1.1.11.3.3.1. Deve implementar roteamento estático;

1.1.11.3.3.2. Deve suportar dual stack

1.1.11.3.3.3. Deve suportar DHCP Client para IPv4 e IPv6

1.1.11.3.3.4. Deve suportar no mínimo 512 rotas IPV4 e 512 rotas IPv6

1.1.11.4. MULTICAST

1.1.11.4.1.1. Deve implementar MLD snooping;

1.1.11.4.1.2. Deve implementar IGMP v2 e v3 (RFC 2236 e RFC 3376);

1.1.11.5. QOS E ACL

1.1.11.5.1.1. Deve implementar a função de rate limit configurado por porta;

1.1.11.5.1.2. Deve implementar Strict priority (SP) queuing

1.1.11.5.1.3. Deve implementar priorização de tráfego em tempo real

1.1.11.5.1.4. Deve implementar priorização de tráfego com no mínimo os seguintes parâmetros: endereço IP, Tipo de Serviço, Número da porta TCP/UDP, porta de origem e Diffserv.

1.1.11.5.1.5. Deve suporta no mínimo oito filas por porta

1.1.11.5.1.6. Deve suportar ACL para IPv4 e IPv6

1.1.11.5.1.7. Deve implementar Acl com base no IP de origem e destino, porta TCP e UDP de origem e destino baseada em VLAN ou por Porta.

1.1.11.6. SEGURANÇA

1.1.11.6.1.1. Deve implementar TACACS+ e/ou RADIUS;

1.1.11.6.1.2. Deve implementar 802.1x;

1.1.11.6.1.3. Deve implementar autenticação baseada em web;

1.1.11.6.1.4. Deve implementar autenticação baseada em endereço MAC;

1.1.11.6.1.5. Deve implementar proteção contra ataques na CPU do switch para prevenção de desligamento do equipamento

1.1.11.6.1.6. Deve implementar SSHv2;

1.1.11.7. GERENCIAMENTO

1.1.11.7.1.1. Deve implementar NTP;

1.1.11.7.1.2. Deve suportar duas imagens de software na flash;

1.1.11.7.1.3. Deve suportar múltiplos arquivos de configuração na flash (mais de um arquivo);

1.1.11.7.1.4. deve suportar detecção de falha e link entre switches;

1.1.11.7.1.5. Deve implementar sFlow;

1.1.11.7.1.6. Deve possuir interface web e/ou via linha de comando para configuração;

1.1.11.7.1.7. Deve implementar Syslog;

1.1.11.7.1.8. Deve implementar TFTP e/ou SFTP;

1.1.11.7.1.9. Deve suportar RMON

1.1.11.7.1.10. Deve suportar Ping e/ou Traceroute para IPv4 e IPv6

1.1.11.7.1.11. Deve implementar SNMP v1/v2/v3

1.1.11.8. LICENCIAMENTO

1.1.11.8.1.1. Deve ser fornecido com a versão de software mais atualizada disponível para o equipamento;

1.1.11.8.1.2. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integralde todas as funcionalidades especificadas;

1.1.11.9. SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO

1.1.11.9.1. A solução deve ser fornecida incluindo solução de gerenciamento centralizado conforme características e especificações descritas no ANEXO C;

1.1.12. SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM – TIPO 4

1.1.12.1. SERVIÇOS DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE LAN E SOFTWARE, INSTALAÇÃO, CONFIGURAÇÃO E TESTES.

1.1.12.1.1. A solução deve ser fornecida incluindo disponibilização de equipamentos e software, instalação, configuração e testes conforme características e especificações descritas no ANEXO D;

1.1.12.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.12.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte

técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO F;

1.1.12.3. REQUISITOS TÉCNICOS

1.1.12.3.1. Deve possuir no mínimo 12 portas 10/100/1000BaseT Gigabit Ethernet BaseT

1.1.12.3.2. Deve possuir 1 portas adicionais híbridas com velocidade de 1/10G BaseT e/ou 1/10G SFP+;

1.1.12.3.3. Deve implementar PoE e PoE+ (Power over Ethernet) de acordo com o padrão IEEE 803.3af e IEEE 802.3at;

1.1.12.3.4. Deve possuir no mínimo 130 watts destinados as portas com PoE+ ativo;

1.1.12.3.5. Deve possuir 1 interface RJ-45, USB-C ou serial para acesso console local

1.1.12.3.6. Deve possuir memória RAM de no mínimo 1GB;

1.1.12.3.7. Deve possuir buffer de pacotes de no mínimo 1MB;

1.1.12.3.8. Deve possuir capacidade de encaminhamento de no mínimo 44 Mpps;

1.1.12.3.9. Deve possuir capacidade de comutação de no mínimo 67 Gbps;

1.1.12.3.10. O switch deve ser do tipo empilhável, com altura máxima de 1RU e instalação em rack (19”). Deve acompanhar todos os componentes necessários para sua fixação no rack;

1.1.12.3.11. Deve possuir fonte de alimentação interna 100/240VAC

1.1.12.3.12. Deve possuir Certificado de Homologação na Anatel, de acordo com a Resolução nº 242;

1.1.12.3.13. FUNCIONALIDADES DE CAMADA 2

1.1.12.3.13.1. Deve implementar VLAN 802.1Q;

1.1.12.3.13.2. Deve implementar suporte a Jumbo Packets de pelo menos 9000 bytes;

1.1.12.3.13.3. Deve implementar Port Mirroring com no mínimo 4 grupos de espelhamento;

1.1.12.3.13.4. Deve implementar funcionalidade que permita a detecção de links unidirecionais;

1.1.12.3.13.5. Deve implementar 4094 VLAN Ids

1.1.12.3.13.6. Deve suportar 256 VLANS configuradas simultaneamente

1.1.12.3.13.7. Deve implementar MVRP (IEEE 802.1Ak);

1.1.12.3.13.8. Deve implementar LLDP (IEEE 802.1ab);

1.1.12.3.13.9. Deve implementar LLDP-MED;

1.1.12.3.13.10. Deve implementar MSTP (IEEE 802.1s);

5.1.4.3.13.11. Possuir tabela ARP de pelo menos 1024 entradas

5.1.4.3.13.12. Deve possuir capacidade mínima da tabela MAC de 8 mil entradas

1.1.12.3.14. FUNCIONALIDADES DE CAMADA 3

1.1.12.3.14.1. Deve implementar roteamento estático;

1.1.12.3.14.2. Deve suportar dual stack

1.1.12.3.14.3. Deve suportar DHCP Client para IPv4 e IPv6

1.1.12.3.14.4. Deve suportar no mínimo 512 rotas IPV4 e 512 rotas IPv6

1.1.12.4. MULTICAST

1.1.12.4.1.1. Deve implementar MLD snooping;

1.1.12.4.1.2. Deve implementar IGMP v2 e v3 (RFC 2236 e RFC 3376);

1.1.12.5. QOS E ACL

1.1.12.5.1.1. Deve implementar a função de rate limit configurado por porta;

1.1.12.5.1.2. Deve implementar Strict priority (SP) queuing

1.1.12.5.1.3. Deve implementar priorização de tráfego em tempo real

1.1.12.5.1.4. Deve implementar priorização de tráfego com no mínimo os seguintes parâmetros: endereço IP, Tipo de Serviço, Número da porta TCP/UDP, porta de origem e Diffserv.

1.1.12.5.1.5. Deve suporta no mínimo oito filas por porta

1.1.12.5.1.6. Deve suportar ACL para IPv4 e IPv6;

1.1.12.5.1.7. Deve implementar ACL com base no IP de origem e destino, porta TCP e UDP de origem e destino baseada em VLAN ou por Porta.

1.1.12.6. SEGURANÇA

1.1.12.6.1.1. Deve implementar TACACS+ e/ou RADIUS;

1.1.12.6.1.2. Deve implementar IEEE 802.1x;

1.1.12.6.1.3. Deve implementar autenticação baseada em web;

1.1.12.6.1.4. Deve implementar autenticação baseada em endereço MAC;

1.1.12.6.1.5. Deve implementar proteção contra-ataques na CPU do switch para prevenção de desligamento do equipamento.

1.1.12.6.1.6. Deve implementar SSHv2;

1.1.12.7. GERENCIAMENTO

1.1.12.7.1.1. Deve implementar NTP;

1.1.12.7.1.2. Deve suportar duas imagens de software na flash;

1.1.12.7.1.3. Deve suportar múltiplos arquivos de configuração na flash (mais de um arquivo);

1.1.12.7.1.4. deve suportar detecção de falha e link entre switches;

1.1.12.7.1.5. Deve implementar sFlow;

1.1.12.7.1.6. Deve possuir interface web e/ou via linha de comando para configuração;

1.1.12.7.1.7. Deve implementar Syslog;

1.1.12.7.1.8. Deve implementar TFTP e/ou SFTP;

1.1.12.7.1.9. Deve suportar RMON

1.1.12.7.1.10. Deve suportar Ping e/ou Traceroute para IPv4 e IPv6

1.1.12.7.1.11. Deve implementar SNMP v1/v2/v3

1.1.12.8. LICENCIAMENTO

1.1.12.8.1.1. Deve ser fornecido com a versão de software mais completa disponível para o equipamento;

1.1.12.8.1.2. Deve ser fornecido com todas as licenças de software necessárias para o funcionamento integral de todas as funcionalidades especificadas;

1.1.12.9. SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO

1.1.12.9.1. A solução deve ser fornecida incluindo solução de gerenciamento centralizado conforme características e especificações descritas no ANEXO C;

1.1.13. SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - PONTO DE ACESSO

DE REDE SEM FIO WIFI INTERNO TIPO 1

1.1.13.1. SERVIÇOS DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIADE WLAN E SOFTWARE, INSTALAÇÃO, CONFIGURAÇÃO E TESTES

1.1.13.1.1. a solução deve ser fornecida incluindo disponibilização de equipamentos e software, instalação, configuração e testes conforme características e especificações descritas no ANEXO E;

1.1.13.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.13.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO F;

1.1.13.3. REQUISITOS TÉCNICOS

1.1.13.3.1. Equipamento de Ponto de Acesso para rede local sem fio com três rádios, configurável via software, com funcionamento simultâneo em pelo menos 02 (dois) rádios nos padrões IEEE 802.11a/n/ac/ax em 5GHz, padrão IEEE 802.11ax em 6GHz, e IEEE 802.11b/g/n/ax em 2.4GHz;

1.1.13.3.2. Os pontos de acesso deverão possuir certificado emitido pelo Wi-Fi Alliance comprovando os seguintes padrões, protocolos e funcionalidades:

1.1.13.3.2.1. IEEE 802.11a;
1.1.13.3.2.2. IEEE 802.11b;
1.1.13.3.2.3. IEEE 802.11g;
1.1.13.3.2.4. IEEE 802.11n;
1.1.13.3.2.5. IEEE 802.11ac;
1.1.13.3.2.6. IEEE 802.11ax;
1.1.13.3.2.7. Wi-Fi 6E;
1.1.13.3.2.8. WPA, WPA2 e WPA3;
1.1.13.3.2.9. Passpoint;
1.1.13.3.2.10. WMM, WMM-PS, Wi-Fi Agile Multiband;

1.1.13.4. ESPECIFICAÇÕES DE RADIO

1.1.13.4.1. Deve permitir, simultaneamente, usuários configurados nos padrões IEEE 802.11a, 802.11b, 802.11g, 802.11n, 801.11ac e 802.11ax;

1.1.13.4.2. Implementar as seguintes taxas de transmissão (Mbps) e com fallback automático:

1.1.13.4.2.1. 802.11b: 1 a 11;
1.1.13.4.2.2. 802.11a/g: 6 a 54;
1.1.13.4.2.3. 802.11n: 6.5 a 300;
1.1.13.4.2.4. 802.11ac: 6.5 a 867;
1.1.13.4.2.5. 802.11ax (2.4GHz): 3.6 a 574;
1.1.13.4.2.6. 802.11ax (5GHz): 3.6 a 1.201;
1.1.13.4.2.7. 802.11ax (6GHz): 3.6 a 2.402;

1.1.13.4.3. Deve suportar 802.11n high-throughput (HT): HT20/40;

1.1.13.4.4. Deve suportar 802.11ac very high throughput (VHT): VHT20/40/80;

1.1.13.4.5. Deve suportar 802.11ax high efficiency (HE): HE20/40/80/160;

1.1.13.4.6. Deve suportar 802.11n/ac packet aggregation: A-MPDU, A-MSDU;

1.1.13.4.7. Operar nas seguintes tecnologias de rádio:

1.1.13.4.7.1. 802.11b: Direct-sequence spread-spectrum (DSSS);

1.1.13.4.7.2. 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM);

1.1.13.4.7.3. 802.11ax: Orthogonal frequency-division multiple access (OFDMA);

1.1.13.4.8. Operar nos seguintes tipos de modulação:

1.1.13.4.8.1. 802.11b: BPSK, QPSK, CCK;

1.1.13.4.8.2. 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM;

1.1.13.4.8.3. 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM;

1.1.13.4.8.4. 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM;

1.1.13.4.9. Possuir capacidade de selecionar automaticamente o canal de transmissão - DFS;

1.1.13.4.10. Deve implementar 802.11ax TWT (Target Wait Time) para suportar dispositivos de baixa potência;

1.1.13.4.11. Deve implementar 802.11mc FTM (Fine Timing Measurement) para alcance de distância de precisão;

1.1.13.4.12. Suportar até 512 clientes associados por rádio;

1.1.13.4.13. Possuir suporte a pelo menos 16 SSIDs em 2.4GHz e 5GHz, e 4 SSIDs em 6GHz;

1.1.13.4.14. Possuir antenas integradas ao equipamento, com padrão de irradiação omnidirecional, tri-band, com ganho de, pelo menos, 2.7 dBi em 2.4GHz, com ganho de, pelo menos, 4.3 dBi em 5GHz, e com ganho de, pelo menos, 4.3 dBi em 6GHz;

1.1.13.4.15. Deve suportar, utilizando a modulação OFDMA, a capacidade de transmitir simultaneamente clientes por canal, independente do dispositivo ou tipo de tráfego;

1.1.13.4.16. Deve suportar utilização de duas das três bandas 2.4GHz, 5GHz e 6GHz disponíveis, permitindo uma flexibilidade máxima na seleção de canais de 2.4 GHz, 5 GHz ou 6 GHz;

1.1.13.4.17. Deve possuir uma interface Bluetooth Low Energy (BLE 5.0) integrada, com as seguintes características:

1.1.13.4.17.1. No mínimo 5dBm de potência de transmissão (class 1) e -100 dBm de sensibilidaade de recepção de sinal;

1.1.13.4.17.2. Deve possuir uma interface IoT (Internet of Things) tipo Zigbee, Lora ou similar integrada;

1.1.13.4.18. Deve ser de arquitetura tri rádio 2.4GHz, 5GHz e 6GHz, podendo operar simultaneamente em dois rádios com MIMO 2x2;

1.1.13.4.19. Deve suportar operação em 2.4GHz com 02 (dois) Spatial Streams Single User (SU) MIMO, com taxa de transmissão de dados de até 565Mbps;

1.1.13.4.20. Deve suportar operação em 5GHz com 02 (dois) Spatial Streams Single User

(SU) MIMO, com taxa de transmissão de dados de até 1.18Gbps;

1.1.13.4.21. Deve suportar operação em 6GHz com 02 (dois) Spatial Streams Single User (SU) MIMO, com taxa de transmissão de dados de até 2.38Gbps;

1.1.13.4.22. Os equipamentos APs devem possuir funcionalidade de coexistência com redes celulares de forma a minimizar as interferências das mesmas;

1.1.13.4.23. Possuir potência máxima de transmissão para frequências de 2.4GHz de no mínimo +20 dBm;

1.1.13.4.24. Possuir potência máxima de transmissão para frequências de 5GHz de no mínimo +20 dBm;

1.1.13.4.25. Possuir potência máxima de transmissão para frequências de 6GHz de no mínimo +20 dBm;

1.1.13.4.26. Capacidade de configurar a potência de transmissão em incrementos de, pelo menos, 0.5 dBm;

1.1.13.5. MODOS DE OPERAÇÃO

1.1.13.5.1. Deve permitir funcionamento em modo autônomo/standalone sem a necessidade de gateway/controladora, e também deve permitir funcionamento em modo com gateway/controladora;

1.1.13.5.2. Deve permitir o gerenciamento através de plataforma nuvem (cloud);

1.1.13.5.3. Deve permitir o gerenciamento através de plataforma local (on-premise).

1.1.13.5.4. Para implementações em larga escala, o Ponto de Acesso deve configurar-se automaticamente ao ser conectado na rede, sendo provisionado através da ferramenta de gerenciamento;

1.1.13.6. OUTRAS INTERFACES

1.1.13.6.1. Possuir LEDs multicoloridos indicativos do estado de operação e da atividade do rádio;

1.1.13.6.2. Deve possuir 01 (uma) interface de rede RJ-45 100/1000/2500BASE-T ou superior;

1.1.13.6.3. Deve implementar PoE 802.3af/at (classe 3 ou superior);

1.1.13.6.4. Deve suportar 802.3az Energy Efficient Ethernet (EEE);

1.1.13.6.5. Deve operar em condições de temperatura entre 5ºC e 45ºC, e umidade entre 10% e 90%;

1.1.13.6.6. Possuir botão de reset que permita reset de fábrica do equipamento;

1.1.13.6.7. Possuir porta de console para gerenciamento e configuração via linha de comando CLI;

1.1.13.6.8. Possuir interface USB2.0;

1.1.13.6.9. Possuir slot de segurança Kensington;

1.1.13.6.10. Possuir estrutura que permita fixação do equipamento e fornecer acessórios para que possa ser feita a fixação em teto ou parede;

1.1.13.6.11. Suportar kits de montagem opcionais para instalar o AP em variedade de superfícies;

1.1.13.7. SEGURANÇA E REGULAMENTAÇÃO

1.1.13.7.1. O equipamento deverá possuir registro na ANATEL;

1.1.13.7.2. O certificado da ANATEL deverá ser apresentado na entrega do equipamento;

1.1.13.8. FUNCIONALIDADES GERAIS

1.1.13.8.1. Deve suportar a criação de arquitetura distribuída ou site único de rede sem fio.

1.1.13.8.2. Deve possuir arquitetura controlada com alta disponibilidade, em caso de falha da controladora principal, um novo controlador deve assumir o papel de controle das funcionalidades da rede WLAN.

1.1.13.8.3. Deve possuir suporte a gerenciamento baseado na web, utilizando os principais navegadores. (Microsoft Internet Explorer, Apple Safari, Google Chrome e Mozilla Firefox).

1.1.13.8.4. Deve permitir atualizações de firmware e configuração automática.

1.1.13.8.5. Deve permitir administrar todos os aspectos de segurança da rede WLAN através de firewall integrado à solução de rede sem fio;

1.1.13.8.6. Deve permitir a criação de regras de acesso baseado em aplicação e em categoria de aplicação.

1.1.13.8.7. Deve realizar o controle de autorização baseado em perfis de acesso, permitindo no mínimo 32 perfis;

1.1.13.8.8. Deve permitir que seja configurado um perfil de acesso, com regras aplicadas de firewall, para o qual será direcionado o usuário após sua autenticação;

1.1.13.8.9. Deve possuir gerenciamento e controle de uso de largura de banda, baseado em SERVIÇOS de utilização de banda ou perfil de acesso.

1.1.13.8.10. Deve permitir associar diferentes tipos de privilégios baseado em autenticação de máquina ou autenticação de usuário.

1.1.13.8.11. Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF;

1.1.13.8.12. Permitir habilitar e desabilitar a divulgação do SSID;

1.1.13.8.13. Permitir habilitar e desabilitar o SSID;

1.1.13.8.14. Implementar diferentes tipos de combinações encriptação/autenticação por SSID;

1.1.13.8.15. Implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;

1.1.13.8.16. Suporte a IPv6;

1.1.13.8.17. Possuir modo dedicado de funcionamento de análise de espectro das faixas de frequência de 2.4 e 5 GHz identificando fontes de interferência nessas faixas;

1.1.13.8.18. Possibilitar análise de espectro nos canais em que estiver provendo acesso;

1.1.13.8.19. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet ou serial (terminal assíncrono);

1.1.13.8.20. Implementar cliente DHCP para configuração automática de rede;

1.1.13.8.21. Deve configurar-se automaticamente ao ser conectado na rede;

1.1.13.8.22. Implementar varredura de RF nas frequências 2.4GHz e 5GHz, para identificação de interferências em dispositivos Wi-Fi, bem como também em dispositivos não Wi-Fi como Bluetooth, Forno Microondas, Telefone sem Fio, entre outros;

1.1.13.8.23. Implementar IEEE 802.1x, com pelo menos os seguintes métodos EAP: EAP-TLS, PEAP-MSCHAPv2;

1.1.13.8.24. Permitir a integração com RADIUS Server com suporte aos métodos EAP citados;

1.1.13.8.25. Implementar WPA com algoritmo de criptografia TKIP e/ou MIC;

1.1.13.8.26. Implementar WPA2 com algoritmo de criptografia AES 128, IEEE 802.11i;

1.1.13.8.27. Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CCM-256 e/ou SAE-AES;

1.1.13.9. SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO

1.1.13.9.1. A solução deve ser fornecida incluindo solução de gerenciamento centralizado conforme características e especificações descritas no ANEXO C;

1.1.14. SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - PONTO DE ACESSO DE REDE SEM FIO WIFI INTERNO TIPO 2

1.1.14.1. SERVIÇOS DE DISPONIBILIZAÇÃO DE CONECTIVIDADE WLAN E SOFTWARE, INSTALAÇÃO, CONFIGURAÇÃO E TESTES

1.1.14.1.1. A solução deve ser fornecida incluindo disponibilização de equipamentos e software, instalação, configuração e testes conforme características e especificações descritas no ANEXO E;

1.1.14.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.14.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO F;

1.1.14.3. REQUISITOS TÉCNICOS

1.1.14.3.1. Equipamento de Ponto de Acesso para rede local sem fio com três rádios, configurável via software, com funcionamento simultâneo em pelo menos 02 (dois) rádios nos padrões IEEE 802.11a/n/ac/ax em 5GHz, padrão IEEE 802.11ax em 6GHz, e IEEE 802.11b/g/n/ax em 2.4GHz;

1.1.14.3.2. Os pontos de acesso deverão possuir certificado emitido pelo Wi-Fi Alliance comprovando os seguintes padrões, protocolos e funcionalidades:

1.1.14.3.2.1. IEEE 802.11a;

1.1.14.3.2.2. IEEE 802.11b;

1.1.14.3.2.3. IEEE 802.11g;

1.1.14.3.2.4. IEEE 802.11n;

1.1.14.3.2.5. IEEE 802.11ac;

1.1.14.3.2.6. IEEE 802.11ax;

1.1.14.3.2.7. Wi-Fi 6E;

1.1.14.3.2.8. WPA, WPA2 e WPA3;

1.1.14.3.2.9. Passpoint;

1.1.14.3.2.10. WMM, WMM-PS, Wi-Fi Agile Multiband;

1.1.14.4. ESPECIFICAÇÕES DE RADIO

1.1.14.4.1. Deve permitir, simultaneamente, usuários configurados nos padrões IEEE 802.11a, 802.11b, 802.11g, 802.11n, 801.11ac e 802.11ax;

1.1.14.4.2. Implementar as seguintes taxas de transmissão (Mbps) e com fallback automático:

1.1.14.4.2.1. 802.11b: 1 a 11;
1.1.14.4.2.2. 802.11a/g: 6 a 54;
1.1.14.4.2.3. 802.11n: 6.5 a 300;
1.1.14.4.2.4. 802.11ac: 6.5 a 867;
1.1.14.4.2.5. 802.11ax (2.4GHz): 3.6 a 574;
1.1.14.4.2.6. 802.11ax (5GHz): 3.6 a 1.201;
1.1.14.4.2.7. 802.11ax (6GHz): 3.6 a 2.402;

1.1.14.4.3. Deve suportar 802.11n high-throughput (HT): HT20/40;
1.1.14.4.4. Deve suportar 802.11ac very high throughput (VHT): VHT20/40/80;
1.1.14.4.5. Deve suportar 802.11ax high efficiency (HE): HE20/40/80/160;
1.1.14.4.6. Deve suportar 802.11n/ac packet aggregation: A-MPDU, A-MSDU;
1.1.14.4.7. Operar nas seguintes tecnologias de rádio:
1.1.14.4.7.1. 802.11b: Direct-sequence spread-spectrum (DSSS);
1.1.14.4.7.2. 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM);
1.1.14.4.7.3. 802.11ax: Orthogonal frequency-division multiple access (OFDMA);
1.1.14.4.8. Operar nos seguintes tipos de modulação:
1.1.14.4.8.1. 802.11b: BPSK, QPSK, CCK;
1.1.14.4.8.2. 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM;
1.1.14.4.8.3. 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM;
1.1.14.4.8.4. 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM;
1.1.14.4.9. Possuir capacidade de selecionar automaticamente o canal de transmissão - DFS;
1.1.14.4.10. Deve implementar 802.11ax TWT (Target Wait Time) para suportar dispositivos de baixa potência;
1.1.14.4.11. Deve implementar 802.11mc FTM (Fine Timing Measurement) para alcance de distância de precisão;
1.1.14.4.12. Suportar até 512 clientes associados por rádio;
1.1.14.4.13. Possuir suporte a pelo menos 16 SSIDs em 2.4GHz e 5GHz, e 4 SSIDs em 6GHz;
1.1.14.4.14. Possuir antenas integradas ao equipamento, com padrão de irradiação omnidirecional, tri-band, com ganho de, pelo menos, 4.4 dBi em 2.4GHz, com ganho de, pelo menos, 6.5 dBi em 5GHz, e com ganho de, pelo menos, 6.0 dBi em 6GHz;
1.1.14.4.15. Deve suportar, utilizando a modulação OFDMA, a capacidade de transmitir simultaneamente clientes por canal, independente do dispositivo ou tipo de tráfego;
1.1.14.4.16. Deve suportar utilização das três bandas 2.4GHz, 5GHz e 6GHz, permitindo uma flexibilidade máxima na seleção de canais de 5 GHz e 6 GHz sem degradação do desempenho;
1.1.14.4.17. Deve possuir uma interface Bluetooth Low Energy (BLE 5.0) integrada, com as seguintes características:
1.1.14.4.17.1. No mínimo 5dBm de potência de transmissão (class 1) e -100 dBm

de sensibilidade de recepção de sinal;

1.1.14.4.17.2. Deve possuir uma interface IoT (Internet of Things) tipo Zigbee, Lora ou similar integrada;

1.1.14.4.18. Deve operar em 2.4GHz, 5GHz e 6GHz simultaneamente com MIMO 2x2;

1.1.14.4.19. Deve suportar operação em 2.4GHz com 02 (dois) Spatial Streams Single User (SU) MIMO, com taxa de transmissão de dados de até 570Mbps;

1.1.14.4.20. Deve suportar operação em 5GHz com 02 (dois) Spatial Streams Single User (SU) MIMO, com taxa de transmissão de dados de até 1.15Gbps;

1.1.14.4.21. Deve suportar operação em 6GHz com 02 (dois) Spatial Streams Single User (SU) MIMO, com taxa de transmissão de dados de até 2.38Gbps;

1.1.14.4.22. Os equipamentos APs devem possuir funcionalidade de coexistência com redes celulares de forma a minimizar as interferências das mesmas;

1.1.14.4.23. Possuir potência máxima de transmissão para frequências de 2.4GHz de no mínimo +20 dBm;

1.1.14.4.24. Possuir potência máxima de transmissão para frequências de 5GHz de no mínimo +20 dBm;

1.1.14.4.25. Possuir potência máxima de transmissão para frequências de 6GHz de no mínimo +20 dBm;

1.1.14.4.26. Capacidade de configurar a potência de transmissão em incrementos de, pelo menos, 0.5 dBm;

1.1.14.5. MODOS DE OPERAÇÃO

1.1.14.5.1. Deve permitir funcionamento em modo autônomo/standalone sem a necessidade de gateway/controladora, e também deve permitir funcionamento em modo com gateway/controladora;

1.1.14.5.2. Deve permitir o gerenciamento através de plataforma nuvem (cloud);

1.1.14.5.3. Deve permitir o gerenciamento através de plataforma local (on-premise).

1.1.14.5.4. Para implementações em larga escala, o Ponto de Acesso deve configurar-se automaticamente ao ser conectado na rede, sendo provisionado através da ferramenta de gerenciamento;

1.1.14.6. OUTRAS INTERFACES

1.1.14.6.1. Possuir LEDs multicoloridos indicativos do estado de operação e da atividade do rádio;

1.1.14.6.2. Deve possuir 02 (duas) interfaces de rede RJ-45 100/1000/2500BASE-T ou superior;

1.1.14.6.3. Suportar a funcionalidade de Link Aggregation (LACP) nas portas de uplink para redundância ou aumento de capacidade;

1.1.14.6.4. Deve implementar PoE 802.3af/at (classe 3 ou superior);

1.1.14.6.5. Deve suportar 802.3az Energy Efficient Ethernet (EEE);

1.1.14.6.6. Deve operar em condições de temperatura entre 5ºC e 45ºC, e umidade entre 10% e 90%;

1.1.14.6.7. Possuir botão de reset que permita reset de fábrica do equipamento;

1.1.14.6.8. Possuir porta de console para gerenciamento e configuração via linha de comando CLI;

1.1.14.6.9. Possuir interface USB2.0;

1.1.14.6.10. Possuir slot de segurança Kensington;

1.1.14.6.11. Possuir estrutura que permita fixação do equipamento e fornecer acessórios para que possa ser feita a fixação em teto ou parede;

1.1.14.6.12. Suportar kits de montagem opcionais para instalar o AP em variedade de superfícies;

1.1.14.7. SEGURANÇA E REGULAMENTAÇÃO

1.1.14.7.1. O equipamento deverá possuir registro na ANATEL;

1.1.14.7.2. O certificado da ANATEL deverá ser apresentado na entrega do equipamento;

1.1.14.8. FUNCIONALIDADES GERAIS

1.1.14.8.1. Deve suportar a criação de arquitetura distribuída ou site único de rede sem fio.

1.1.14.8.2. Deve possuir arquitetura controlada com alta disponibilidade, em caso de falha da controladora principal, um novo controlador deve assumir o papel de controle das funcionalidades da rede WLAN.

1.1.14.8.3. Deve possuir suporte a gerenciamento baseado na web, utilizando os principais navegadores. (Microsoft Internet Explorer, Apple Safari, Google Chrome e Mozilla Firefox).

1.1.14.8.4. Deve permitir atualizações de firmware e configuração automática.

1.1.14.8.5. Deve permitir administrar todos os aspectos de segurança da rede WLAN através de firewall integrado à solução de rede sem fio;

1.1.14.8.6. Deve permitir a criação de regras de acesso baseado em aplicação e em categoria de aplicação.

1.1.14.8.7. Deve realizar o controle de autorização baseado em perfis de acesso, permitindo no mínimo 32 perfis;

1.1.14.8.8. Deve permitir que seja configurado um perfil de acesso, com regras aplicadas de firewall, para o qual será direcionado o usuário após sua autenticação;

1.1.14.8.9. Deve possuir gerenciamento e controle de uso de largura de banda, baseado em SERVIÇOS de utilização de banda ou perfil de acesso.

1.1.14.8.10. Deve permitir associar diferentes tipos de privilégios baseado em autenticação de máquina ou autenticação de usuário.

1.1.14.8.11. Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF;

1.1.14.8.12. Permitir habilitar e desabilitar a divulgação do SSID;

1.1.14.8.13. Permitir habilitar e desabilitar o SSID;

1.1.14.8.14. Implementar diferentes tipos de combinações encriptação/autenticação por SSID;

1.1.14.8.15. Implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;

1.1.14.8.16. Suporte a IPv6;

1.1.14.8.17. Possuir modo dedicado de funcionamento de análise de espectro das faixas de frequência de 2.4 e 5 GHz identificando fontes de interferência nessas faixas;

1.1.14.8.18. Possibilitar análise de espectro nos canais em que estiver provendo acesso;

1.1.14.8.19. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet ou serial (terminal assíncrono);

1.1.14.8.20. Implementar cliente DHCP para configuração automática de rede;

1.1.14.8.21. Deve configurar-se automaticamente ao ser conectado na rede;

1.1.14.8.22. Implementar varredura de RF nas frequências 2.4GHz e 5GHz, para identificação de interferências em dispositivos Wi-Fi, bem como também em dispositivos não Wi-Fi como Bluetooth, Forno Microondas, Telefone sem Fio, entre outros;

1.1.14.8.23. Implementar IEEE 802.1x, com pelo menos os seguintes métodos EAP: EAP-TLS, PEAP-MSCHAPv2;

1.1.14.8.24. Permitir a integração com RADIUS Server com suporte aos métodos EAP citados;

1.1.14.8.25. Implementar WPA com algoritmo de criptografia TKIP e/ou MIC;

1.1.14.8.26. Implementar WPA2 com algoritmo de criptografia AES 128, IEEE 802.11i;

1.1.14.8.27. Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CCM-256 e/ou SAE-AES;

1.1.14.9. SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO

1.1.14.9.1. A solução deve ser fornecida incluindo solução de gerenciamento centralizado conforme características e especificações descritas no ANEXO C;

1.1.15. SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - PONTO DE ACESSO DE REDE SEM FIO WIFI INTERNO TIPO 3

1.1.15.1. SERVIÇOS DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE WLAN E SOFTWARE, INSTALAÇÃO, CONFIGURAÇÃO E TESTES

1.1.15.1.1. A solução deve ser fornecida incluindo disponibilização de equipamentos e software, instalação, configuração e testes conforme características e especificações descritas no ANEXO E;

1.1.15.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.15.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO F;

1.1.15.3. REQUISITOS TÉCNICOS

1.1.15.3.1. Equipamento de Ponto de Acesso para rede local sem fio com três rádios, configurável via software, com funcionamento simultâneo em pelo menos 02 (dois) rádios nos padrões IEEE 802.11a/n/ac/ax em 5GHz, padrão IEEE 802.11ax em 6GHz, e IEEE 802.11b/g/n/ax em 2.4GHz;

1.1.15.3.2. Os pontos de acesso deverão possuir certificado emitido pelo Wi-Fi Alliance comprovando os seguintes padrões, protocolos e funcionalidades:

1.1.15.3.2.1. IEEE 802.11a;

1.1.15.3.2.2. IEEE 802.11b;

1.1.15.3.2.3. IEEE 802.11g;

1.1.15.3.2.4. IEEE 802.11n;

1.1.15.3.2.5. IEEE 802.11ac;

1.1.15.3.2.6. IEEE 802.11ax;

1.1.15.3.2.7. Wi-Fi 6E;

1.1.15.3.2.8. WPA, WPA2 e WPA3;
1.1.15.3.2.9. Passpoint;
1.1.15.3.2.10. WMM, WMM-PS, Wi-Fi Agile Multiband;

1.1.15.4. ESPECIFICAÇÕES DE RADIO

1.1.15.4.1. Deve permitir, simultaneamente, usuários configurados nos padrões IEEE 802.11a, 802.11b, 802.11g, 802.11n, 801.11ac e 802.11ax;
1.1.15.4.2. Implementar as seguintes taxas de transmissão (Mbps) e com fallback automático:
1.1.15.4.2.1. 802.11b: 1 a 11;
1.1.15.4.2.2. 802.11a/g: 6 a 54;
1.1.15.4.2.3. 802.11n: 6.5 a 600;
1.1.15.4.2.4. 802.11ac: 6.5 a 1.733;
1.1.15.4.2.5. 802.11ax (2.4GHz): 3.6 a 1.147;
1.1.15.4.2.6. 802.11ax (5GHz): 3.6 a 2.402;
1.1.15.4.2.7. 802.11ax (6GHz): 3.6 a 4.804;
1.1.15.4.3. Deve suportar 802.11n high-throughput (HT): HT20/40;
1.1.15.4.4. Deve suportar 802.11ac very high throughput (VHT): VHT20/40/80/160 (80+80);
1.1.15.4.5. Deve suportar 802.11ax high efficiency (HE): HE20/40/80/160;
1.1.15.4.6. Deve suportar 802.11n/ac packet aggregation: A-MPDU, A-MSDU;
1.1.15.4.7. Operar nas seguintes tecnologias de rádio:
1.1.15.4.7.1. 802.11b: Direct-sequence spread-spectrum (DSSS);
1.1.15.4.7.2. 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM);
1.1.15.4.7.3. 802.11ax: Orthogonal frequency-division multiple access (OFDMA);
1.1.15.4.8. Operar nos seguintes tipos de modulação:
1.1.15.4.8.1. 802.11b: BPSK, QPSK, CCK;
1.1.15.4.8.2. 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM;
1.1.15.4.8.3. 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM;
1.1.15.4.8.4. 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM;
1.1.15.4.9. Possuir capacidade de selecionar automaticamente o canal de transmissão - DFS;
1.1.15.4.10. Deve implementar 802.11ax TWT (Target Wait Time) para suportar dispositivos de baixa potência;
1.1.15.4.11. Deve implementar 802.11mc FTM (Fine Timing Measurement) para alcance de distância de precisão;
1.1.15.4.12. Suportar até 512 clientes associados por rádio;
1.1.15.4.13. Possuir suporte a pelo menos 16 SSIDs em 2.4GHz e 5GHz, e 4 SSIDs em 6GHz;
1.1.15.4.14. Possuir antenas integradas ao equipamento, com padrão de irradiação omnidirecional, tri-band, com ganho de, pelo menos, 4.6 dBi em 2.4GHz, com ganho de, pelo menos, 5.2 dBi em 5GHz, e com ganho de, pelo menos, 5.3 dBi em 6GHz;

1.1.15.4.15. Deve suportar, utilizando a modulação OFDMA, a capacidade de transmitir simultaneamente clientes por canal, independente do dispositivo ou tipo de tráfego;

1.1.15.4.16. Deve suportar utilização das três bandas 2.4GHz, 5GHz e 6GHz, permitindo uma flexibilidade máxima na seleção de canais de 5 GHz e 6 GHz sem degradação do desempenho;

1.1.15.4.17. Deve possuir uma interface Bluetooth Low Energy (BLE 5.0) integrada, com as seguintes características:

1.1.15.4.17.1. No mínimo 5dBm de potência de transmissão (class 1) e -100 dBm de sensibilidade de recepção de sinal;

1.1.15.4.17.2. Deve possuir uma interface IoT (Internet of Things) tipo Zigbee, Lora ou similar integrada;

1.1.15.4.18. Deve operar em 2.4GHz, 5GHz e 6GHz simultaneamente com MIMO 4x4;

1.1.15.4.19. Deve suportar operação em 2.4GHz com 04 (quatro) Spatial Streams MIMO, com taxa de transmissão de dados de até 1 Gbps;

1.1.15.4.20. Deve suportar operação em 5GHz com 04 (quatro) Spatial Streams MIMO, com taxa de transmissão de dados de até 2.2 Gbps;

1.1.15.4.21. Deve suportar operação em 6GHz com 04 (quatro) Spatial Streams MIMO, com taxa de transmissão de dados de até 4.6 Gbps;

1.1.15.4.22. Deve suportar Multi User (MU) MIMO com downlink e uplink em 5GHz e 6GHz, e Multi User (MU) MIMO com downlink em 2.4GHz;

1.1.15.4.23. Os equipamentos APs devem possuir funcionalidade de coexistência com redes celulares de forma a minimizar as interferências das mesmas;

1.1.15.4.24. Possuir potência máxima de transmissão para frequências de 2.4GHz de no mínimo +23 dBm;

1.1.15.4.25. Possuir potência máxima de transmissão para frequências de 5GHz de no mínimo +23 dBm;

1.1.15.4.26. Possuir potência máxima de transmissão para frequências de 6GHz de no mínimo +23 dBm;

1.1.15.4.27. Capacidade de configurar a potência de transmissão em incrementos de, pelo menos, 0.5 dBm;

1.1.15.5. MODOS DE OPERAÇÃO

1.1.15.5.1. Deve permitir funcionamento em modo autônomo/standalone sem a necessidade de gateway/controladora, e também deve permitir funcionamento em modo com gateway/controladora;

1.1.15.5.2. Deve permitir o gerenciamento através de plataforma nuvem (cloud);

1.1.15.5.3. Deve permitir o gerenciamento através de plataforma local (on-premise).

1.1.15.5.4. Para implementações em larga escala, o Ponto de Acesso deve configurar-se automaticamente ao ser conectado na rede, sendo provisionado através da ferramenta de gerenciamento;

1.1.15.6. OUTRAS INTERFACES

1.1.15.6.1. Possuir LEDs multicoloridos indicativos do estado de operação e da atividade do rádio;

1.1.15.6.2. Deve possuir 02 (duas) interfaces de rede RJ-45 100/1000/2500BASE-T ou superior;

1.1.15.6.3. Suportar a funcionalidade de Link Aggregation (LACP) nas portas de uplink para redundância ou aumento de capacidade;

1.1.15.6.4. Deve implementar PoE 802.3af/at (classe 3 ou superior);

1.1.15.6.5. Deve suportar 802.3az Energy Efficient Ethernet (EEE);

1.1.15.6.6. Deve operar em condições de temperatura entre 5ºC e 45ºC, e umidade entre 10% e 90%;

1.1.15.6.7. Possuir botão de reset que permita reset de fábrica do equipamento;

1.1.15.6.8. Possuir porta de console para gerenciamento e configuração via linha de comando CLI;

1.1.15.6.9. Possuir interface USB2.0;

1.1.15.6.10. Possuir slot de segurança Kensington;

1.1.15.6.11. Possuir estrutura que permita fixação do equipamento e fornecer acessórios para que possa ser feita a fixação em teto ou parede;

1.1.15.6.12. Suportar kits de montagem opcionais para instalar o AP em variedade de superfícies;

1.1.15.7. SEGURANÇA E REGULAMENTAÇÃO

1.1.15.7.1. O equipamento deverá possuir registro na ANATEL;

1.1.15.7.2. O certificado da ANATEL deverá ser apresentado na entrega do equipamento;

1.1.15.8. FUNCIONALIDADES GERAIS

1.1.15.8.1. Deve suportar a criação de arquitetura distribuída ou site único de rede sem fio.

1.1.15.8.2. Deve possuir arquitetura controlada com alta disponibilidade, em caso de falha da controladora principal, um novo controlador deve assumir o papel de controle das funcionalidades da rede WLAN.

1.1.15.8.3. Deve possuir suporte a gerenciamento baseado na web, utilizando os principais navegadores. (Microsoft Internet Explorer, Apple Safari, Google Chrome e Mozilla Firefox).

1.1.15.8.4. Deve permitir atualizações de firmware e configuração automática.

1.1.15.8.5. Deve permitir administrar todos os aspectos de segurança da rede WLAN através de firewall integrado à solução de rede sem fio;

1.1.15.8.6. Deve permitir a criação de regras de acesso baseado em aplicação e em categoria de aplicação.

1.1.15.8.7. Deve realizar o controle de autorização baseado em perfis de acesso, permitindo no mínimo 32 perfis;

1.1.15.8.8. Deve permitir que seja configurado um perfil de acesso, com regras aplicadas de firewall, para o qual será direcionado o usuário após sua autenticação;

1.1.15.8.9. Deve possuir gerenciamento e controle de uso de largura de banda, baseado em SERVIÇOS de utilização de banda ou perfil de acesso.

1.1.15.8.10. Deve permitir associar diferentes tipos de privilégios baseado em autenticação de máquina ou autenticação de usuário.

1.1.15.8.11. Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF;

1.1.15.8.12. Permitir habilitar e desabilitar a divulgação do SSID;

1.1.15.8.13. Permitir habilitar e desabilitar o SSID;

1.1.15.8.14. Implementar diferentes tipos de combinações encriptação/autenticação por

SSID;

1.1.15.8.15. Implementar padrão WMM da Wi-Fi Alliance para priorização de tráfego, suportando aplicações em tempo real, tais como, VoIP, vídeo, dentre outras;

1.1.15.8.16. Suporte a IPv6;

1.1.15.8.17. Possuir modo dedicado de funcionamento de análise de espectro das faixas de frequência de 2.4 e 5 GHz identificando fontes de interferência nessas faixas;

1.1.15.8.18. Possibilitar análise de espectro nos canais em que estiver provendo acesso;

1.1.15.8.19. Permitir a atualização remota do sistema operacional e arquivos de configuração utilizados no equipamento via interfaces ethernet ou serial (terminal assíncrono);

1.1.15.8.20. Implementar cliente DHCP para configuração automática de rede;

1.1.15.8.21. Deve configurar-se automaticamente ao ser conectado na rede;

1.1.15.8.22. Implementar varredura de RF nas frequências 2.4GHz e 5GHz, para identificação de interferências em dispositivos Wi-Fi, bem como também em dispositivos não Wi-Fi como Bluetooth, Forno Microondas, Telefone sem Fio, entre outros;

1.1.15.8.23. Implementar IEEE 802.1x, com pelo menos os seguintes métodos EAP: EAP-TLS, PEAP-MSCHAPv2;

1.1.15.8.24. Permitir a integração com RADIUS Server com suporte aos métodos EAP citados;

1.1.15.8.25. Implementar WPA com algoritmo de criptografia TKIP e/ou MIC;

1.1.15.8.26. Implementar WPA2 com algoritmo de criptografia AES 128, IEEE 802.11i;

1.1.15.8.27. Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CCM-256 e/ou SAE-AES;

1.1.15.9. SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO

1.1.15.9.1. A solução deve ser fornecida incluindo solução de gerenciamento centralizado conforme características e especificações descritas no ANEXO C;

1.1.16. SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - PONTO DE ACESSO DE REDE SEM FIO WIFI EXTERNO TIPO 4

1.1.16.1. SERVIÇOS DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE WLAN E SOFTWARE, INSTALAÇÃO, CONFIGURAÇÃO E TESTES

1.1.16.1.1. a solução deve ser fornecida incluindo disponibilização de equipamentos e software, instalação, configuração e testes conforme características e especificações descritas no ANEXO E;

1.1.16.2. SERVIÇO DE MANUTENÇÃO E SUPORTE TÉCNICO

1.1.16.2.1. A solução deve ser fornecida incluindo serviço de manutenção e suporte técnico a ser prestado pela CONTRATANTE, conforme características e especificações descritas no ANEXO F;

1.1.16.3. REQUISITOS TÉCNICOS

1.1.16.3.1. Equipamento de Ponto de Acesso Externo para rede sem fios, com

funcionamento simultâneo com dois rádios nos padrões IEEE 802.11a/n/ac em 5GHz e IEEE 802.11b/g/n/ax em 2.4GHz;

1.1.16.3.2. Os pontos de acesso deverão possuir certificado emitido pelo Wi-Fi Alliance comprovando os seguintes padrões, protocolos e funcionalidades:

1.1.16.3.2.1. IEEE 802.11a;
1.1.16.3.2.2. IEEE 802.11b;
1.1.16.3.2.3. IEEE 802.11g;
1.1.16.3.2.4. IEEE 802.11n;
1.1.16.3.2.5. IEEE 802.11ac;
1.1.16.3.2.6. IEEE 802.11ax;

1.1.16.4. ESPECIFICAÇÕES DE RADIO

1.1.16.4.1. Implementar as seguintes taxas de transmissão (Mbps) e com fallback automático:

1.1.16.4.1.1. 802.11b: 1 a 11;
1.1.16.4.1.2. 802.11a/g: 6 a 54;
1.1.16.4.1.3. 802.11n: 6.5 a 300;
1.1.16.4.1.4. 802.11ac: 6.5 a 867;
1.1.16.4.1.5. 802.11ax (2.4GHz): 3.6 a 574;

1.1.16.4.2. Deve suportar 802.11n high-throughput (HT): HT20/40;
1.1.16.4.3. Deve suportar 802.11ac very high throughput (VHT): VHT20/40/80
1.1.16.4.4. Deve suportar 802.11ax high efficiency (HE): HE20/40/80
1.1.16.4.5. Deve suportar 802.11n/ac/ax packet aggregation: A-MPDU, A-MSDU;
1.1.16.4.6. Operar nas seguintes tecnologias de radio:

1.1.16.4.6.1. 802.11b: Direct-sequence spread-spectrum (DSSS);
1.1.16.4.6.2. 802.11a/g/n/ac: Orthogonal frequency-division multiplexing (OFDM);
1.1.16.4.6.3. 802.11ax: Orthogonal frequency-division multiple access (OFDMA);

1.1.16.4.7. Operar nos seguintes tipos de modulação:

1.1.16.4.7.1. 802.11b: BPSK, QPSK, CCK;
1.1.16.4.7.2. 802.11a/g/n: BPSK, QPSK, 16-QAM, 64-QAM;
1.1.16.4.7.3. 802.11ac: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM;
1.1.16.4.7.4. 802.11ax: BPSK, QPSK, 16-QAM, 64-QAM, 256-QAM, 1024-QAM;

1.1.16.4.8. Suportar até 256 clientes associados por rádio;
1.1.16.4.9. Possuir suporte a pelo menos 16 SSIDs;
1.1.16.4.10. Possuir antenas internas integradas ao equipamento, com padrão de irradiação omnidirecional, dual-band, com ganho de, pelo menos, 3.1 dBi em 2.4GHz e com ganho de, pelo menos, 5.2 dBi em 5GHz;
1.1.16.4.11. Deve suportar, utilizando a modulação OFDMA, a capacidade de transmitir simultaneamente clientes por canal, com as seguintes possibilidades:
1.1.16.4.12. Deve operar em 5GHz e 2.4GHz 2x2 MIMO;
1.1.16.4.13. Deve suportar operação em dual-radio e em 5GHz com 02 (dois) Spatial Streams Single User (SU) MIMO, com taxa de transmissão de dados de até

1.1Gbps;

1.1.16.4.14. Deve suportar operação em tri-radio e em 2.4GHz com 02 (dois) Spatial Streams Single User (SU) MIMO, com taxa de transmissão de dados de até 565Mbps;

1.1.16.4.15. Os equipamentos APs devem possuir funcionalidade de coexistência com redes celulares de forma a minimizar as interferências das mesmas;

1.1.16.4.16. Possuir potência máxima de transmissão para frequências de 2.4GHz de no mínimo +22 dBm.

1.1.16.4.17. Possuir potência máxima de transmissão para frequências de 5GHz de no mínimo + 22 dBm.

1.1.16.5. Capacidade de configurar a potência de transmissão em incrementos de 0.5 dBm;

1.1.16.6. OUTRAS INTERFACES E GABINETE

1.1.16.6.1. Deverá possuir 1 (uma) interface ethernet, com velocidade de 10/100/1000 Mbps, utilizando conector RJ-45, para conexão à rede local;

1.1.16.6.2. Deve implementar PoE 802.3af/at (classe 3 ou superior);

1.1.16.6.3. Deve suportar 802.3az Energy Efficient Ethernet (EEE);

1.1.16.6.4. Deverá possuir, no mínimo, um rádio embarcado para IoT, o qual deve ser compatível com BLE ou ZigBee;

1.1.16.6.4.1. Caso não possua rádio embarcado para IoT, deverá dispor de uma porta USB para inserção de módulo IoT compatível com BLE ou ZigBee;

1.1.16.6.5. Deve operar em condições de temperatura entre -35ºC e 50ºC, e umidade entre 10% e 90%;

1.1.16.6.6. Resistência a água e poeira conforme IP66 e IP67;

1.1.16.6.7. Capacidade de tolerância à salinidade/maresia;

1.1.16.6.8. Possuir estrutura que permita fixação do equipamento e fornecer acessórios para que possa ser feita a fixação em poste;

1.1.16.7. SEGURANÇA E REGULAMENTAÇÃO

1.1.16.7.1. O equipamento deverá possuir registro na ANATEL;

1.1.16.7.2. O certificado da ANATEL deverá ser apresentado na entrega do equipamento;

1.1.16.8. FUNCIONALIDADES GERAIS

1.1.16.8.1. Deve permitir o gerenciamento através de controladora local e/ou utilizando solução de gerenciamento em nuvem pública do mesmo fabricante.

1.1.16.8.2. Deve suportar a criação de arquitetura distribuída ou site único de rede sem fio.

1.1.16.8.3. Deve possuir arquitetura controlada com alta disponibilidade, em caso de falha da controladora principal, um novo controlador deve assumir o papel de controle das funcionalidades da rede WLAN.

1.1.16.8.4. Deve ser capaz de gerenciar todos os APs baseado em grupo, devendo oferecer suporte a no mínimo 120 APs por grupo.

1.1.16.8.5. Deve possuir suporte a gerenciamento baseado na web, utilizando os principais navegadores. (Microsoft Internet Explorer, Apple Safari, Google Chrome e Mozilla Firefox)

1.1.16.8.6. Deve permitir atualizações de firmware e configuração automática.

1.1.16.8.7. Deve permitir administrar todos os aspectos de segurança da rede WLAN através de firewall integrado à solução de rede sem fio;

1.1.16.8.8. Deve permitir a criação de regras de acesso baseado em aplicação e em categoria de aplicação.

1.1.16.8.9. Deve realizar o controle de autorização baseado em perfis de acesso, permitindo no mínimo 32 perfis;

1.1.16.8.10. Deve permitir que seja configurado um perfil de acesso, com regras aplicadas de firewall, para o qual será direcionado o usuário após sua autenticação;

1.1.16.8.11. Deve possuir gerenciamento e controle de uso de largura de banda, baseado em SERVIÇOS de utilização de banda ou perfil de acesso.

1.1.16.8.12. Deve permitir associar diferentes tipos de privilégios baseado em autenticação de máquina ou autenticação de usuário.

1.1.16.8.13. Deve permitir o gerenciamento inteligente de potência;

1.1.16.8.14. Permitir o ajuste dinâmico de nível de potência e canal de rádio de modo a otimizar o tamanho da célula de RF;

1.1.16.8.15. Permitir habilitar e desabilitar a divulgação do SSID;

1.1.16.8.16. Permitir habilitar e desabilitar o SSID;

1.1.16.8.17. Implementar diferentes tipos de combinações encriptação/autenticação por SSID;

1.1.16.8.18. Implementar cliente DHCP para configuração automática de rede;

1.1.16.8.19. Deve configurar-se automaticamente ao ser conectado na rede;

1.1.16.8.20. Implementar varredura de RF nas frequências 2.4GHz e 5GHz, para identificação de interferências em dispositivos Wi-Fi, bem como também em dispositivos não Wi-Fi como Bluetooth, Forno Microondas, Telefone sem Fio, entre outros;

1.1.16.8.21. Implementar IEEE 802.1x, com pelo menos os seguintes métodos EAP: EAP-TLS, PEAP-MSCHAPv2;

1.1.16.8.22. Permitir a integração com RADIUS Server com suporte aos métodos EAP citados;

1.1.16.8.23. Implementar WPA com algoritmo de criptografia TKIP e/ou MIC;

1.1.16.8.24. Implementar WPA2 com algoritmo de criptografia AES 128, IEEE 802.11i;

1.1.16.8.25. Implementar WPA3 com algoritmo de criptografia AES-CCM-128, AES-CCM-256 e/ou SAE-AES;

1.1.16.9. SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO

1.1.16.9.1. A solução deve ser fornecida incluindo solução de gerenciamento centralizado conforme características e especificações descritas no ANEXOC;

1.1.17. INJETOR POE 802.3

1.1.17.1. CARACTERÍSTICAS GERAIS

1.1.17.1.1. Deve ser fabricado ou homolagado pelo mesmo fabricante dos Pontos de Acesso de Rede sem Fio dos **ITENS 11 AO 14;**

1.1.17.2. CARACTERÍSTICAS ESPECÍFICAS - INJETOR POE 802.3

1.1.17.2.1. Deve possuir potência de saída de, pelo menos, 30W;

1.1.17.2.2. Deve possuir uma porta de entrada Ethernet;

1.1.17.2.3. Deve possuir uma porta de saída PoE;

1.1.18. SOLUÇÃO DE POLÍTICA E AUTENTICAÇÃO DE USUÁRIOS DE REDE SEM FIO

1.1.18.1. SERVIÇOS DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE AUTENTICAÇÃO, INSTALAÇÃO, CONFIGURAÇÃO E TESTES

1.1.18.1.1. PLANEJAMENTO:

1.1.18.1.1.1. Reunião de Kick-off – Deve ser realizada em duas etapas: a primeira com a equipe de implementação, abordando aspectos técnicos, integração, comunicação, e a segunda com o cliente tratando as formas de acompanhamento ao longo do projeto e prazo;

1.1.18.1.1.2. Visão geral do projeto, a fim de alinhar os objetivos e metas técnicas;

1.1.18.1.1.3. Escopo do Projeto;

1.1.18.1.1.4. Principais Entregas;

1.1.18.1.1.5. Limites do Projeto;

1.1.18.1.1.6. Possíveis riscos que podem ocorrer, bem como um plano de prevenção e/ou recuperação;

1.1.18.1.1.7. Equipe de execução do Projeto;

1.1.18.1.1.8. Prioridade do Projeto;

1.1.18.1.1.9. Cronograma do Projeto;

1.1.18.1.1.10. Esclarecimento de dúvidas;

1.1.18.1.1.11. Reunião de Follow-up – Deve ser realizada pelo menos uma vez por semana durante o período de implementação do projeto. Poderá ser feita de forma remota;

1.1.18.1.1.12. Relato breve quantificando do status das principais atividades do projeto;

1.1.18.1.1.13. Apresentação de fatos e informações relevantes que permitam análise e acompanhamento do andamento do projeto;

1.1.18.1.1.14. Avaliação de possíveis sanções que poderão ser aplicadas caso ocorram atrasos ou imprevistos no projeto, especialmente as que envolvem qualidade do trabalho, cronograma e custos;

1.1.18.1.1.15. Reunião EndUp – Deve ser uma reunião formal a ser realizada ao término de todas as atividades do projeto, com a presença do cliente, gerente do projeto e equipe do projeto;

1.1.18.1.1.16. Descrição resumida do projeto, desde seu início até sua finalização;

1.1.18.1.1.17. Síntese das fases e marcos principais e caracterização do cumprimento de tudo que ficou acertado e aceito pelo cliente em cada fase;

1.1.18.1.1.18. Certificação de que o projeto que está sendo entregue neste momento cumpre todos os requisitos acordados no início, e/ou modificados e redimensionados pelas partes ao longo dos trabalhos;

1.1.18.1.1.19. Entrega formal da documentação resultante da implementação do projeto;

1.1.18.1.2. **IMPLANTAÇÃO**:

1.1.18.1.2.1. Os serviços deverão ser executados na sua totalidade pela CONTRATADA e deverão obrigatoriamente ter o acompanhamento da equipe técnica da CONTRATANTE;

1.1.18.1.2.2. O escopo de implementação, migração de serviços, configuração de políticas e funcionalidades para os produtos deste termo de referência, contempla configurações lógicas e testes na sede da CONTRATANTE;

1.1.18.1.2.3. A instalação deverá ser executada no local definido pelo CONTRATANTE, mediante prévio agendamento e em acordo com o cronograma;

1.1.18.1.2.4. Em até 30 (trinta) dias corridos da assinatura do Contrato, a CONTRATADA deverá submeter à verificação e aprovação pela área Técnica de TI da CONTRATANTE o plano completo, mencionado neste Termo.

1.1.18.1.3. **RECURSOS**:

1.1.18.1.3.1. Os recursos humanos a serem alocados pela CONTRATADA, suas qualificações mínimas e os seus respectivos papéis e responsabilidades no projeto:

1.1.18.1.3.2. Gerente de Projetos – Profissional com certificação PMP ativa e experiência comprovada no gerenciamento de projetos de implantação e migração de soluções de infraestrutura de TI. Caberá a ele a liderança da equipe de projeto e as atividades de gerenciamento e facilitação para o alcance dos objetivos do projeto segundo as melhores práticas de mercado.

1.1.18.1.3.3. Analista (s) Integrador (es) – conjunto com um ou mais profissionais que (individualmente ou conjuntamente):

1.1.18.1.3.3.1. Reúna as certificações:

1.1.18.1.3.4. Certificação oficial do fabricante em nível Profissional na solução de NAC/Autenticação do fabricante ofertado neste certame;

1.1.18.1.3.5. Caberá a este(s) profissional(ais) equipe o desenvolvimento do projeto de arquitetura futura, a execução e coordenação de atividades de migração, implantação, instalação, configuração e testes; e outras atividades técnicas conforme as prescrições deste edital.

1.1.18.1.4. A CONTRATADA deverá comprovar o vínculo societário ou empregatício e as qualificações do(s) técnico(s) que vier(em) prestar serviços nas dependências do CONTRATANTE;

1.1.18.1.5. A comprovação de que a empresa possui em seu quadro funcional os profissionais solicitados dar-se-á mediante cópias autenticadas das Carteiras de Trabalho ou fichas de Registro de Empregado, cópia do ato de investidura no cargo ou cópia do contrato social e suas alterações em se tratando de sócio, ou ainda através de contrato de prestação de serviços;

1.1.18.1.6. **REQUISITOS TÉCNICOS**

1.1.18.1.7. Solução de autenticação de usuários e dispositivos para controle de acesso a rede deverá ser disponibilizada em nuvem publica, fornecida pelo Contrato.

1.1.18.1.8. Cada item contratado da solução deverá permitir autenticação e controle de até 500 dispositivos e/ou usuários conectados à rede de formas simultânea.

1.1.18.1.9. As licenças que se aplicam aos dispositivos/usuários devem acompanhar período mínimo de 01 ano de subscrição, podendo ter sua prorrogação aplicada conforme as prorrogações contratuais previstas neste termo de referência.

1.1.18.1.10. Possuir plataforma unificada que combina acesso de convidado incorporando identidade, informações físicas de dispositivo e elementos condicionais em um conjunto de políticas.

1.1.18.1.11. Suporte a seguintes fontes para autenticação:

- **1.1.18.1.11.1.** Microsoft Active Directory
- **1.1.18.1.11.2.** LDAP-compliant directory
- **1.1.18.1.11.3.** Radius
- **1.1.18.1.11.4.** Microsoft Azure Active Directory
- **1.1.18.1.11.5.** Google G Suite
- **1.1.18.1.11.6.** HTTP
- **1.1.18.1.11.7.** Lista estática de endereços MAC

1.1.18.1.12. Deve suportar "Single Sign-on" (SSO) através de SAML v2.0 e/ou OpenID Connect e/ou OAuth 2.0

1.1.18.1.13. Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:

- **1.1.18.1.13.1.** Atributos do usuário autenticado,
- **1.1.18.1.13.2.** Hora do dia, dia da semana,
- **1.1.18.1.13.3.** Tipo de dispositivo utilizado,
- **1.1.18.1.13.4.** Localização do usuário;
- **1.1.18.1.13.5.** Tipo de autenticação utilizado

1.1.18.1.14. Permitir a visualização de todas informações relativas a cada transação/autenticação em uma única tela, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise

1.1.18.1.15. Deve possuir Dashboard customizável, onde deve permitir a visualização em forma de gráfico e/ou tabela de no mínimo as seguintes informações:

- **1.1.18.1.15.1.** Lista com os últimos Alertas do sistema;
- **1.1.18.1.15.2.** Requisições de autenticação dos últimos 7 dias, incluindo RADIUS e Web Authentication;
- **1.1.18.1.15.3.** Status das autenticações aceitas e rejeitadas nos últimos 7 dias;
- **1.1.18.1.15.4.** Últimas falhas de autenticação;
- **1.1.18.1.15.5.** Lista com as últimas autenticações;
- **1.1.18.1.15.6.** Lista com as últimas autenticações com sucesso;

1.1.18.1.15.7. Utilização de CPU do sistema;

1.1.18.1.16. Caso exista licenciamento distinto para usuários/dispositivos da rede sem fio (wireless) e usuários/dispositivos da rede cabeada (wired), deverão ser fornecidas as duas licenças para o número total de usuários solicitados;

1.1.18.1.17. Deve permitir que cada dispositivo receba uma chave pré-compartilhada exclusiva durante o registro do dispositivo.

1.1.18.1.18. Deve suportar, no mínimo, 5 dos seguintes métodos de autenticação:

1.1.18.1.18.1. EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)

1.1.18.1.18.2. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP- PWD)

1.1.18.1.18.3. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)

1.1.18.1.18.4. EAP-TLS

1.1.18.1.18.5. PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5

1.1.18.1.18.6. Windows Machine Authentication

1.1.18.1.18.7. SMB v2/v3

1.1.18.1.18.8. WPA3

1.1.18.1.18.9. MPSK e/ou DPSK

1.1.18.1.18.10. WEB Authentication

1.1.18.1.19. Deve suportar EDUROAM;

1.1.18.1.20. Suporte a integração com plataforma de terceiros usando HTTP/RESTful API.

1.1.18.1.21. Suporte aos seguintes recursos através de IPv6:

1.1.18.1.21.1. Administração via WEB e CLI

1.1.18.1.21.2. Servidores de autenticação e autorização com endereçamento IPv6;

1.1.18.1.21.3. Syslog, DNS, NTP;

1.1.18.1.21.4. Fontes de Syslog para processamento de eventos

1.1.18.1.22. A solução deve permitir a geração e o envio através de e-mail ou SMS de alertas relativos as seguintes atividades anormais detectadas na rede:

1.1.18.1.22.1. Autenticações

1.1.18.1.22.2. Acesso a dispositivos de rede

1.1.18.1.22.3. Atividades irregulares nos servidores da solução

1.1.18.1.23. A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML e PDF;

1.1.18.1.24. Deve possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilidade de usuários visitantes através de um portal web seguro;

1.1.18.1.25. Deve implementar a criação de grupos de autorizadores com privilégios distintos, por SSID, de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;

1.1.18.1.26. Deve realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;

1.1.18.1.27. Deve implementar as funcionalidades de geração aleatória de lotes de credenciais temporárias pré-autorizadas;

1.1.18.1.28. Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv;

1.1.18.1.29. Deve permitir a criação de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta;

1.1.18.1.30. Deve permitir que o visitante crie sua própria credencial temporária ("self-service") através do portal web, sem a necessidade de um autorizador;

1.1.18.1.31. Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo autorizador ou pelo visitante, em caso de auto-serviço, especificando quais informações cadastrais dos visitantes são obrigatórias ou opcionais;

1.1.18.1.32. Deve permitir a customização do nível de segurança da senha temporária que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de caracteres especiais e números para compor a senha;

1.1.18.1.33. Deve exigir que o usuário visitante aceite o "Termo de uso da rede" a cada login ou apenas no primeiro login;

1.1.18.1.34. Deve permitir o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), email e impressão local

1.1.18.1.35. Deve permitir que a customização da página de registro de visitantes para campos relacionados a confirmação de sponsorship;

1.1.18.1.36. Deve permitir o gerenciamento das credenciais de visitantes;

1.1.18.1.37. Deve permitir a configuração de contas de usuários visitantes com as seguintes características: Prazo de validade, largura de banda;

1.1.18.1.38. Deve permitir o login automático de usuários que realizem o auto-registro;

1.1.18.1.39. Deve permitir a autenticação de usuário anônimo sem necessidade de prover usuário e senha;

1.1.18.1.40. Deve permitir a criação de token de acesso;

1.1.18.1.41. Deve permitir a criação e gerenciamento de múltiplas contas de usuários visitantes;

1.1.18.1.42. Deve permitir a desconexão de múltiplas sessões ativas;

1.1.18.1.43. Deve permitir autenticação através de social login nativa na solução;

1.1.19. SOLUÇÃO DE POLÍTICA E AUTENTICAÇÃO DE USUÁRIOS DE REDE SEM FIO COM VERIFICAÇÃO DE POSTURA DE DISPOSITIVO

1.1.19.1. SERVIÇOS DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE AUTENTICAÇÃO, INSTALAÇÃO, CONFIGURAÇÃO E TESTES

1.1.19.1.1. PLANEJAMENTO:

1.1.19.1.1.1. Reunião de Kick-off – Deve ser realizada em duas etapas: a primeira com a equipe de implementação, abordando aspectos técnicos, integração, comunicação, e a segunda com o cliente tratando as formas de acompanhamento ao longo do projeto e prazo;

1.1.19.1.1.2. Visão geral do projeto, a fim de alinhar os objetivos e metas

técnicas;

1.1.19.1.1.3. Escopo do Projeto;

1.1.19.1.1.4. Principais Entregas;

1.1.19.1.1.5. Limites do Projeto;

1.1.19.1.1.6. Possíveis riscos que podem ocorrer, bem como um plano de prevenção e/ou recuperação;

1.1.19.1.1.7. Equipe de execução do Projeto;

1.1.19.1.1.8. Prioridade do Projeto;

1.1.19.1.1.9. Cronograma do Projeto;

1.1.19.1.1.10. Esclarecimento de dúvidas;

1.1.19.1.1.11. Reunião de Follow-up – Deve ser realizada pelo menos uma vez por semana durante o período de implementação do projeto. Poderá ser feita de forma remota;

1.1.19.1.1.12. Relato breve quantificando do status das principais atividades do projeto;

1.1.19.1.1.13. Apresentação de fatos e informações relevantes que permitam análise e acompanhamento do andamento do projeto;

1.1.19.1.1.14. Avaliação de possíveis sanções que poderão ser aplicadas caso ocorram atrasos ou imprevistos no projeto, especialmente as que envolvem qualidade do trabalho, cronograma e custos;

1.1.19.1.1.15. Reunião EndUp – Deve ser uma reunião formal a ser realizada ao término de todas as atividades do projeto, com a presença do cliente, gerente do projeto e equipe do projeto;

1.1.19.1.1.16. Descrição resumida do projeto, desde seu início até sua finalização;

1.1.19.1.1.17. Síntese das fases e marcos principais e caracterização do cumprimento de tudo que ficou acertado e aceito pelo cliente em cada fase;

1.1.19.1.1.18. Certificação de que o projeto que está sendo entregue neste momento cumpre todos os requisitos acordados no início, e/ou modificados e redimensionados pelas partes ao longo dos trabalhos;

1.1.19.1.1.19. Entrega formal da documentação resultante da implementação do projeto;

1.1.19.1.2. **IMPLANTAÇÃO**:

1.1.19.1.2.1. Os serviços deverão ser executados na sua totalidade pela CONTRATADA e deverão obrigatoriamente ter o acompanhamento da equipe técnica da CONTRATANTE;

1.1.19.1.2.2. O escopo de implementação, migração de serviços, configuração de políticas e funcionalidades para os produtos deste termo de referência, contempla configurações lógicas e testes na sede da CONTRATANTE;

1.1.19.1.2.3. A instalação deverá ser executada no local definido pelo CONTRATANTE, mediante prévio agendamento e em acordo com o cronograma;

1.1.19.1.2.4. Em até 30 (trinta) dias corridos da assinatura do Contrato, a CONTRATADA deverá submeter à verificação e aprovação pela área Técnica de TI da CONTRATANTE o plano completo, mencionado neste

Termo.

1.1.19.1.3. RECURSOS:

1.1.19.1.3.1. Os recursos humanos a serem alocados pela CONTRATADA, suas qualificações mínimas e os seus respectivos papéis e responsabilidades no projeto:

1.1.19.1.3.2. Gerente de Projetos – Profissional com certificação PMP ativa e experiência comprovada no gerenciamento de projetos de implantação e migração de soluções de infraestrutura de TI. Caberá a ele a liderança da equipe de projeto e as atividades de gerenciamento e facilitação para o alcance dos objetivos do projeto segundo as melhores práticas de mercado.

1.1.19.1.3.3. Analista (s) Integrador (es) – conjunto com um ou mais profissionais que (individualmente ou conjuntamente):

1.1.19.1.3.3.1. Reúna as certificações:

1.1.19.1.3.4. Certificação oficial do fabricante em nível Profissional na solução de NAC/Autenticação do fabricante ofertado neste certame;

1.1.19.1.3.5. Caberá a este(s) profissional(ais) equipe o desenvolvimento do projeto de arquitetura futura, a execução e coordenação de atividades de migração, implantação, instalação, configuração e testes; e outras atividades técnicas conforme as prescrições deste edital.

1.1.19.1.4. A CONTRATADA deverá comprovar o vínculo societário ou empregatício e as qualificações do(s) técnico(s) que vier(em) prestar serviços nas dependências do CONTRATANTE;

1.1.19.1.5. A comprovação de que a empresa possui em seu quadro funcional os profissionais solicitados dar-se-á mediante cópias autenticadas das Carteiras de Trabalho ou fichas de Registro de Empregado, cópia do ato de investidura no cargo ou cópia do contrato social e suas alterações em se tratando de sócio, ou ainda através de contrato de prestação de serviços;

1.1.19.1.6. REQUISITOS TÉCNICOS

1.1.19.1.7. Solução de autenticação de usuários e dispositivos para controle de acesso a rede deverá ser disponibilizada em nuvem publica, fornecida pelo Contrato.

1.1.19.1.8. Cada item contratado da solução deverá permitir autenticação de até 500 dispositivos e/ou usuários conectados à rede de formas simultânea.

1.1.19.1.9. As licenças que se aplicam aos dispositivos/usuários devem acompanhar período mínimo de 01 ano de subscrição, podendo ter sua prorrogação aplicada conforme as prorrogações contratuais previstas neste termo de referência.

1.1.19.1.10. Possuir plataforma unificada que combina acesso de convidado incorporando identidade, informações físicas de dispositivo e elementos condicionais em um conjunto de políticas.

1.1.19.1.11. Suporte a seguintes fontes para autenticação:

1.1.19.1.11.1. Microsoft Active Directory

1.1.19.1.11.2. Kerberos

1.1.19.1.11.3. Base SQL interna

1.1.19.1.11.4. LDAP-compliant directory
1.1.19.1.11.5. Radius
1.1.19.1.11.6. Microsoft Azure Active Directory
1.1.19.1.11.7. Google G Suite
1.1.19.1.11.8. HTTP
1.1.19.1.11.9. Lista estática de endereços MAC

1.1.19.1.12. Deve suportar "Single Sign-on" (SSO) através de SAML v2.0 e/ou OpenID Connect e/ou OAuth 2.0

1.1.19.1.13. Deve implementar gerenciamento e aplicação de políticas de autorização de acesso de usuários com base em:

1.1.19.1.13.1. Atributos do usuário autenticado,
1.1.19.1.13.2. Hora do dia, dia da semana,
1.1.19.1.13.3. Tipo de dispositivo utilizado,
1.1.19.1.13.4. Localização do usuário;
1.1.19.1.13.5. Tipo de autenticação utilizado

1.1.19.1.14. Permitir a visualização de todas informações relativas a cada transação/autenticação em uma única tela, como Data e Hora, Mac Address do dispositivo, classificação do dispositivo, Usuário, equipamento que requisitou a autenticação (origem), Método de autenticação utilizado, fonte de autenticação utilizada para validação, perfil de acesso aplicado, todos atributos de entrada do protocolo utilizados na requisição (ex. RADIUS), informações de resposta da solução para o elemento de rede, alertas em caso de falha, e exibição dos Log já filtrados para a requisição em análise

1.1.19.1.15. Deve possuir Dashboard customizável, onde deve permitir a visualização em forma de gráfico e/ou tabela de no mínimo as seguintes informações:

1.1.19.1.15.1. Lista com os últimos Alertas do sistema;
1.1.19.1.15.2. Requisições de autenticação dos últimos 7 dias, incluindo RADIUS, TACACS+ e Web Authentication;
1.1.19.1.15.3. Status das autenticações aceitas e rejeitadas nos últimos 7 dias;
1.1.19.1.15.4. Últimas falhas de autenticação;
1.1.19.1.15.5. Lista com as últimas autenticações;
1.1.19.1.15.6. Lista com as últimas autenticações com sucesso;
1.1.19.1.15.7. Utilização de CPU do sistema;

1.1.19.1.16. Caso exista licenciamento distinto para usuários/dispositivos da rede sem fio (wireless) e usuários/dispositivos da rede cabeada (wired), deverão ser fornecidas as duas licenças para o número total de usuários solicitados;

1.1.19.1.17. Deve permitir que cada dispositivo receba uma chave pré-compartilhada exclusiva durante o registro do dispositivo.

1.1.19.1.18. Deve suportar, no mínimo, 5 dos seguintes métodos de autenticação:

1.1.19.1.18.1. EAP-FAST (EAP-MSCHAPv2, EAP-GTC, EAP-TLS)
1.1.19.1.18.2. PEAP (EAP-MSCHAPv2, EAP-GTC, EAP-TLS, EAP-PEAP-Public, EAP- PWD)
1.1.19.1.18.3. TTLS (EAP-MSCHAPv2, EAP-GTC, EAP- TLS, EAP-MD5, PAP, CHAP)
1.1.19.1.18.4. EAP-TLS

1.1.19.1.18.5. PAP, CHAP, MSCHAPv1, MSCHAPv2, and EAP-MD5
1.1.19.1.18.6. Windows Machine Authentication
1.1.19.1.18.7. SMB v2/v3
1.1.19.1.18.8. WPA3
1.1.19.1.18.9. MPSK e/ou DPSK
1.1.19.1.18.10. WEB Authentication

1.1.19.1.19. Deve suportar EDUROAM;

1.1.19.1.20. Suporte a integração com plataforma de terceiros usando HTTP/RESTful API.

1.1.19.1.21. Suporte aos seguintes recursos através de IPv6:
1.1.19.1.21.1. Administração via WEB e CLI
1.1.19.1.21.2. Servidores de autenticação e autorização com endereçamento IPv6;
1.1.19.1.21.3. Syslog, DNS, NTP;
1.1.19.1.21.4. Fontes de Syslog para processamento de eventos

1.1.19.1.22. A solução deve permitir a geração e o envio através de e-mail ou SMS de alertas relativos as seguintes atividades anormais detectadas na rede:
1.1.19.1.22.1. Autenticações
1.1.19.1.22.2. Acesso a dispositivos de rede
1.1.19.1.22.3. Atividades irregulares nos servidores da solução

1.1.19.1.23. A solução deve possuir ferramenta para geração de relatórios de maneira centralizada, permitindo o agendamento e envio por e-mail em formato HTML e PDF;

1.1.19.1.24. Deve possuir ferramenta para gerenciar os processos de credenciamento, autenticação, autorização e contabilidade de usuários visitantes através de um portal web seguro;

1.1.19.1.25. Deve implementar a criação de grupos de autorizadores com privilégios distintos, por SSID, de criação de credenciais temporárias e atribuição de permissões de acesso aos clientes;

1.1.19.1.26. Deve realizar a autenticação dos autorizadores em base externa do tipo Microsoft Active Directory ou LDAP e atribuir o privilégio ao autorizador de acordo com o seu perfil;

1.1.19.1.27. Deve implementar as funcionalidades de geração aleatória de lotes de credenciais temporárias pré-autorizadas;

1.1.19.1.28. Deve implementar a importação e exportação da relação de credenciais temporárias através de arquivos txt ou csv;

1.1.19.1.29. Deve permitir a criação de validade das credenciais, baseando o início da validade na criação da conta ou no primeiro login da conta;

1.1.19.1.30. Deve permitir que o visitante crie sua própria credencial temporária (“self-service”) através do portal web, sem a necessidade de um autorizador;

1.1.19.1.31. Deve permitir a customização do formulário de criação de credenciais, a ser preenchido pelo autorizador ou pelo visitante, em caso de auto-serviço, especificando quais informações cadastrais dos visitantes são obrigatórias ou opcionais;

1.1.19.1.32. Deve permitir a customização do nível de segurança da senha temporária

que será gerada ao visitante, especificando a quantidade mínima de caracteres e o uso de caracteres especiais e números para compor a senha;

1.1.19.1.33. Deve exigir que o usuário visitante aceite o "Termo de uso da rede" a cada login ou apenas no primeiro login;

1.1.19.1.34. Deve permitir o envio das credenciais aos usuários registrados através de mensagens SMS (Short Message Service), email e impressão local

1.1.19.1.35. Deve permitir que a customização da página de registro de visitantes para campos relacionados a confirmação de sponsorship;

1.1.19.1.36. Deve permitir o gerenciamento das credenciais de visitantes;

1.1.19.1.37. Deve permitir a configuração de contas de usuários visitantes com as seguintes características: Prazo de validade, largura de banda;

1.1.19.1.38. Deve permitir o login automático de usuários que realizem o auto-registro;

1.1.19.1.39. Deve permitir a autenticação de usuário anônimo sem necessidade de prover usuário e senha;

1.1.19.1.40. Deve permitir a criação de token de acesso;

1.1.19.1.41. Deve permitir a criação e gerenciamento de múltiplas contas de usuários visitantes;

1.1.19.1.42. Deve permitir a desconexão de múltiplas sessões ativas;

1.1.19.1.43. Deve permitir autenticação através de social login nativa na solução;

1.1.19.1.44. Deve possuir funcionalidade para verificação das políticas de segurança implementadas nos dispositivos conectados a rede, através de agentes instalados ou temporários.

1.1.19.1.45. Para a verificação de postura, deve ter a capacidade de analisar até 100 dispositivos simultaneamente;

1.1.19.1.46. Deve suportar a verificação, no mínimo, nos sistemas operacionais:

1.1.19.1.46.1. Windows 7, Windows 8, Windows 10 e Windows 11;

1.1.19.1.46.2. Mac OSX 10.10 e superior

1.1.19.1.46.3. Linux

1.1.19.1.46.3.1. Red Hat

1.1.19.1.46.3.2. Ubuntu

1.1.19.1.46.3.3. Fedora

1.1.19.1.46.3.4. SUSE

1.1.19.1.46.3.5. CentOS

1.1.19.1.47. Permitir a execução do agente como serviço quando instalado em sistemas Windows;

1.1.19.1.48. Permitir o uso de agentes instalados nos dispositivos, ou agente temporários para o uso em dispositivos de terceiros que necessitem acesso a rede.

1.1.19.1.49. Permitir o gerenciamento centralizado das políticas, e permitir que os usuário/dispositivos que estiverem fora das políticas de seguranças, sejam direcionados para um segmento de rede específico ou determinação de uma política de acesso restritiva, permitindo ainda que estes consigam se adequar a respectiva política através da remediação dos problemas;

1.1.19.1.50. Permitir que a solução realize a adequação da política (remediação) de forma automática, sem necessidade de intervenção do usuário.

1.1.19.1.51. Deve suportar a verificação de pelos menos os seguintes serviços:

1.1.19.1.51.1. Firewall
1.1.19.1.51.2. Conexões de rede
1.1.19.1.51.3. Windows Hotfixes
1.1.19.1.51.4. Aplicações instaladas
1.1.19.1.51.5. Serviços
1.1.19.1.51.6. Dispositivos USB
1.1.19.1.51.7. Processos
1.1.19.1.51.8. Checagem de arquivos

1.1.19.1.52. Deve suportar a verificação de anti-vírus com pelos menos os seguintes parâmetros:

1.1.19.1.52.1. Produto instalado
1.1.19.1.52.2. Versão instalada
1.1.19.1.52.3. Data da ultima atualização
1.1.19.1.52.4. Data da ultima verificação

1.1.19.1.53. A plataforma deve suportar a integração com SCCM ou WSUS.

1.1.19.1.54. Deve permitir a verificação de postura de dispositivos Windows 10 sem a necessidade de instalação prévia de agentes, executando todas as operações de verificação em "background", ou seja, transparente ao usuário final;

1.1.20. SERVIÇO DE INSTALAÇÃO FÍSICA DE ACCESS POINT – ATÉ 50 METROS

1.1.20.1. Os serviços deverão ser executados na sua totalidade pela CONTRATADA e deverão obrigatoriamente ter o acompanhamento da equipe técnica da CONTRATANTE;

1.1.20.2. Todo o material e mão de obra necessários à instalação deverão ser fornecidos pela CONTRATADA, sem ônus adicional a CONTRATANTE, tais como: acessórios de fixação, canaletas e cabeamento metálico compatível com os equipamentos até o ponto de rede da CONTRATANTE mais próximo;

1.1.20.3. No caso dos pontos de acesso, todos, sem exceção, estarão em “alcance de cabeamento” não superior a 50 (cinquenta) metros até o switch da CONTRATANTE mais próximo;

1.1.20.4. Considerar o alcance de cabeamento como a distância interna, considerando dutos e passagens no forro, paredes e pisos, entre o AP e o switch da CONTRATANTE;

1.1.20.5. Caso necessário, o fornecimento de patch panels será de responsabilidade da CONTRATANTE;

1.1.20.6. Após a instalação inicial, oficializada com a emissão do Termo de Aceitação Definitiva (TAD), a CONTRATANTE se responsabilizará por quaisquer novas instalações e cabeamentos.

1.1.21. SERVIÇO DE INSTALAÇÃO FÍSICA DE ACCESS POINT – ATÉ 100 METROS

1.1.21.1. Os serviços deverão ser executados na sua totalidade pela CONTRATADA e deverão obrigatoriamente ter o acompanhamento da equipe técnica da

CONTRATANTE;

1.1.21.2. Todo o material e mão de obra necessários à instalação deverão ser fornecidos pela CONTRATADA, sem ônus adicional a CONTRATANTE, tais como: acessórios de fixação, canaletas e cabeamento metálico compatível com os equipamentos até o ponto de rede da CONTRATANTE mais próximo;

1.1.21.3. No caso dos pontos de acesso, todos, sem exceção, estarão em "alcance de cabeamento" não superior a 100 (cem) metros até o switch da CONTRATANTE mais próximo;

1.1.21.4. Considerar o alcance de cabeamento como a distância interna, considerando dutos e passagens no forro, paredes e pisos, entre o AP e o switch da CONTRATANTE;

1.1.21.5. Caso necessário, o fornecimento de patch panels será de responsabilidade da CONTRATANTE;

1.1.21.6. Após a instalação inicial, oficializada com a emissão do Termo de Aceitação Definitiva (TAD), a CONTRATANTE se responsabilizará por quaisquer novas instalações e cabeamentos.

1.1.22. DESCRIÇÃO TÉCNICA DETALHADA APLICADAS AO ITEM 17 E ITEM 18

1.1.22.1. O sistema de cabeamento estruturado a ser fornecido deve atender aos padrões e especificações rigorosas necessárias para garantir a transmissão confiável e de alta velocidade de dados em uma infraestrutura de rede. A seguir, estão as especificações técnicas para os componentes essenciais do sistema:

1.1.22.2. CABO DE REDE UTP CAT6A:

6.1.19.2.1 Categoria: Cat6A (Categoria 6A).

6.1.19.2.2 Fio sólido de cobre eletrolítico nu, recozido, com diâmetro nominal de 23AWG;

6.1.19.2.3 Para distribuição horizontal da rede, cobre recozido rígido isolado em polietileno de alta densidade, com um elemento central em material termoplástico para separação dos 04 pares entre si, características elétricas e mecânicas compatíveis com os padrões da categoria 6A.

6.1.19.2.4 Deve suportar SERVIÇOSs de transmissão de até 10 Gb (Multi Gigabit Ethernet);

6.1.19.2.5 Capa em PVC, anti-chama, com marcação de comprimento em espaços inferiores a 1 metro.

6.1.19.2.6 Tensão de ruptura mínima de 400N e tensão de puxamento máxima de 110N;

6.1.19.2.7 Condutor de cobre nu, coberto por polietileno termoplástico adequado. Os condutores são trançados em pares. Capa externa em material não propagante a chama em cumprimento com as diretivas européias RoHS (Restriction of Hazardous Substances);

6.1.19.2.8 Deve atender as normas ANSI/TIA-568.2-D, ISO/IEC 11801, UL 444, ABNT NBR 14703 e ABNT NBR 14705.

6.1.19.2.9 Polietileno de alta densidade com diâmetro nominal 1.0mm;

6.1.19.2.10 Os condutores isolados são reunidos dois a dois, formando o par. Os passos de torcimento devem ser adequados, de modo a atender os níveis de diafonia previstos e minimizar o deslocamento relativo entre si;

6.1.19.2.11 Devem ser fornecidos na cor Azul, Cinza ou Vermelho;

6.1.19.2.12 Deve atender a flamabilidade mínima de CM: norma UL 1581-Vertical tray Section 1160 (UL1685) CMR: norma UL 1666 (Riser);

6.1.19.2.13 Deve ter gravação com Marcação Sequencial Métrica decrescente (305-001 m), Rastreabilidade com identificação do Processo de fabricação (Y) e data detalhada AAMMDDHHmm (AA – Ano, MM – Mês, DD – dia, HH – Hora, mm – Minuto);

6.1.19.2.14 Material deve ser homologado e/ou certificado pela Anatel;

1.1.22.3. PATCH PANEL 24 PORTAS CAT6A:

6.1.19.3.1 Categoria: Cat6A (Categoria 6A).

6.1.19.3.2 Portas: O patch panel deve ter 24 portas fêmeas RJ45.

6.1.19.3.3 Conexões: Cada porta deve possuir uma conexão Keystone RJ45 Cat6A.

6.1.19.3.4 Montagem: O patch panel deve ser projetado para montagem em rack padrão de 19 polegadas.

6.1.19.3.5 Material: Deve ser construído com material resistente e durável.

6.1.19.3.6 Identificação: Cada porta deve ser identificada numericamente e/ou por cores para facilitar a identificação e manutenção.

6.1.19.3.7 Será aceito patch panel do tipo descarregado, deverá ser fornecido a quantidade de tomadas/conectores RJ45 CAT6 conforme quantidade de tomadas demandadas para a conexão dos pontos de acesso.

1.1.22.4. TOMADAS RJ45 FÊMEA CAT6A:

6.1.19.4.1 Categoria: Cat6A (Categoria 6A).

6.1.19.4.2 Suporte a IEEE 802.3, 10G BASE-T, 1000 BASE T, 1000 BASE TX, EIA/TIA-854, ANSI-

6.1.19.4.3 EIA/TIA862, ATM, Vídeo, Sistemas de Automação Predial e todos os protocolos LAN anteriores.

6.1.19.4.4 Compatível com Patch Panel descarregado, caixas e espelhos;

6.1.19.4.5 Deve exceder os limites estabelecidos na norma para CAT.6A

6.1.19.4.6 Até 500MHz, conforme a ANSI/TIA 568 C.2 e ISO 11801 classe EA

6.1.19.4.7 Inserção do cabo em ângulo de 90° ou 180°

6.1.19.4.8 Acessório para proteção do contato IDC e manutenção do cabo crimpado;

6.1.19.4.9 Fornecido com tampa de proteção frontal (dust cover) removível e articulada com local para inserção, (na própria tampa), do ícone de identificação.

6.1.19.4.10 Suporte ao PoE 802.3af e 802.3at

6.1.19.4.11 Padrão de montagem T568A e T568B;

6.1.19.4.12 Quantidade de ciclos de inserção mínimo 750 RJ45

6.1.19.4.13 Deve atender as normas ANSI/TIA-568-C.2 ISO/IEC 11801 NBR 14565 FCC parte 68.

6.1.19.4.14 A crimpagem deve atender o as especificações estabelecidas pelas normas vigentes;

6.1.19.4.15 Material do corpo do produto deve ser termoplástico de alto impacto não propagante à chama UL 94V-0.

6.1.19.4.16 Diâmetro do condutor 26 a 22 AWG.

6.1.19.4.17 Identificação das tomadas deve atender às exigências do NTI, segundo como padrão RxPPxPTxxx, sendo: (R – Rack, PP – Patch Panel, PT – numeração do

ponto de telecomunicação, X – sendo a numeração sequencial).

6.1.19.4.18 Material deve ser homologado e/ou certificado pela Anatel;.

6.1.19.4.19 Deverá ser fornecido as caixas sobrepor para instalação das tomadas fêmeas RJ45, conforme a estrutura utilizada (tubo condulete ou canaletas) dos pontos de redes no local e posição indicado pela contratante.

6.1.19.4.20 Deve ser considerado para a passagem do cabeamento tubo condulete ou canaletas em PVC, assim como todos os acessórios necessários para sua fixação;

1.1.22.5. PATCH CORD CAT6A

6.1.19.5.1 PatchCord CAT6A para tráfego de voz, dados e imagem com o tamanho de 150 cm de comprimento e será utilizado para manobra dentro do rack e/ou conexão do ponto de acesso ao ponto de rede;

6.1.19.5.2 Tipo de conector: rj-45; Tipo de cabo: u/utp cat.6; Cor: Azul ou Vermelho;

6.1.19.5.3 Quantidade de pares: 04 pares, 24 awg;

6.1.19.5.4 Padrão de montagem: T568a;

6.1.19.5.5 Temperatura de operação: - 10º c a + 60º c;

6.1.19.5.6 Capacitância mutua 1 khz: 56 pf/m (máximo);

6.1.19.5.7 Prova de tensão elétrica entre condutores: 1500 vdc/3s;

6.1.19.5.8 Velocidade de propagação nominal: 66%.

6.1.19.5.9 Atende as normas TIA/EIA 568 C.2, ANSI/TIA/EIA-569, ANSI/TIA/EIA 606B, FCC PART 68 E ISO/IEC 11.801;

6.1.19.5.10 Material de contato elétrico produzido em 8 vias de bronze fosforoso com 50 µin (1,27µm) de ouro e 100µin (2,54µm) de níquel; material do corpo do conector feito em termoplástico transparente não propagante à chama (ul 94v-0), com resistência máxima do condutor de 93,8 ω/km;

6.1.19.5.11 Armazenado em embalagem individual, para preservar todas as propriedades do material até seu uso efetivo;

6.1.19.5.12 Material deve ser homologado e/ou certificado pela Anatel;

1.1.22.6. OBSERVAÇÕES GERAIS:

1.1.22.6.1. Todos os componentes do sistema devem cumprir os padrões e regulamentações nacionais e internacionais aplicáveis.

1.1.22.6.2. Deve ser considerado todos os acessórios necessário para fixação da intraestrutura do cabeamento, tais como: cx sobrepor, tubulações, canaletas.

1.1.22.6.3. Deve ser fornecida uma documentação técnica detalhada, incluindo diagramas de instalação e certificações de conformidade dos produtos.

1.1.22.6.4. A instalação e configuração dos componentes devem ser realizadas por técnicos qualificados e certificados em cabeamento estruturado.

1.1.22.6.5. Garantia: O fornecedor deve oferecer garantia dos produtos e serviços, com um período mínimo de garantia de 36 meses a partir da data de instalação.

1.1.22.6.6. Para os serviços de instalação e remanejamento de infraestrutura de cabeamento lógico estruturado deverão ser efetuados todos os testes necessários para comprovar que as instalações estão em condição de funcionar corretamente e de acordo com as especificações e normas estabelecidas.

1.1.22.6.7. Desta forma a contratada deverá executar certificação e identificação dos pontos

de redes instalados, utilizando equipamentos específicos para esta finalidade;

1.1.22.6.8. Não será aceito teste feito apenas por testador convencional de rede;

1.1.22.6.9. A contratada deverá utilizar certificadores de rede como equipamentos da fluke networks ou similar;

1.1.22.6.10. Os certificados de garantia deverão ser para instalação lógica, devendo ser efetuados os seguintes testes:

1.1.22.6.11. Testes para cabeamento lógico estruturado:

1.1.22.6.12. Near End Crosstalk (NEXT),

1.1.22.6.13. Far End Crosstalk (FEXT),

1.1.22.6.14. Attenuation, Delay skew,

1.1.22.6.15. Structural Return Loss (SRL).

1.1.23. SERVIÇO DE SITE SURVEY

1.1.23.1. O serviço de Site Survey previsto para a Solução de Rede Sem Fios deverá ser realizado pela CONTRATADA após a CONTRATANTE definir o local para a instalação dos equipamentos de Ponto de Acesso sem Fio.

1.1.23.2. Para tanto, a CONTRATANTE determinará os pontos exatos para instalação dos pontos de acesso, conforme indicativo do Site Survey realizado previamente. Essas instalações serão solicitadas sob demanda e conforme conveniência.

1.1.23.3. O projeto de redes sem fio para os padrões 802.11a, 802.11b e 802.11g, 802.11n, 802.11ac e 802.11ax deve seguir a geografia do prédio em planta baixa fornecida pela CONTRATANTE, contemplando o nível mínimo de -67 dBm em todos os locais conforme critério da CONTRATANTE.

1.1.23.3.1. Caso a CONTRATANTE não possua as plantas baixas relativas aos locais de instalação, o posicionamento deverá ser definido no momento da implantação, conforme disponibilidade no local;

1.1.23.4. O serviço de Site Survey deve ser realizado mediante o uso de equipamentos e softwares para análise, relatórios e troubleshooting de redes wireless, com as características listadas abaixo:

1.1.23.4.1. Planejamento e otimização de redes Wi-Fi com mapa de calor de sinal;

1.1.23.4.2. Gráficos de cobertura, alcance de sinal e ruído;

1.1.23.4.3. Simulação de cobertura, sinal e desempenho;

1.1.23.5. Com os resultados obtidos no relatório, a CONTRATADA deverá demarcar os locais onde deverão ser instalados os pontos de acesso, de forma a maximizar a cobertura do sinal da rede sem fio, minimizando possíveis interferências externas que foram detectadas.

1.1.23.6. A demarcação dos pontos para instalação dos pontos de acesso deverá ser na forma de adesivos possuindo a identificação dos pontos de acessos que serão instalados em cada local.

1.1.23.7. Após a execução do serviço a CONTRATADA deverá produzir um relatório com os resultados obtidos e entregá-lo a CONTRATANTE.

1.1.23.8. A CONTRATANTE exigirá o prazo de 5 (cinco) dias úteis para a análise dos documentos e caso seja necessária alguma readequação a CONTRATADA deverá executá-la em no máximo 3 (três) dias úteis.

1.1.23.9. Após a entrega do Relatório Final a CONTRATANTE solicitará um novo prazo, que poderá ser de até 90 (noventa) dias, para adequar a infraestrutura conforme especificado no relatório final.

1. DA COMPLEXIDADE DO SERVIÇO

1.1. A adoção do valor de referência único facilita à contabilização dos serviços, todavia, demanda a definição dos parâmetros relativos a ponderação aplicável ao dimensionamento do serviço; nesse sentido, para efeito de cada projeto a ser contratado, serão adotados os seguintes pesos de complexidade:

Complexidade	Serviços	Peso Complexidade
Baixa	Monitoramento de chamados de terceiros. Atendimento aos usuários na modalidade emergencial. Assistência técnica remota (plantão). Atividades de apoio à: monitoramento de ações, acompanhamento de atividades, registros em sistemas básicos, formatação de artefatos básicos de projetos de sistemas, prototipação e atividades similares.	1,00
Intermediária	Assistência Técnica Presencial. Análise e levantamento de processos. Criação e implantação da base de conhecimento na solução de gerenciamento de serviços e atualização dos scripts de atendimento. Operação de sistemas complexos, apoiar na criação de artefatos de projetos, especificação casos de uso, regras de negócio, elaboração de diagramas de processos e estratégia, atendimento a demanda de média complexidade de clientes internos, mapeamento de processos e atividades similares.	1,05
Alta	Automação de processos na solução de gerenciamento de serviços. Desenvolvimento de painel de controle (*dashboards*), portfólio e catálogo de serviços. Desenvolvimento de novos relatórios. Implantação de novos processos, apoio na criação e desenvolvimento de projetos, estudos de viabilidade de projetos, criação de novos processos, desenvolvimento de novos sistemas, aperfeiçoamento de processos de gestão do cliente final ou ETICE, apoio na implantação de novos sistemas no cliente final ou ETICE, e atividades similares.	1,10

Especialista	Customização na solução de gerenciamento de serviços. Execução de demanda eventual ou projeto não contemplado dos demais itens em razão de sua necessidade pontual de execução que requeiram conhecimento técnico em áreas correlatas sejam infraestrutura, sistemas, segurança da informação ou atividades similares.	1,15

Tabela - Definições de complexidade do serviço

2. DO CATÁLOGO DE SERVIÇOS

2.1. Conforme o ITIL, o Catálogo de serviço é um conjunto de informações sobre os serviços de TIC disponíveis para uso, trata-se de um conteúdo dinâmico, que requer revisão e alterações periódicas para que esteja adequado a realidade da TI, demandando assim um processo específico de gerenciamento, para que possa ser atual e aderente.

2.2. No contexto da presente especificação técnica, **buscou-se a elaboração de um catálogo que permitisse atender uma vasta gama de necessidades relativas a serviços em nuvem**, todavia, conforme as melhores práticas de gerenciamento de serviços e frameworks de mercado a exemplo do ITIL e COBIT o catálogo de serviços por tratar-se de um conteúdo dinâmico, necessita de revisões e adequações que venham a ser necessárias com vistas a assegurar sua aderência ao negócio. Assim com vistas a assegurar a aplicação das boas práticas de forma a suportar adequadamente as necessidades de negócio o catálogo de serviços que integra o presente instrumento estará sujeito a melhorias para a realização do objeto ajustado a realidade da ETICE e dos seus clientes finais.

2.3. Em função da evolução da maturidade da ETICE e em função da dinâmica dos processos, a versão inicial do catálogo de **serviços poderá sofrer revisões** com vistas a se adequar a realidade da ETICE e de seus clientes finais na ocasião, através de projetos específicos para revisão do catálogo de serviços.

2.4. A versão inicial do Catálogo de Serviços - (ANEXO G) elenca os tipos de solicitações contempladas pelo objeto do serviço, fornecendo referência a parâmetros que definem a ponderação do serviço.

3. DAS CONDIÇÕES DE EXECUÇÃO

3.1. O objeto desta especificação técnica tem por escopo **serviços de natureza contínua, prestados sob demanda**, para operacionalização de processos descritos no catálogo de serviços, assim como serviços pontuais, prestados sob demanda para a execução de projetos, que venham a ser necessários a efetivação dos objetivos estratégicos da ETICE e seus cliente finais no que dependam da tecnologia da informação e comunicação usando ambiente de nuvens.

3.2. A ETICE poderá a seu critério utilizar as USTs contratadas para a execução de serviços continuados (processos) ou pontuais (projetos) sem ônus ao objeto contratual, considerando especificações do catálogo de serviços.

4. DA SOLICITAÇÃO DE SERVIÇOS

4.1. Mensalmente ou em caso de necessidade serão abertas ordens de serviço, com os Serviços Técnicos devidamente identificados e associados a uma estimativa (UST) relacionadas aos

serviços a serem executados.

4.2. A partir da abertura da OS, todas as atividades necessárias para a execução dos serviços deverão estar relacionadas às demandas devidamente registradas em ferramenta de Gestão de Demandas. Quando não houver disponibilidade desta ferramenta, poderá ser realizada por qualquer outra compatível.

4.3. Para o encerramento de uma demanda é necessário o registro das atividades que evidenciam o seu atendimento.

4.4. O cálculo do número de USTs relativas aos serviços solicitados, será realizado por ocasião da emissão da ordem de serviços (OS) que poderá contemplar a execução de um ou mais serviço. Esse agrupamento só deverá ser aplicado para serviços com durações semelhantes, para não ocasionar retardo no encerramento da OS. O referido cálculo deverá ser feito para cada serviço solicitado na OS conforme a seguinte fórmula:

UST= (Esforço x complexidade)
onde:
UST: corresponde ao quantitativo de unidades de serviços técnicos estimados para a realização do serviço.
Esforço: Somatório da estimativa de todos os esforços decorrentes da alocação temporal de um ou mais recursos necessários ao serviço, considerados os pesos aplicados a cada recurso. Ou seja, **Esforço = Fator * Número de horas alocadas.**
Complexidade: peso quanto ao tipo predominante de atividades inerentes a sua realização do serviço.

4.5. Para aplicação da fórmula da UST ajustada por serviço, deve-se considerar que:

4.6. O dimensionamento do esforço para o serviço demandará estudo para definição de estimativas da alocação recursos necessários ao serviço, considerando quantitativos e a alocação temporal dos recursos para atendimento demanda.

4.7. A CONTRATADA poderá adotar o fator médio de 1,368 do ANEXO H para dimensionar o esforço;

4.8. Caso opte por não usar o fator médio a CONTRATADA deverá dimensionar o esforço adotando os pesos definidos no ANEXO H – LISTA DE PERFIS TÉCNICOS dos recursos;

5. DO CANCELAMENTO DOS SERVIÇOS

5.1. Nos casos em que a demanda for cancelada por solicitação do cliente final ou da ETICE, o trabalho já executado deverá ser medido, avaliado e pago.

5.2. Quando do cancelamento do serviço, a CONTRATADA deverá entregar os produtos do serviço executado, imediatamente, mesmo que inacabados.

5.3. O pagamento dos serviços cancelados está vinculado à entrega dos produtos parciais elaborados pela CONTRATADA até o momento do cancelamento.

Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP:60.130-240 - Fortaleza/CE
Fone: (85) 3108-0000
www.etice.ce.gov.br

ANEXO C - CARACTERÍSTICAS E ESPECIFICAÇÕES DA SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DOS ITENS 1 A 6

1. Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede do mesmo fabricante desde que não sejam software livre;
2. O módulo de gerência deve ser capaz de gerenciar e administrar as soluções descritas nos itens 1 a 6;
3. O gerenciamento centralizado poderá ser entregue como appliance virtual compatível/homologado com/para VMWare ESX (vSphere 5.1, 5.5 ou 6) ou em nuvem do fabricante;
   - 3.1. Caso a solução de gerenciamento centralizado seja entregue como appliance virtual em ambiente de virtualização da CONTRATANTE, a mesma deverá:
     - 3.1.1. Caso a solução possua licenças relacionadas a capacidade de logs indexados e armazenamento, deverá ser ofertada a de maior capacidade suportada ou ilimitada;
     - 3.1.2. Caso haja licenciamento pelo número de gateways gerenciados, deve estar licenciada para gerenciar o quantitativo total de equipamentos contratados;
     - 3.1.3. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;
     - 3.1.4. Todos os logs da solução devem ser indexados e seu licenciamento deve ser o de maior capacidade;
   - 3.2. Caso a solução de gerenciamento seja entregue em nuvem do fabricante, deverá fornecer o mínimo de retenção de 3 meses de logs;
     - 3.2.1. Caso haja licenciamento pelo número de gateways gerenciados, deve estar licenciada para gerenciar o quantitativo total de equipamentos contratados;
4. A solução de gerência deverá ser separada dos gateways de segurança, que irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste documento;
5. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;
6. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;
7. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);
8. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;
9. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
10. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;
11. Suportar backup das configurações e rollback de configuração para a última configuração salva;

12. Suportar validação de regras antes da aplicação;
13. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
14. Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da regra selecionada;
15. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;
16. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
17. Permitir a criação de certificados digitais para autenticação de usuários;
18. A solução deve permitir o login de multiplos usuários administradores simultaneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução.
19. A solução deve permitir a integração da ferramenta com provedores de identidade para authenticação dos administradores da solução via SAML 2.0;
20. A solução deve permitir revisar e aprovar alterações de políticas de segurança feitas por outros administradores.
21. A solução deve possuir logs, correlação de eventos e relatórios de auditoria dos administradores da solução;
22. Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados;
23. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;
24. Deve ser possível exportar os logs em CSV ou TXT;
25. O visualizador de log deve ter um recurso de pesquisa de texto livre;
26. Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML;
27. Possibilitar rotação do log;
28. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:
    28.1. Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego;
29. Deve permitir a criação de relatórios personalizados;
30. Deve possuir capacidade de integração com soluções de terceiros via API e também suportar configurações através de RestAPI.
31. Deve consolidar logs e relatórios de todos os dispositivos administrados;
32. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;
33. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;
34. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;
35. Permitir que os relatórios possam ser salvos, enviados e impressos;
36. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como

a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc;

37. A solução deve prover, no mínimo, as seguintes funcionalidade para análise avançada dos incidentes:
38. Visualizar quantidade de tráfego utilizado de aplicações e navegação;
39. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;
40. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;
41. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;
42. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;
43. Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;
44. Criar certificados digitais para acesso dos usuários VPN;
45. Criar certificados digitais para VPNs Site-to-Site;
46. Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a sua maior capacidade ou ilimitada;
47. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;
48. Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição.
49. A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web, conteudo de arquivos, prevenção de ameaças e Sandbox, todos a partir de um único local centralizado possibilitando a procura correlacionada de logs em uma única tela, como por exemplo pesquisar logs de Antivirus e navegação web simultaneamente na mesma query de pesquisa.
50. O relatório das emulações (sandboxing) deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;
51. A A plataforma de gerência centralizada e monitoração deve possibilitar a procura por IPs e redes, sendo que os resultados mostrem estes Pps e redes nos campos de origem e destino do logs na mesma tela de pesquisa.
52. Possuir mecanismo para que logs antigos sejam removidos automaticamente;
53. Possuir a capacidade de personalização de gráficos como barra, linha e tabela;
54. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;
55. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;
56. A solução deve ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

57. A solução deve fornecer conteúdo de correlação pré-definido organizado por categoria;

58. A solução deve ser capaz de personalizar e criar regras de correlação;

59. A solução deve fornecer uma interface gráfica para criação das regras citadas no item anterior;

60. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

61. SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO LÓGICA DE SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DOS ITENS 1 A 6

61.1. PLANEJAMENTO:

61.1.1. Reunião de Kick-off – Deve ser realizada em duas etapas: a primeira com a equipe de implementação, abordando aspectos técnicos, integração, comunicação, e a segunda com o cliente tratando as formas de acompanhamento ao longo do projeto e prazo;

61.1.2. Visão geral do projeto, a fim de alinhar os objetivos e metas técnicas;

61.1.2.1. Escopo do Projeto;

61.1.2.2. Principais Entregas;

61.1.2.3. Limites do Projeto;

61.1.2.4. Possíveis riscos que podem ocorrer, bem como um plano de prevenção e/ou recuperação;

61.1.2.5. Equipe de execução do Projeto;

61.1.2.6. Prioridade do Projeto;

61.1.2.7. Cronograma do Projeto;

61.1.2.8. Esclarecimento de dúvidas;

61.1.2.9. Reunião de Follow-up – Deve ser realizada pelo menos uma vez por semana durante o período de implementação do projeto. Poderá ser feita de forma remota;

61.1.2.10. Relato breve quantificando do status das principais atividades do projeto;

61.1.2.11. Apresentação de fatos e informações relevantes que permitam análise e acompanhamento do andamento do projeto;

61.1.2.12. Avaliação de possíveis sanções que poderão ser aplicadas caso ocorram atrasos ou imprevistos no projeto, especialmente as que envolvem qualidade do trabalho, cronograma e custos;

61.1.2.13. Reunião EndUp – Deve ser uma reunião formal a ser realizada ao término de todas as atividades do projeto, com a presença do cliente, gerente do projeto e equipe do projeto;

61.1.2.14. Descrição resumida do projeto, desde seu início até sua finalização;

61.1.2.15. Síntese das fases e marcos principais e caracterização do cumprimento de tudo que ficou acertado e aceito pelo cliente em cada fase;

61.1.2.16. Certificação de que o projeto que está sendo entregue neste momento cumpre todos os requisitos acordados no início, e/ou modificados e redimensionados pelas partes ao longo dos trabalhos;

61.1.2.17. Entrega formal da documentação resultante da implementação do projeto;

61.2. IMPLANTAÇÃO:

61.2.1. Os serviços deverão ser executados na sua totalidade pela CONTRATADA e deverão obrigatoriamente ter o acompanhamento da equipe técnica da CONTRATANTE;

61.2.2. O escopo de implementação, migração de serviços, configuração de políticas e funcionalidades para os produtos deste termo de referência, contempla configurações lógicas e testes na sede da CONTRATANTE;

61.2.3. A instalação deverá ser executada no local definido pelo CONTRATANTE, mediante prévio agendamento e em acordo com o cronograma;

61.2.4. Em até 30 (trinta) dias corridos da assinatura do Contrato, a CONTRATADA deverá submeter à verificação e aprovação pela área Técnica de TI da CONTRATANTE o plano completo, mencionado neste Termo.

61.2.5. RECURSOS:

61.2.6. Os recursos humanos a serem alocados pela CONTRATADA, suas qualificações mínimas e os seus respectivos papéis e responsabilidades no projeto:

61.2.7. Gerente de Projetos – Profissional com certificação PMP ativa e experiência comprovada no gerenciamento de projetos de implantação e migração de soluções de infraestrutura de TI. Caberá a ele a liderança da equipe de projeto e as atividades de gerenciamento e facilitação para o alcance dos objetivos do projeto segundo as melhores práticas de mercado.

61.2.8. Analista (s) Integrador (es) – conjunto com um ou mais profissionais que (individualmente ou conjuntamente):

61.2.9. Reúna as certificações:

61.2.10. Certificação oficial do fabricante em nível Profissional na solução de segurança do fabricante ofertado neste certame;

61.2.11. Caberá a este(s) profissional(ais) equipe o desenvolvimento do projeto de arquitetura futura, a execução e coordenação de atividades de migração, implantação, instalação, configuração e testes; e outras atividades técnicas conforme as prescrições deste edital.

CARACTERÍSTICAS E ESPECIFICAÇÕES DA SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DOS ITENS 9 A 16

1. A solução de gerenciamento deve ser acessada através de provedores de nuvem pública, sem depender de instalações locais de software ou equipamentos para o seu funcionamento;

2. As funcionalidades descritas deverão ser providas no modelo SaaS (Software as a Service), como serviço, ou seja, todos os recursos de hardware, software, suporte, manutenção e segurança, para funcionamento da solução deverão ser providos pelo fornecedor;

3. A solução de gerenciamento deverá ser acessível através de navegador WEB padrão, com criptografia de tráfego SSL v1.3;

4. Todo acesso deverá ser controlado com autenticação de usuário em base própria e externa, utilizando Single-Sign-on através do protocolo SAML ou OAuth 2.0;

5. A solução de gerenciamento deverá permitir a gestão, monitoramento e ferramentas de diagnóstico para access points, controladoras wi-fi e switches, através de um único painel;

6. Toda a comunicação entre a solução de gerenciamento e os dispositivos gerenciados deverá ser feita através de conexão segura SSL v1.3;

7. As URLs de destino necessárias para estabelecimento da comunicação com os dispositivos a serem gerenciados deverão ser disponibilizadas;

8. A solução de gerenciamento deverá encaminhar por e-mail o convite para o usuário concluir seu cadastro, incluindo a definição de senha, para acesso a plataforma, assim que seu e-mail for incluído como novo usuário;

9. Deve disponibilizar aplicativo gratuito através das lojas oficiais (App Store e Google Play);

10. Toda a configuração, bem como a versão de software em que os equipamentos deverão utilizar, deverão ser automaticamente enviadas após a conclusão da implantação através do aplicativo;

11. Os equipamentos deverão permitir o acesso local, sem necessidade de abertura de chamado técnico com o fabricante, para realização das configurações iniciais para acesso a solução de gerenciamento, nos casos onde não houver serviço de configuração dinâmica de endereços IPs para acesso à Internet;

12. Toda a solução de gerenciamento deverá estar disponível em português, permitindo alternar para o Inglês conforme desejado pelo operador;

13. A solução de gerenciamento deve permitir a configuração baseada em grupos, permitindo que em um mesmo grupo possam ser definidas graficamente as configurações para switches e pontos de acesso WI- FI e controladoras;

14. As configurações do grupo ao qual o equipamento está associado deverão ser substituídas pelas configurações associadas ao equipamento específico (interfaces, VLAN, endereçamento IP, gateway, hostname);

15. Os grupos devem permitir dois modos de configuração dos equipamentos, interface gráfica e através de templates em arquivos de linha de comando;

16. Deverá permitir a visualização das diferenças de configuração entre o arquivo template e a configuração vigente no equipamento;

17. Deverá permitir que os equipamentos sejam movimentados entre grupos diferentes, assumindo sempre a configuração do grupo de destino;

18. Deverá permitir que as configurações sejam salvas através de acesso direto aos equipamentos via FTP e TFTP;

19. Deverá promover o SZTP (Secure Zero Touch Provisioning) RFC 8572 das configurações de equipamentos sem necessidade de acesso local;

20. Deverá permitir a configuração de política de conformidade de versão de software dos equipamentos por grupo de configuração;

21. Deverá executar a atualização de software automática quando o equipamento for associado ao grupo de destino, obedecendo a versão definida na política de conformidade;

22. Deverá permitir programar a atualização de software por localidade, definindo a data e horário para execução;

23. Deverá possuir API (Application Programming Interface) aberta que permita o acesso e integração a solução de gerenciamento, não só para monitoramento, mas também para configuração dos equipamentos e seus grupos;

24. Monitoramento (status e estatísticas) de clientes

25. Presença (detalhes de clientes conectados.

26. Segurança (reportar alertas de WIDS)

27. Deverá permitir o encaminhamento de alertas utilizando e-mail e/ou WEBHOOK, considerando, no mínimo, os seguintes escopos de alertas para encaminhamento:

27.1 Alertas de Usuários
27.2 Alertas de Pontos de Acesso WI-FI
27.3 Alertas de Switches
27.4 Controladoras
27.5 Alertas de conectividade com a solução de gerência
27.6 Alertas de auditoria
27.7 Alertas de localidade

28. Deverá identificar o dispositivo conectado a rede através da rede WIFI, expondo os seguintes parâmetros:

28.1 Categoria
28.2 Família
28.3 Sistema Operacional

29. Atributos de fluxo de tráfego por dispositivo.

30. Deverá permitir a integração, através de API.

31. Funcionalidade de relatórios:

31.1 Capacidade de geração de relatório para armazenagem de informações;
31.2 Coleta de informações da rede por períodos de tempo pré-definidos;
31.3 Capacidade de geração e envio automático de relatórios por e-mail;
31.4 Caso seja utilizado soluções de terceiros para a geração de relatórios, estas devem ser homologadas pela pelo fornecedor dos equipamentos de rede."

32. Funcionalidade de Gerenciamento de Convidados (Guests)

32.1 Deve possuir recurso de gerenciamento de convidados permite que os usuários convidados se conectem à rede e, ao mesmo tempo, permite que o administrador controle o acesso dos usuários convidados à rede.
32.2 Os administradores podem criar um perfil de página inicial para seus usuários convidados.
32.3 Deve permitir a personalização do layout da página inicial (vertical ou horizontal) com base no tipo de dispositivo.
32.4 Permitir que os convidados acessem a Internet fornecendo as credenciais configuradas pelos operadores convidados ou suas respectivas credenciais de login na rede social.
32.5 Permitir acesso utilizando logins sociais das rede Google, Twitter, and LinkedIn

33. A ferramenta deve ter capacidade de criar uma conta com permissão apenas de poder criar contas de usuários da rede Wi-Fi sem que tenha acesso as configurações dos elementos de rede ou outros serviços

34. Permitir a criação de contas de usuários da rede Wi-Fi com prazos de tempo

35. Deve permitir que os visitantes ou usuários convidados podem se registrar usando a página inicial ao tentar acessar a rede. A senha é entregue aos usuários por meio de impressão, SMS ou e-mail dependendo das opções selecionadas durante o cadastro.

36. As licenças que se aplicam aos dispositivos devem acompanhar período mínimo de 01 ano de subscrição, podendo ter sua prorrogação aplicada conforme as prorrogações contratuais prevista neste termo de referência.

37. Deve fornecer as credenciais de login por meio de impressão, mensagens de texto SMS ou e-mail.

38. SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO LÓGICA DE SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO DOS ITENS 9 A 16

38.1 PLANEJAMENTO:

38.1.1. Reunião de Kick-off – Deve ser realizada em duas etapas: a primeira com a equipe de implementação, abordando aspectos técnicos, integração, comunicação, e a segunda com o cliente tratando as formas de acompanhamento ao longo do projeto e prazo;

38.1.2. Visão geral do projeto, a fim de alinhar os objetivos e metas técnicas;

38.1.2.1. Escopo do Projeto;

38.1.2.2. Principais Entregas;

38.1.2.3. Limites do Projeto;

38.1.2.4. Possíveis riscos que podem ocorrer, bem como um plano de prevenção e/ou recuperação;

38.1.2.5. Equipe de execução do Projeto;

38.1.2.6. Prioridade do Projeto;

38.1.2.7. Cronograma do Projeto;

38.1.2.8. Esclarecimento de dúvidas;

38.1.2.9. Reunião de Follow-up – Deve ser realizada pelo menos uma vez por semana durante o período de implementação do projeto. Poderá ser feita de forma remota;

38.1.2.10. Relato breve quantificando do status das principais atividades do projeto;

38.1.2.11. Apresentação de fatos e informações relevantes que permitam análise e acompanhamento do andamento do projeto;

38.1.2.12. Avaliação de possíveis sanções que poderão ser aplicadas caso ocorram atrasos ou imprevistos no projeto, especialmente as que envolvem qualidade do trabalho, cronograma e custos;

38.1.2.13. Reunião EndUp – Deve ser uma reunião formal a ser realizada ao término de todas as atividades do projeto, com a presença do cliente, gerente do projeto e equipe do projeto;

38.1.2.14. Descrição resumida do projeto, desde seu início até sua finalização;

38.1.2.15. Síntese das fases e marcos principais e caracterização do cumprimento de tudo que ficou acertado e aceito pelo cliente em cada fase;

38.1.2.16. Certificação de que o projeto que está sendo entregue neste momento cumpre todos os requisitos acordados no início, e/ou modificados e redimensionados pelas partes ao longo dos trabalhos;

38.1.2.17. Entrega formal da documentação resultante da implementação do projeto;

38.2 IMPLANTAÇÃO:

38.2.1. Os serviços deverão ser executados na sua totalidade pela CONTRATADA e deverão obrigatoriamente ter o acompanhamento da equipe técnica da CONTRATANTE;

38.2.2. O escopo de implementação, migração de serviços, configuração de políticas e funcionalidades para os produtos deste termo de referência, contempla configurações lógicas e testes na sede da CONTRATANTE;

38.2.3. A instalação deverá ser executada no local definido pelo CONTRATANTE, mediante prévio agendamento e em acordo com o cronograma;

38.2.4. Em até 30 (trinta) dias corridos da assinatura do Contrato, a CONTRATADA deverá submeter à verificação e aprovação pela área Técnica de TI da CONTRATANTE o plano completo, mencionado neste Termo.

38.2.5. RECURSOS:

38.2.5.1. Os recursos humanos a serem alocados pela CONTRATADA, suas qualificações mínimas e os seus respectivos papéis e responsabilidades no projeto:

38.2.5.1.1. Gerente de Projetos – Profissional com certificação PMP ativa e experiência comprovada no gerenciamento de projetos de implantação e migração de soluções de infraestrutura de TI. Caberá a ele a liderança da equipe de projeto e as atividades de gerenciamento e facilitação para o alcance dos objetivos do projeto segundo as melhores práticas de mercado.

38.2.5.1.2. Analista (s) Integrador (es) – conjunto com um ou mais profissionais que (individualmente ou conjuntamente):

38.2.5.1.3. Reúna as certificações:

38.2.5.1.4. Certificação oficial do fabricante em nível Profissional na solução de rede WLAN do fabricante ofertado neste certame;

38.2.5.1.5. Caberá a este(s) profissional(ais) equipe o desenvolvimento do projeto de arquitetura futura, a execução e coordenação de atividades de migração, implantação, instalação, configuração e testes; e outras atividades técnicas conforme as prescrições deste edital.

ANEXO D - CARACTERÍSTICAS E ESPECIFICAÇÕES DA SERVIÇOS DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE SEGURA, INSTALAÇÃO CONFIGURAÇÃO E TESTES (ITENS 1 A 8)

1. PLANEJAMENTO:

1.1 Reunião de Kick-off – Deve ser realizada em duas etapas: a primeira com a equipe de implementação, abordando aspectos técnicos, integração, comunicação, e a segunda com o cliente tratando as formas de acompanhamento ao longo do projeto e prazo;

1.2 Visão geral do projeto, a fim de alinhar os objetivos e metas técnicas;

1.3 Escopo do Projeto;

1.4 Principais Entregas;

1.5 Limites do Projeto;

1.6 Possíveis riscos que podem ocorrer, bem como um plano de prevenção e/ou recuperação;

1.7 Equipe de execução do Projeto;

1.8 Prioridade do Projeto;

1.9 Cronograma do Projeto;

1.10 Esclarecimento de dúvidas;

1.11 Reunião de Follow-up – Deve ser realizada pelo menos uma vez por semana durante o período de implementação do projeto. Poderá ser feita de forma remota;

1.12 Relato breve quantificando do status das principais atividades do projeto;

1.13 Apresentação de fatos e informações relevantes que permitam análise e acompanhamento do andamento do projeto;

1.14 Avaliação de possíveis sanções que poderão ser aplicadas caso ocorram atrasos ou imprevistos no projeto, especialmente as que envolvem qualidade do trabalho, cronograma e custos;

1.15 Reunião EndUp – Deve ser uma reunião formal a ser realizada ao término de todas as atividades do projeto, com a presença do cliente, gerente do projeto e equipe do projeto;

1.16 Descrição resumida do projeto, desde seu início até sua finalização;

1.17 Síntese das fases e marcos principais e caracterização do cumprimento de tudo que ficou acertado e aceito pelo cliente em cada fase;

1.18 Certificação de que o projeto que está sendo entregue neste momento cumpre todos os requisitos acordados no início, e/ou modificados e redimensionados pelas partes ao longo dos trabalhos;

1.19 Entrega formal da documentação resultante da implementação do projeto;

2. IMPLANTAÇÃO:

2.1 Os serviços deverão ser executados na sua totalidade pela CONTRATADA e deverão obrigatoriamente ter o acompanhamento da equipe técnica da CONTRATANTE;

2.2 O escopo de implementação, migração de serviços, configuração de políticas e funcionalidades para os produtos deste termo de referência, contempla configurações lógicas e testes na sede da CONTRATANTE;

2.3 A instalação deverá ser executada no local definido pelo CONTRATANTE, mediante

prévio agendamento e em acordo com o cronograma;

2.4 Em até 30 (trinta) dias corridos da assinatura do Contrato, a CONTRATADA deverá submeter à verificação e aprovação pela área Técnica de TI da CONTRATANTE o plano completo, mencionado neste Termo.

2.5 Os produtos e soluções terão como prazo de entrega um período de 60 dias corridos a partir da data de emissão da ordem de compra ou execução.

3. RECURSOS:

3.1 Os recursos humanos a serem alocados pela CONTRATADA, suas qualificações mínimas e os seus respectivos papéis e responsabilidades no projeto:

3.1.1 Gerente de Projetos – Profissional com certificação PMP ativa e experiência comprovada no gerenciamento de projetos de implantação e migração de soluções de infraestrutura de TI. Caberá a ele a liderança da equipe de projeto e as atividades de gerenciamento e facilitação para o alcance dos objetivos do projeto segundo as melhores práticas de mercado.

3.1.2 Analista (s) Integrador (es) – conjunto com um ou mais profissionais que (individualmente ou conjuntamente):

3.1.2.1 Reúna as certificações:

3.1.2.2 Certificação oficial do fabricante em nível Expert na solução de segurança do fabricante ofertado neste certame;

3.2 Caberá a este(s) profissional(ais) equipe o desenvolvimento do projeto de arquitetura futura, a execução e coordenação de atividades de migração, implantação, instalação, configuração e testes; e outras atividades técnicas conforme as prescrições deste edital.

CARACTERÍSTICAS E ESPECIFICAÇÕES DA SERVIÇOS DE DISPONIBILIZAÇÃO DE SOLUÇÃO DE CONECTIVIDADE LAN E SOFTWARE, INSTALAÇÃO CONFIGURAÇÃO E TESTES (ITENS 9 A 12)

4. PLANEJAMENTO:

4.1 Reunião de Kick-off – Deve ser realizada em duas etapas: a primeira com a equipe de implementação, abordando aspectos técnicos, integração, comunicação, e a segunda com o cliente tratando as formas de acompanhamento ao longo do projeto e prazo;

4.2 Visão geral do projeto, a fim de alinhar os objetivos e metas técnicas;

4.3 Escopo do Projeto;

4.4 Principais Entregas;

4.5 Limites do Projeto;

4.6 Possíveis riscos que podem ocorrer, bem como um plano de prevenção e/ou recuperação;

4.7 Equipe de execução do Projeto;

4.8 Prioridade do Projeto;

4.9 Cronograma do Projeto;

4.10 Esclarecimento de dúvidas;

4.11 Reunião de Follow-up – Deve ser realizada pelo menos uma vez por semana durante o período de implementação do projeto. Poderá ser feita de forma remota;

4.12 Relato breve quantificando do status das principais atividades do projeto;

4.13 Apresentação de fatos e informações relevantes que permitam análise e acompanhamento do andamento do projeto;

4.14 Avaliação de possíveis sanções que poderão ser aplicadas caso ocorram atrasos ou imprevistos no projeto, especialmente as que envolvem qualidade do trabalho, cronograma e custos;

4.15 Reunião EndUp – Deve ser uma reunião formal a ser realizada ao término de todas as atividades do projeto, com a presença do cliente, gerente do projeto e equipe do projeto;

4.16 Descrição resumida do projeto, desde seu início até sua finalização;

4.17 Síntese das fases e marcos principais e caracterização do cumprimento de tudo que ficou acertado e aceito pelo cliente em cada fase;

4.18 Certificação de que o projeto que está sendo entregue neste momento cumpre todos os requisitos acordados no início, e/ou modificados e redimensionados pelas partes ao longo dos trabalhos;

4.19 Entrega formal da documentação resultante da implementação do projeto;

5. IMPLANTAÇÃO:

5.1 Os serviços deverão ser executados na sua totalidade pela CONTRATADA e deverão obrigatoriamente ter o acompanhamento da equipe técnica da CONTRATANTE;

5.2 O escopo de implementação, migração de serviços, configuração de políticas e funcionalidades para os produtos deste termo de referência, contempla configurações lógicas e testes na sede da CONTRATANTE;

5.3 A instalação deverá ser executada no local definido pelo CONTRATANTE, mediante prévio agendamento e em acordo com o cronograma;

5.4 Em até 30 (trinta) dias corridos da assinatura do Contrato, a CONTRATADA deverá submeter à verificação e aprovação pela área Técnica de TI da CONTRATANTE o plano completo, mencionado neste Termo.

5.5 Os produtos e soluções terão como prazo de entrega um período de 60 dias corridos a partir da data de emissão da ordem de compra ou execução.

6. RECURSOS:

6.1 Os recursos humanos a serem alocados pela CONTRATADA, suas qualificações mínimas e os seus respectivos papéis e responsabilidades no projeto:

6.1.1 Gerente de Projetos – Profissional com certificação PMP ativa e experiência comprovada no gerenciamento de projetos de implantação e migração de soluções de infraestrutura de TI. Caberá a ele a liderança da equipe de projeto e as atividades de gerenciamento e facilitação para o alcance dos objetivos do projeto segundo as melhores práticas de mercado.

Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP:60.130-240 - Fortaleza/CE
Fone: (85) 3108-0000
www.etice.ce.gov.br

6.1.2 Analista (s) Integrador (es) – conjunto com um ou mais profissionais que (individualmente ou conjuntamente):

6.1.2.1 Reúna as certificações:

6.1.2.2 Certificação oficial do fabricante em nível Profissional na solução de rede LAN/SWITCH do fabricante ofertado neste certame;

6.2 Caberá a este(s) profissional(ais) equipe o desenvolvimento do projeto de arquitetura futura, a execução e coordenação de atividades de migração, implantação, instalação, configuração e testes; e outras atividades técnicas conforme as prescrições deste edital.

ANEXO E - CARACTERÍSTICAS E ESPECIFICAÇÕES DA SERVIÇOS DE DISPONIBILIZAÇÃO DE CONECTIVIDADE WLAN E SOFTWARE, INSTALAÇÃO CONFIGURAÇÃO E TESTES (ITENS 13 A 16)

1. Ficarão a cargo da contratada o trabalho de fixação dos dispositivos, instalação dos injetores PoE (quando for o caso), conectorização de patch cords, configuração dos dispositivos e demais atividades técnicas necessárias para operacionalização dos access points. O serviço de passagem de cabeamento entre o patch panel e o ponto de acesso não está no escopo do serviço de instalação da contratada;
2. **PLANEJAMENTO:**
   - **2.1.** Reunião de Kick-off – Deve ser realizada em duas etapas: a primeira com a equipe de implementação, abordando aspectos técnicos, integração, comunicação, e a segunda com o cliente tratando as formas de acompanhamento ao longo do projeto e prazo;
   - **2.2.** Visão geral do projeto, a fim de alinhar os objetivos e metas técnicas;
   - **2.3.** Escopo do Projeto;
   - **2.4.** Principais Entregas;
   - **2.5.** Limites do Projeto;
   - **2.6.** Possíveis riscos que podem ocorrer, bem como um plano de prevenção e/ou recuperação;
   - **2.7.** Equipe de execução do Projeto;
   - **2.8.** Prioridade do Projeto;
   - **2.9.** Cronograma do Projeto;
   - **2.10.** Esclarecimento de dúvidas;
   - **2.11.** Reunião de Follow-up – Deve ser realizada pelo menos uma vez por semana durante o período de implementação do projeto. Poderá ser feita de forma remota;
   - **2.12.** Relato breve quantificando do status das principais atividades do projeto;
   - **2.13.** Apresentação de fatos e informações relevantes que permitam análise e acompanhamento do andamento do projeto;
   - **2.14.** Avaliação de possíveis sanções que poderão ser aplicadas caso ocorram atrasos ou imprevistos no projeto, especialmente as que envolvem qualidade do trabalho, cronograma e custos;
   - **2.15.** Reunião EndUp – Deve ser uma reunião formal a ser realizada ao término de todas as atividades do projeto, com a presença do cliente, gerente do projeto e equipe do projeto;
   - **2.16.** Descrição resumida do projeto, desde seu início até sua finalização;
   - **2.17.** Síntese das fases e marcos principais e caracterização do cumprimento de tudo que ficou acertado e aceito pelo cliente em cada fase;
   - **2.18.** Certificação de que o projeto que está sendo entregue neste momento cumpre todos os requisitos acordados no início, e/ou modificados e redimensionados pelas partes ao longo dos trabalhos;
   - **2.19.** Entrega formal da documentação resultante da implementação do projeto;
3. **IMPLANTAÇÃO:**
   - **3.1.** Os serviços deverão ser executados na sua totalidade pela CONTRATADA e deverão obrigatoriamente ter o acompanhamento da equipe técnica da CONTRATANTE;
   - **3.2.** O escopo de implementação, migração de serviços, configuração de políticas e funcionalidades para os produtos deste termo de referência, contempla configurações lógicas e testes na sede da CONTRATANTE;

3.3. A instalação deverá ser executada no local definido pelo CONTRATANTE, mediante prévio agendamento e em acordo com o cronograma;

3.4. Em até 30 (trinta) dias corridos da assinatura do Contrato, a CONTRATADA deverá submeter à verificação e aprovação pela área Técnica de TI da CONTRATANTE o plano completo, mencionado neste Termo.

3.5. Os produtos e soluções terão como prazo de entrega um período de 60 dias corridos a partir da data de emissão da ordem de compra ou execução.

4. RECURSOS:

4.1. Os recursos humanos a serem alocados pela CONTRATADA, suas qualificações mínimas e os seus respectivos papéis e responsabilidades no projeto:

4.2. Gerente de Projetos – Profissional com certificação PMP ativa e experiência comprovada no gerenciamento de projetos de implantação e migração de soluções de infraestrutura de TI. Caberá a ele a liderança da equipe de projeto e as atividades de gerenciamento e facilitação para o alcance dos objetivos do projeto segundo as melhores práticas de mercado.

4.3. Analista (s) Integrador (es) – conjunto com um ou mais profissionais que (individualmente ou conjuntamente):

4.3.1. Reúna as certificações:

4.3.2. Certificação oficial do fabricante em nível Profissional na solução de rede WLAN do fabricante ofertado neste certame;

4.4. Caberá a este(s) profissional(ais) equipe o desenvolvimento do projeto de arquitetura futura, a execução e coordenação de atividades de migração, implantação, instalação, configuração e testes; e outras atividades técnicas conforme as prescrições deste edital.

4.5. A CONTRATADA deverá comprovar o vínculo societário ou empregatício e as qualificações do(s) técnico(s) que vier(em) prestar serviços nas dependências do CONTRATANTE;

4.6. A comprovação de que a empresa possui em seu quadro funcional os profissionais solicitados dar- se-á mediante cópias autenticadas das Carteiras de Trabalho ou fichas de Registro de Empregado, cópia do ato de investidura no cargo ou cópia do contrato social e suas alterações em se tratando de sócio, ou ainda através de contrato de prestação de serviços;

1. A CONTRATADA dará suporte e assistência técnica 24X7 conforme descrito abaixo caso um dos itens 1 a 8 seja contratado:

2. A CONTRATADA será responsável pela administração e manutenção do serviço em regime de 24x7 para atendimentos remotos e o regime 8x5 para atendimentos que possam ser necessários na forma presencial, durante todo o período do serviço comtemplado nesse Edital. As tarefas atinentes ao transporte, deslocamento e remessa necessários, seja na implementação, substituição e/ ou remoção de equipa- mentos defeituosos será de responsabilidade da CONTRATADA.

3. Para garantir a qualidade e disponibilidade do serviço, deverá ser disponibilizado pela empresa CONTRATADA uma ferramenta de monitoramento com estrutura dedicada

4. A ferramenta deve ser acompanhada de todos os itens necessários para operacionalização, tais como: softwares de apoio (sistema operacional, etc) e licenças de softwares;

5. O serviço de monitoramento 24x7 deverá ser prestado OBRIGATÓRIA E INDISPENSAVELMENTE através de NOCs (Network Operation Center) redundantes da empresa CONTRATADA que já deverão estar em pleno funcionamento até a data da assinatura do Contrato. Será o ponto único de contato com a equipe técnica da CONTRATANTE para abertura de chamados, incidentes, problemas, dúvidas e requisições relacionadas aos serviços contratados, atuando como a primeira instância de atendimento à CONTRATANTE.

6. Os serviços prestados pelo NOC compreendem, entre outros, os seguintes procedimentos:

6.1. Monitoramento pró-ativo do ambiente de rede WAN do CONTRATANTE;

6.2. Suporte técnico para identificação e resolução de problemas em software e nos equipamentos;

6.3. Resolução de problemas quanto acesso à internet, sites remotos, serviços de rede oferecidos aos funcionários do CONTRATANTE;

6.4. Resolução de problemas referente aos meios de Acesso WAN, tais como: MPLS e Ethernet;

6.5. Suporte em criação de políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

6.6. Resolução de problemas referente a políticas, configurações, parametrizações de quaisquer ordens relativos aos equipamentos ofertados;

6.7. Suporte à criação, geração e parametrização de relatórios e eventos de segurança de quaisquer naturezas detectados e prevenidos pelos equipamentos ofertados;

7. Encaminhar incidentes ao fabricante da solução;

8. Suporte em demais configurações de segurança, redundância e gerência;

9. Suporte, administração e monitoramento das políticas e tarefas de backup das configurações;

10. Apoio técnico para tarefas de auditoria e análise de logs.

11. A CONTRATADA deverá agir de forma reativa para incidentes, restabelecimento do serviço o mais rápido possível minimizando o impacto, seja por meio da uma solução de contorno ou definitiva. Ainda caberá a CONTRATADA agir de forma proativa aplicando medidas para a boa manutenção afim de garantir a regularidade da operação do serviço.

12. O atendimento e suporte técnico especializado de 1° (primeiro nível) será sempre telefônico e remoto em regime 24x7 e assim, responsável pelo acompanhamento e gestão dos chamados, controle dos Indicadores de monitoramento, atuando como ponto único de contato entre

a CONTRATANTE e profissionais da equipe da CONTRATADA.

13. O atendimento e suporte técnico especializado de 2° (segundo nível) poderá ser presencial ou remoto em regime 8x5 em todo estado do Ceará caso o suporte remoto não seja suficiente para resolução do problema. Responsável pela prevenção e resolução de incidentes, problemas e requisições, identificando a causa raiz de eventual problema e buscando sua solução. Execução de atividades remotas e/ou presenciais em incidentes, solicitações de maior complexidade.

14. Os Técnicos deverão ser capacitados e certificados para prestação dos serviços, resolução de incidentes, problemas e solicitações nos equipamentos ofertados. O comparecimento de um técnico ao local da necessidade será de no máximo 48 (quarenta e oito) horas para atendimentos na área que abrange e define a Região Metropolitana de Fortaleza e de até 5 (cinco) dias para as outras demais localidades (interior do Estado) e devendo sempre atender aos critérios de SLA determinados nesse Edital.

15. Para abertura dos chamados de suporte, a CONTRATADA deverá disponibilizar número telefônico 0800 (ou equivalente a ligação local), também serviço via portal WEB e/ou e-mail (em português). Na abertura do chamado, o órgão ao fazê-lo, receberá naquele momento, o número, data e hora de abertura do chamado. Este será considerado o início para contagem dos SLAS. O fechamento do chamado deverá ser comunicado pela CONTRATADA para fins de contagem do tempo de atendimento e resolução do chamado.

16. A CONTRATADA deverá possuir na sua equipe profissionais com as seguintes certificações obriga- tórias e indispensáveis em face da complexidade da prestação dos serviços requeridos e ainda mais da rede computacional:

16.1. Profissional com nível professional na solução ofertada

16.2. Profissional com certificação ITIL Foundation;

16.3. Profissional com certificação PMP;

17. A atualização de firmware quando disponibilizado exclusivamente pelo próprio fabricante dos equipamentos deverá ser executada pela CONTRATADA sem custo adicional, sempre que requisitado pela CONTRATANTE. Toda e qualquer atualização só poderá ser aplicada mediante autorização da CONTRATANTE. As atualizações deverão ocorrer em data e horário determinado pela CONTRATADA em comum acordo e autorização da CONTRATANTE visando manter em normal funcionamento a rede onde estiverem funcionando.

18. A CONTRATADA deverá fornecer informações de monitoramento on-line, via dashboard que permita o acompanhamento em tempo real do estado dos ativos. Deverá ainda apresentar relatórios mensais, por meio digital (DOCX, XLSX ou PDF), com o diagnóstico e controle dos equipamentos monitorados (dados, informações, descrição, indicadores e métricas que permitam quantificar o desempenho e a disponibilidade da ope- ração do serviço).

19. A CONTRATADA deverá disponibilizar uma ferramenta de Service Desk comprovadamente ade- rente as boas práticas do ITIL e que contenha o detalhamento dos chamados com no mínimo as seguintes informações: o funcionário do órgão/entidade que realizou a abertura do chamado, data e hora de abertura, data e hora de atendimento, data e hora de solução, o funcionário do órgão/entidade que realizou o encerramento do chamado, descrição detalhada do problema e das ações tomadas para sua resolução e a relação dos equipa- mentos ou componentes substituídos, especificando marca, modelo, fabricante e número de série).

20. Os relatórios de chamados abertos poderão ser solicitados a qualquer instante pela CONTRATAN- TE dentro das condições estipuladas, respeitando, no entanto, um prazo de até 48

(quarenta e oito) horas uteis. Esses relatórios deverão ser retidos pelo tempo mínimo equivalente a vigência do contrato e após o seu encerramento inutilizados.

21. A CONTRATADA deverá comunicar ao CONTRATANTE, os casos de eminente falha operacional dos equipamentos ou de qualquer outra ação que possa vir a colocar em risco a operação da rede dela, mesmo que a falha não tenha sido consumada, mas que tenha sido detectada a existência do risco.

22. A CONTRATANTE deverá definir pessoas do seu Quadro de Funcionários que terão acesso de Ad- ministração nos equipamentos disponibilizados e essas pessoas deverão comunicar à empresa CONTRATADA qualquer alteração de configuração realizada nos equipamentos fornecidos nessa contratação e nessa situação respondendo por sua conta e risco pelas intervenções que possam ter efetuado.

23. A CONTRATADA deverá respeitar os tempos máximos de ATENDIMENTOS e SLA (Nível de Acordo de Serviço) abaixo descritos, sob a pena de multa no caso de falhas em seu integral cumprimento:

24. Operação parada (incidente que gere parada total de algum serviço contemplado nesse contrato) o tempo de atendimento será de até 2 (duas) horas.

25. Operação impactada (incidente que gere parada parcial de algum serviço contemplado nesse contrato) o tempo de atendimento será de até 4 (quatro) horas.

26. Requisição de serviço (solicitações de mudanças nos equipamentos ou serviços do contrato) o tempo de atendimento será de até 8 (oito) horas.

27. Informações de contrato (solicitação de informação, parecer ou relatório de algum serviço contemplado no contrato) o tempo de atendimento será de até 12 (doze) horas.

ANEXO G - CATÁLOGO DE SERVIÇOS

O catálogo de serviços apresentado na tabela abaixo lista as complexidades esperadas para cada serviço a ser executado.

Este catálogo pode ser alterado pontualmente na medição de serviços no caso de ser detectado pela CONTRATADA e aprovado pelo CONTRATANTE que o serviço apresenta para uma determinada atividade uma complexidade diferente da listada.

Este catálogo pode ser alterado continuamente no caso de ser detectado pela CONTRATADA e aprovado pelo CONTRATANTE que o serviço apresenta para a maioria das atividades relacionadas a ele uma complexidade diferente da listada.

SERVIÇO	COMPLEXIDADE
Avaliação e descoberta de portfólio de aplicações e suas interdependências para construção de plano para migração.	Intermediário
Avaliação de infraestrutura existente para dimensionamento de infraestrutura necessária em ambiente de nuvem.	Intermediário
Migração de cargas de trabalho entre sistemas operacionais(Linux/ Windows)	Intermediário
Migração de cargas de trabalho entre bancos de dados heterogêneos.	Alta
Migração de bases de dados on-premises para nuvem, com ou sem atualização de versão, para: outros motores suportados; bases de dados para propósitos específicos (NoSQL).	Alta
Migração de containers on-premises para soluções de orquestração e repositório de containers gerenciados.	Alta
Migração de cargas de trabalho, elegíveis, de máquinas virtuaispara containers.	Alta
Migração de cargas de trabalho, elegíveis, máquinas virtuais oucontainers para modelo sem servidor.	Alta
Migração de cargas de trabalho em máquinas virtuais paraserviços gerenciados e não gerenciados elegíveis.	Alta
Implementação de mecanismo de alta disponibilidade, escalabilidade horizontal automatizada, monitoramento, verificações de saúde e balanceamento de carga.	Alta

Construção de data warehouse e/ou datamarts a partir de uma ou mais fontes de dados, escalabilidade vertical e horizontal e otimizações de consultas	Especialista
Construção de soluções de analytics a partir de uma ou mais fontes de dados, escalabilidade vertical e horizontal e otimizações de consultas	Especialista
Construção de soluções de Big Data a partir de uma ou mais fontes de dados, escalabilidade vertical e horizontal e otimizações de consultas	Especialista
Desenvolvimento e implementação de projetos que envolvem tecnologias de Inteligência Artificial, linguagens e aprendizado de máquina, redes neurais, preditivas e demais tecnologiasenvolvidas.	Especialista
Desenvolvimento e implementação de projetos de atendimento virtual, robôs e demais ferramentas de conversação inteligente automatizada.	Especialista
Desenvolvimento e implementação de projetos que envolvem soluções de IoT (Internet das Coisas).	Especialista
Implementação de rede de entrega de conteúdo para conteúdo(site) estáticos.	Intermediário
Criação/configuração de topologia de redes interconectadas com isolamento, firewall, ACL's (Access Control Lists) e auditoria.	Intermediário
Implementação e configuração de conectividade do ambienteon-premises com ambiente em nuvem.	Intermediário
Configuração de serviço de DNS, público ou privado, eintegração com serviço de DNS on-premises.	Intermediário
Implementação de modelo de categorização de custos combase em rótulos, orçamentos e alarmes de consumo mensal.	Baixa
Implementação de controles para filtro de requisições Web classificadas como nocivas.	Intermediário
Configuração de cofre de senhas para armazenamento de credenciais, chaves e outros dados sensíveis.	Intermediário
Automação do provisionamento e gerência de configuração de serviços e recursos de nuvem com modelo de infraestrutura como código e autosserviço.	Alta
Implementação de solução para gerenciamento e automaçãode backup de dados nos serviços de nuvem ou ambiente on-premises.	Intermediário

Implementação de solução para backup de dados de longaretenção com políticas de ciclo de vida.	Intermediário
Implementação de processos de transferência de grandes volumes de dados para nuvem, incluindo processo de backup e restauração em novo ambiente.	Intermediário
Desenho e implantação de arquitetura para continuidade de negócios e recuperação de desastres em ambiente de nuvemde acordo com requisitos de RTO (Recovery Time Objective) e RPO (Recovery Point Objective).	Especialista
Apresentação de workshops/transferência de conhecimentopara detalhamento de entregáveis.	Baixa
Configuração de estrutura de contas em conformidade commelhores práticas de segurança.	Intermediário
Avaliação de ambiente em nuvem sobre perspectiva de segurança, desempenho, confiabilidade, custos e eficiência operacional e aplicação de correções apropriadas.	Alta
Migração fim-a-fim de máquinas virtuais incluindo os processos de conversão, importação, configuração e testes do ambiente migrado.	Alta
Implementação de ambiente para virtualização de desktops,incluindo configuração de redes, autenticação, políticas de gerenciamento e imagens personalizadas com configurações e aplicativos.	Alta
Gerenciamento dos provedores de serviço, orquestração,bilhetagem, implementação de mecanismos de controle, otimização de custos, sustentação e operação de ambiente de Nuvem com execução de tarefas do dia a dia: monitoramento, aplicações de patches, backup, atendimento de requisições de tarefas e mudanças.	Baixa
Serviço de monitoramento dos recursos e componentes dasolução.	Baixo

Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP:60.130-240 - Fortaleza/CE
Fone: (85) 3108-0000
www.etice.ce.gov.br

ANEXO H - LISTA DE PERFIS TÉCNICOS

1. A tabela a seguir estabelece relação entre os perfis técnicos dos recursos a serem alocados na execução dos serviços, sejam profissionais ou materiais, com o peso adotado do para efeito de cálculo do esforço considerado no dimensionamento de USTs do serviço.

Item	Perfil Técnico	Requisitos Técnicos Mínimos Obrigatórios de Enquadramento	Peso
1	Auxiliar Técnico I	**Do Auxiliar Técnico de TIC de Nível I** Enquadram-se profissionais com formação de nível médio em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência comprovada e no mínimo 01 (um) ano em atividades e funções correlatas ao serviço. **Do Auxiliar Técnico de Processo de Negócio de Nível I** Enquadram-se profissionais com formação de nível médio em qualquer área compatível com o processo de negócio objeto da atividade, com experiência comprovada e no mínimo 01 (um) ano em atividades e funções correlatas ao serviço.	0,25
2	Auxiliar Técnico II	**Do Auxiliar Técnico de TIC de Nível II** Enquadram-se profissionais com formação de nível médio em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência comprovada e no mínimo 02 (dois) anos em atividades e funções correlatas ao serviço. **Do Auxiliar Técnico de Processo de Negócio Nível II** Enquadram-se profissionais com formação de nível médio em qualquer área compatível com o processo de negócio objeto da atividade, com experiência comprovada e no mínimo 02 (dois) anos em atividades e funções correlatas ao serviço.	0,50
3	Técnico I	**Do Técnico de TIC de Nível I** Enquadram-se profissionais com formação de nível médio em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência mínima de 03 (três) anos em atividades e funções correlatas ao serviço. **Do Técnico de Processo de Negócio Nível I** Enquadram-se profissionais com formação de nível médio em qualquer área compatível área compatível com o processo de	1

		negócio objeto da atividade, com experiência mínima de, 03 (três) anos em atividades e funções correlatas ao serviço.	
4	Técnico II	**Do Técnico de TIC de Nível II** Enquadram-se profissionais com formação de nível superior em andamento com, pelo menos, 50% (cinquenta por cento) do curso concluído em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço com experiência comprovada de no mínimo 03 (três) anos em atividades e funções correlatas ao serviço. Ou	1,5

		Alternativamente, profissionais com formação de nível médio em qualquer área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência mínima de 05 (cinco) anos em atividades e funções correlatas ao serviço. **Do Técnico de Processo de Negócio Nível II** Enquadram-se profissionais com formação de nível superior em andamento com, pelo menos, 50% (cinquenta por cento) do curso concluído em área compatível com o processo de negócio objeto da atividade, com experiência comprovada de no mínimo 03 (três) anos em atividades e funções correlatas ao serviço. Ou Alternativamente, profissionais com formação de nível médio em qualquer em área compatível com o processo de negócio objeto da atividade, com experiência comprovada mínima de 05 (cinco) anos em atividades e funções correlatas ao serviço.	
5	Analista I	**Do Analista de TIC de Nível I** Enquadram-se os profissionais com formação de nível superior em área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, e experiência comprovada de no mínimo 05 (cinco) anos em atividades e funções correlatas ao serviço, **Do Analista de Processo de Negócio Nível I** Enquadram-se profissionais com formação de nível superior compatível com o processo de negócio objeto da atividade, com experiência mínima de 05 (cinco) anos em atividades e funções correlatas ao processo objeto da atividade.	2,0
6	Analista II	**Do Analista de TIC de Nível II** Enquadram-se os profissionais com formação de nível superior e pós- graduação (no mínimo Lato Sensu) concluída ou em andamento em área compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, e experiência comprovada de no mínimo 06 (seis) anos em atividades e funções correlatas ao serviço; Ou, Alternativamente, formação de nível superior compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, com experiência mínima de 08 (oito) anos em atividades e funções correlatas ao serviço. **Do Analista de Processo de Negócio Nível II**	2,50

		Enquadram-se os profissionais com formação de nível superior e pós- graduação (no mínimo Lato Sensu) concluída ou em andamento em área compatível com o processo de negócio objeto da atividade, com experiência comprovada de no mínimo 06 (seis) anos em atividades e funções correlatas ao processo objeto da atividade. Ou, Alternativamente, formação de nível superior compatível com o processo de negócio objeto da atividade, com experiência mínima de 08 (oito) anos em atividades e funções correlatas ao processo objeto da atividade.	
7	Especialista I	**Do Especialista de TIC de Nível I** Enquadram-se os profissionais com formação de nível superior e pós- graduação (no mínimo Lato Sensu) compatível com as técnicas e tecnologias	3,00
		aplicadas às atividades inerentes ao serviço, e experiência comprovada de no mínimo 07 (sete) anos em atividades e funções correlatas ao serviço; Ou, Alternativamente, formação de nível superior compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividades e funções correlatas ao serviço. **Do Especialista de Processo de Negócio Nível I** Enquadram-se os profissionais com formação de nível superior e pós- graduação (no mínimo Lato Sensu) em área compatível com o processo de negócio objeto da atividade, com experiência comprovada de, no mínimo, 07 (sete) anos em atividades e funções correlatas ao processo objeto da atividade. Ou, Alternativamente, formação de nível superior compatível com o processo de negócio objeto da atividade, com certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividades e funções correlatas ao processo objeto da atividade.	

8	Especialista II	**Do Especialista de TIC de nível II** Enquadram-se os profissionais com formação de nível superior e pós- graduação (no mínimo Stricto Sensu) compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço e experiência comprovada de, no mínimo, 08 (oito) anos em atividades e funções correlatas ao serviço, Ou, Alternativamente, formação de nível superior e pós-graduação (no mínimo Lato Sensu) compatível com as técnicas e tecnologias aplicadas às atividades inerentes ao serviço, certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividades e funções correlatas ao serviço. **Do Especialista de Processo de Negócio nível II** Enquadram-se os profissionais com formação de nível superior e pós- graduação (no mínimo Stricto Sensu) em área compatível com o processo de negócio objeto da atividade, com experiência comprovada de, no mínimo, 08 (oito) anos em atividades e funções correlatas ao processo objeto da atividade; Ou, Alternativamente, formação de nível superior e pós-graduação (no mínimo Lato Sensu) compatível com o processo de negócio objeto da atividade, com certificações de proficiência técnica correlata e experiência mínima de 10 (dez) anos em atividades e funções correlatas ao processo objeto da atividade.	3,50

2. Com vistas a favorecer o processo de precificação do serviço no que se refere a alocação de recursos necessários ao serviço, considerada a necessidade de execução contínua de dadas atividades, a aceitabilidade definida dos perfis por serviços relacionados no catálogo de serviços, e cenários atuais relativos aos serviços demandados, estima-se que para correta execução dos serviços, os recursos necessários serão alocados com base na seguinte distribuição de tempo:

Perfil Técnico	**Alocação estimada**
Auxiliar I	17%
Auxiliar II	17%
Técnico I	16%
Técnico II	16%
Analista I	16%

Analista II	8%
Especialista I	5%
Especialista II	5%

3. Considerando os serviços listados no catálogo, seus pesos e distribuições adote-se apenas como referência para precificação, o fator médio de 1,368 para conversão entre horas de alocação e UST conforme a seguinte fórmula: Número de horas alocadas = (Número de UST_mês/(1,368*COMPLEXIDADE)). Esse fator foi definido com consideração a média de todos os pesos aplicáveis aos serviços no catálogo, permitindo uma aproximação do quantitativo em horas, da alocação necessária de recursos para a execução dos serviços.
   3.1. A CONTRATADA deverá propor um fator diferente do fator médio para aqueles casos em que a alocação real não está de acordo com a alocação estimada, o qual será avaliado pela CONTRATANTE.

Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP:60.130-240 - Fortaleza/CE
Fone: (85) 3108-0000
www.etice.ce.gov.br

ANEXO I - DO ACORDO DE NÍVEIS DE SERVIÇOS – SLA

1. A gestão e fiscalização do contrato se darão mediante o estabelecimento e acompanhamento de indicadores de desempenho, disponibilidade e qualidade, que comporão o Acordo de Nível de Serviço (SLA) entre a Contratante e Contratada.
2. Será de responsabilidade da CONTRATADA o atendimento de 1º nível.
3. A manutenção corretiva consistirá no conserto de defeitos e/ou falhas de funcionamento apresentados nos sistemas deverão ser realizados em 2º e 3º nível, de maneira remota, de segunda a sexta-feira, exceto feriados, no horário de 8:00 às 18:00 horas.
   3.1. Os chamados de 2º e 3º níveis fora destes períodos (emergenciais) deverão ser atendidos pelo serviço de plantão, independentemente de ser sábado, domingo ou feriado. Os chamados de plantão incorrem em uma remuneração adicional medida em Unidades de Suporte Técnico (UST).
4. Os incidentes, situações inesperadas e não programadas, deverão ser atendidas pelos serviços de suporte da CONTRATADA. Os incidentes têm a seguinte classificação:
   Severidade 1 ou Alta: Ambiente/Sistema está indisponível ou usuário sem acesso;
   Severidade 2 ou Média: Uma função do Ambiente/Sistema está indisponível;
   Severidade 3 ou Baixa: O Ambiente/Sistema está disponível, porém apresentando lentidão, erros que forçam o reinício do sistema e/ou de operações no mesmo, e/ou alguma intermitência em seu funcionamento.

   4.1. A CONTRATADA deverá prestar, durante a vigência deste contrato, serviços de suporte a produção e manutenção corretiva abrangendo no mínimo:
   4.2. Investigação e resolução de problemas no ambiente, mesmo que para isso seja necessário acionar o suporte do fabricante;
   4.3. Nível de serviço (SLA), para chamados abertos entre o horário compreendido entre as 08 horas e 18 horas em dias úteis, conforme tabela a seguir:

Severidade	Descrição	Prazo máximo para início do atendimento remoto	Prazo máximo para a solução remota	Prazo máximo para início do Atendimento Presencial	Prazo máximo de Solução
1 - Crítica	Situação emergencial ou problema crítico que cause a indisponibilidade de sistema.	Até 2 horas	Até 8 horas	Até 12 horas após abertura do chamado remoto	Até 24 horas após abertura do chamado remoto

2 - Alta	Impacto de alta significância relacionado à utilização da solução: ocorrência de indisponibilidade de funcionalidade.	Até 4 horas	Até 16 horas	Até 48 horas após abertura do chamado remoto	Até 72 horas após abertura do chamado remoto
3 - Média	Impacto de baixa Significância relacionado à utilização da solução. Não há ocorrência de indisponibilidade de funcionalidade, sendo contornável por solução paliativa sem grandes esforços ou retrabalho.	Até 6 horas	Até 24 horas	Até 72 horas após abertura do chamado remoto	Até 96 horas após abertura do chamado remoto

4.4. Caso seja necessário o complemento de informações para atendimento do chamado, que impossibilitem a resolução do chamado pela CONTRATADA, a CONTRATANTE será solicitada para fornecer a informação, e os prazos serão suspensos ou prorrogados até o recebimento das informações.

4.5. O tempo em horas, previsto no SLA, será computado a partir da abertura do chamado até a sua regularização, nesse caso, uma solução de contorno poderá ser utilizada, caso a solução definitiva não seja possível de ser executada imediatamente.

4.6. A CONTRATADA deverá atender no mínimo 90% (noventa por cento) dos chamados dentro do SLA estabelecido na tabela.

Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP:60.130-240 - Fortaleza/CE
Fone: (85) 3108-0000
www.etice.ce.gov.br

ANEXO J – MODELO DE PROPOSTA

- Tabela 1 – Serviços de Conectividade com Gerência em Nuvem com SERVIÇOS de Disponibilização de solução de conectividade, Software, Instalação, Configurações e Testes.

ITEM	DESCRITIVO	UND	QTD (a)	Valor Unitário Mensal (b)	Valor Anual (c=a x b x12)	Serviços de Disponibilização (Valor Único Unitário) (d)	Serviços de Disponibilização (Valor Único Total) (e=a x d)	Valor Global (f=c + e)
1	SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 1	SERV	200					
2	SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 2	SERV	50					
3	SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 3	SERV	30					
4	SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 4	SERV	20					
5	SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 5	SERV	12					

Empresa de Tecnologia da Informação do Ceará - Etice
Av. Pontes Vieira 220 - São João do Tauape
CEP:60.130-240 - Fortaleza/CE
Fone: (85) 3108-0000
www.etice.ce.gov.br

6	SERVIÇO DE CONECTIVIDADE SEGURA COM GERÊNCIA EM NUVEM - TIPO 6	SERV	10					
7	SERVIÇO DE ACESSO SEGURO DE DISPOSITIVOS A REDE COM GERENCIA EM NUVEM	SERV	10000					
8	SERVIÇO DE VISIBILIDADE DE SEGURANÇA PARA REDE EM NUVEM	SERV	10000					
9	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - TIPO 1	SERV	50					

10	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - TIPO 2	SERV	200					
11	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM -TIPO 3	SERV	200					
12	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - TIPO 4	SERV	200					
13	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - PONTO DE ACESSO DE REDE SEM FIO WIFI INTERNO - TIPO 1	SERV	5000					
14	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - PONTO DE ACESSO DE REDE SEM FIO WIFI INTERNO - TIPO 2	SERV	2000					
15	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - PONTO DE ACESSO DE REDE SEM FIO WIFI INTERNO - TIPO 3	SERV	1000					
16	SERVIÇO DE CONECTIVIDADE COM GERÊNCIA EM NUVEM - PONTO DE ACESSO DE REDE	SERV	1000					

	SEM FIO WIFI EXTERNO - TIPO 4							
17	INJETOR POE 802.3	INJETOR POE	1000					
18	SOLUÇÃO DE POLÍTICA E AUTENTICAÇÃO DE USUÁRIOS DE REDE SEM FIO	SERV	50					
19	SOLUÇÃO DE POLÍTICA E AUTENTICAÇÃO DE USUÁRIOS DE REDE SEM FIO COM VERIFICAÇÃO DE POSTURA DE DISPOSITIVO	SERV	10					
20	SERVIÇO DE INSTALAÇÃO FÍSICA ATÉ 50 METROS	SERV	4000					
21	SERVIÇO DE INSTALAÇÃO FÍSICA ATÉ 100 METROS	SERV	2000					
22	SERVIÇO DE SITE SURVEY	SERV	300					
Soma (g)								**R$**

(t1) Valor Total em R$ (igual a “g”)

_____

- Tabela 2 – SERVIÇOS DE GERENCIAMENTO, ORQUESTRAÇÃO DA NUVEM, SUSTENTAÇÃO EMERGENCIAL, ADMINISTRAÇÃO DOS PROJETOS.

ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QTD (a)	VALOR UNIT (b)	VALOR ANUAL (c = a x b)
23	SERVIÇOS DE GERENCIAMENTO, ORQUESTRAÇÃO DA NUVEM, SUSTENTAÇÃO	UST	30000		

	EMERGENCIAL, ADMINISTRAÇÃO DOS PROJETOS.				
TOTAL (d)					**R$**

(t2) Valor Total em R$ (igual a “d”)

Valor Total da Proposta (t1+t2)