

ESTUDO TÉCNICO PRELIMINAR

Processo nº 9079618110000798.000048/2025-57

**ESTUDOS PRELIMINARES**

O presente documento visa analisar a viabilidade da presente contratação, bem como levantar os elementos essenciais que servirão para compor o Termo de Referência ou projeto Básico, de forma a melhor atender às necessidades da Administração.

**Dados do Processo:**

<b>Órgão Responsável pela Contratação:</b>	Conselho Regional de Contabilidade do Espírito Santo.
<b>Objeto:</b>	Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente, tudo em conformidade com as condições e exigências estabelecidas neste instrumento.
<b>Nº do Processo Administrativo:</b>	9079618110000798.000048/2025-57

**1. Justificativa para a Contratação Conjunta de Serviços de Tecnologia da Informação:**

**1.1. Introdução**

O presente estudo tem como objetivo fundamental apresentar a justificativa técnica e legal para a contratação conjunta de diversos serviços de Tecnologia da Informação (TI) pelo Conselho Regional de Contabilidade do Espírito Santo (CRCES). A decisão por uma contratação unificada, em detrimento da fragmentação em múltiplos contratos, fundamenta-se em princípios basilares da administração pública, notadamente a economicidade, a eficiência, a segurança jurídica e a busca pela solução mais vantajosa para a Administração, em consonância com as diretrizes estabelecidas pela Lei nº 14.133/21.

A infraestrutura de TI do CRCES, conforme detalhado ao longo deste documento, é um pilar essencial para a continuidade e a qualidade dos serviços prestados à sociedade e à classe contábil. A complexidade e a interdependência dos serviços de Wi-Fi corporativo, backup, suporte técnico e firewall demandam uma abordagem integrada para garantir a robustez, a segurança e a disponibilidade dos sistemas críticos. A contratação isolada de cada um desses componentes não apenas eleva os riscos operacionais, mas também compromete a gestão eficiente e a otimização dos recursos públicos.

Este texto abordará os aspectos técnicos e jurídicos que sustentam a opção pela contratação conjunta, destacando os benefícios em termos de economicidade, a mitigação de problemas inerentes à multiplicidade de prestadores de serviços e a conformidade com a legislação vigente, em especial a Lei nº 14.133/2021 e as melhores práticas de contratação de soluções de TI para a Administração Pública.

**1.2. Da Necessidade da Contratação e a Interdependência dos Serviços de TI**

O Conselho Regional de Contabilidade do Espírito Santo (CRCES) reconhece a Tecnologia da Informação como um elemento estratégico e indispensável para o cumprimento de sua missão institucional. A atual infraestrutura de TI, embora funcional, enfrenta desafios significativos que justificam a presente contratação. Conforme o documento de Estudos Preliminares, o CRCES dispõe de apenas um funcionário técnico especializado em TI, o que resulta em sobrecarga de trabalho e na impossibilidade de atender a todas as demandas operacionais e administrativas complexas, como a manutenção de servidores, gestão de incidentes, monitoramento contínuo de redes, implementação de políticas de segurança da informação e suporte técnico especializado. Adicionalmente, a rede cabeada existente apresenta falhas que impactam diretamente a conectividade e a produtividade da instituição.

A contratação em questão visa suprir essas lacunas e fortalecer a infraestrutura de TI do CRCES, abrangendo os seguintes serviços essenciais e interdependentes:

•**Solução de Acesso via Wi-Fi:** Fundamental para garantir conectividade de alta qualidade e superar as limitações da rede cabeada atual,

promovendo a mobilidade e a eficiência no ambiente de trabalho.

•**Firewall de Próxima Geração:** Crucial para fortalecer a segurança da rede, proteger os dados do CRCES contra ameaças cibernéticas e garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD).

•**Serviços Continuados de Suporte (N1, N2 e N3):** Essenciais para a manutenção da infraestrutura tecnológica, garantia do funcionamento adequado dos sistemas críticos, gestão de incidentes e mudanças, e monitoramento contínuo da infraestrutura.

•**Backup Corporativo (Local e em Nuvem):** Indispensável para assegurar a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, garantindo a continuidade dos negócios e a conformidade com a LGPD.

A natureza desses serviços é intrinsecamente interligada. A eficácia de um sistema de backup, por exemplo, depende diretamente da segurança da rede (Firewall) e da capacidade de suporte técnico para gerenciar eventuais falhas. Da mesma forma, a qualidade da conectividade Wi-Fi impacta a performance de todas as aplicações e serviços que trafegam pela rede. A contratação fragmentada desses serviços, com diferentes prestadores, geraria uma série de desafios e riscos que serão detalhados nas seções seguintes, comprometendo a eficiência e a segurança da infraestrutura de TI do CRCES.

### 1.3. Arcabouço Legal: A Lei nº 14.133/2021 e os Princípios da Contratação Pública

A Nova Lei de Licitações e Contratos Administrativos, Lei nº 14.133, de 1º de abril de 2021, trouxe inovações significativas para o processo de contratação pública no Brasil, com o objetivo de modernizar, otimizar e tornar mais eficientes as aquisições e contratações realizadas pela Administração Pública. Em seu Art. 5º, a Lei elenca uma série de princípios que devem nortear a aplicação da norma, dentre os quais se destacam a economicidade, a eficiência, o interesse público, o planejamento, a transparência, a segurança jurídica e a vantajosidade. Estes princípios são pilares para a justificativa da contratação conjunta dos serviços de TI.

A Lei nº 14.133/2021, ao contrário da legislação anterior, enfatiza a busca pela solução mais vantajosa para a Administração, que não se restringe apenas ao menor preço, mas considera a relação custo-benefício, a qualidade, a inovação e a sustentabilidade. A contratação conjunta de serviços de TI, quando devidamente justificada, alinha-se perfeitamente a essa premissa, pois permite uma visão sistêmica e integrada da infraestrutura, otimizando recursos e minimizando riscos.

Embora a Lei nº 14.133/2021 defina a 'contratação integrada' especificamente para obras e serviços de engenharia (Art. 6º, XXXII), o conceito subjacente de agrupar itens interdependentes para obter maior eficiência e vantajosidade pode ser analogicamente aplicado à contratação de serviços de TI. A Instrução Normativa SGD/ME Nº 94, de 23 de dezembro de 2022, que disciplina as contratações de soluções de Tecnologia da Informação e Comunicação (TIC) pelos órgãos e entidades do SISP, reforça a importância do planejamento e da busca por soluções que atendam às necessidades de forma abrangente e eficiente.

O Estudo Técnico Preliminar (ETP), conforme previsto na Lei nº 14.133/2021 e detalhado na IN SGD/ME Nº 94/2022, é o documento fundamental que embasa a decisão pela contratação. Ele deve contemplar a análise comparativa de soluções e custos, a estimativa do custo total da

contratação e a declaração da viabilidade da contratação. A presente justificativa, ao demonstrar os benefícios da contratação conjunta, serve como subsídio para o ETP, evidenciando que a opção por um único prestador para os serviços de Wi-Fi, backup, suporte e firewall é a que melhor atende aos princípios da Lei e às necessidades do CRCES.

Outro ponto relevante é a Matriz de Alocação de Riscos, que se torna ainda mais crucial em contratações complexas como a de serviços de TI. A Lei nº 14.133/2021 exige a definição clara de riscos e responsabilidades entre as partes. Em uma contratação conjunta, a alocação de riscos é simplificada, pois a responsabilidade pela integração e funcionamento dos diversos componentes recai sobre um único fornecedor, facilitando a gestão e a resolução de eventuais problemas.

### 1.4. Economicidade e Vantagens da Contratação Conjunta

A busca pela economicidade é um dos princípios fundamentais que regem as contratações públicas, conforme expresso no Art. 5º da Lei nº 14.133/2021. A contratação conjunta dos serviços de TI, em vez de licitações separadas para cada item (Wi-Fi, backup, suporte e firewall), representa uma estratégia que maximiza a eficiência na aplicação dos recursos públicos e gera uma série de vantagens econômicas e operacionais para o CRCES.

Primeiramente, a contratação de um único fornecedor para a gestão integrada de múltiplos serviços de TI permite a obtenção de economias de escala. Ao consolidar a demanda, o CRCES ganha maior poder de negociação, o que pode resultar em propostas mais competitivas e preços unitários mais vantajosos para cada serviço. A diluição de custos administrativos e operacionais do fornecedor em um contrato de maior escopo tende a refletir em um custo total da contratação mais baixo para a Administração Pública.

Além disso, a contratação conjunta simplifica os processos administrativos e burocráticos. A gestão de um único contrato, em comparação com a gestão de múltiplos contratos, reduz significativamente a carga de trabalho da equipe interna do CRCES, liberando recursos humanos para outras atividades estratégicas. Isso se traduz em economia de tempo e, consequentemente, de recursos financeiros, uma vez que menos horas de trabalho são dedicadas à fiscalização e acompanhamento de diversos contratos.

A otimização dos recursos também se manifesta na redução de custos indiretos. A coordenação entre diferentes fornecedores, a resolução de conflitos de responsabilidade e a necessidade de interface entre sistemas distintos geram custos ocultos e ineficiências. Com um único prestador, esses custos são minimizados, pois a responsabilidade pela integração e pelo funcionamento harmonioso de toda a infraestrutura de TI recai sobre uma única empresa, que possui o conhecimento global do ambiente e a capacidade de gerenciar as interdependências de forma proativa.

Por fim, a contratação conjunta contribui para a previsibilidade orçamentária. Com um contrato abrangente, o CRCES tem uma visão mais clara e consolidada dos custos totais envolvidos na manutenção e gestão de sua infraestrutura de TI, facilitando o planejamento financeiro e a alocação de recursos de forma mais eficiente ao longo do tempo. Essa previsibilidade é essencial para uma gestão pública responsável e transparente.

### 1.5. Mitigação de Problemas e Impactos Negativos da Multiplicidade de Prestadores

A contratação fragmentada de serviços de Tecnologia da Informação, com a pulverização de responsabilidades entre múltiplos prestadores, embora possa parecer, à primeira vista, uma estratégia de diversificação, acarreta uma série de problemas e impactos negativos que comprometem a eficiência, a segurança e a continuidade das operações do CRCES. A experiência demonstra que a gestão de diversos contratos para serviços interdependentes de TI pode gerar complexidades e vulnerabilidades que superam quaisquer supostas vantagens.

Um dos principais desafios reside na incompatibilidade e nas falhas de integração entre os diferentes sistemas e equipamentos fornecidos por empresas distintas. A infraestrutura de TI do CRCES, conforme descrito, é híbrida e complexa, envolvendo soluções de Wi-Fi, backup, suporte e firewall, além de infraestrutura hiperconvergente, acessos VDI, máquinas virtuais e desktops físicos. A falta de um gerenciamento unificado pode levar a problemas de interoperabilidade, dificultando a comunicação entre os componentes e resultando em falhas operacionais, interrupções de serviço e degradação da performance geral do ambiente. A identificação da causa raiz de um problema torna-se um processo moroso e dispendioso, pois cada fornecedor pode atribuir a falha ao outro, criando um cenário de “empurra-empurra” de responsabilidades.

A dificuldade na gestão e fiscalização contratual é outro impacto negativo significativo. A multiplicidade de contratos implica na necessidade de gerenciar diferentes prazos, escopos, níveis de serviço (SLAs) e pontos de contato. Isso sobrecarrega a equipe interna do CRCES, que já é reduzida, desviando seu foco de atividades estratégicas para a burocracia administrativa. A fiscalização torna-se mais complexa, exigindo um esforço desproporcional para garantir que cada fornecedor esteja cumprindo suas obrigações de forma isolada, sem uma visão integrada do impacto no ambiente como um todo.

A diluição da responsabilidade é um risco inerente à contratação fragmentada. Em caso de incidentes de segurança, falhas de sistema ou perda de dados, a apuração do responsável pela falha e a consequente aplicação de sanções contratuais tornam-se extremamente difíceis. Essa incerteza jurídica pode atrasar a resolução de problemas críticos, gerar prejuízos financeiros e de imagem para o CRCES, e comprometer a conformidade com regulamentações como a LGPD. Com um único prestador, a responsabilidade pela integridade e funcionamento de toda a infraestrutura é centralizada, facilitando a governança e a responsabilização.

Adicionalmente, a fragmentação pode levar a custos elevados e ineficiências operacionais. A ausência de uma visão consolidada da infraestrutura impede a otimização de recursos e a identificação de redundâncias ou gargalos. Cada fornecedor pode operar de forma isolada, sem considerar o impacto de suas ações no ambiente geral, o que pode resultar em investimentos desnecessários ou na subutilização de ativos. A falta de padronização e a necessidade de múltiplas interfaces de comunicação entre os fornecedores também contribuem para o aumento dos custos operacionais.

Por fim, a vulnerabilidade de segurança é amplificada em um ambiente com múltiplos prestadores. A gestão de segurança da informação exige uma abordagem holística e integrada. A fragmentação pode criar brechas e pontos cegos, dificultando a implementação de políticas de segurança consistentes e a resposta rápida a ameaças cibernéticas. Um único fornecedor, com uma visão abrangente da infraestrutura, está em melhor posição para implementar e gerenciar soluções de segurança de forma eficaz, garantindo a proteção dos dados e sistemas do CRCES.

Diante desses riscos e impactos negativos, a contratação conjunta de serviços de TI emerge como a solução mais prudente e vantajosa para o CRCES, garantindo a sinergia entre os serviços, a otimização da gestão, a clareza na alocação de responsabilidades e a segurança da infraestrutura tecnológica.

#### 1.6. Conclusão

Diante do exposto, a contratação conjunta dos serviços de Tecnologia da Informação para o Conselho Regional de Contabilidade do Espírito Santo (CRCES), abrangendo Wi-Fi corporativo, backup, serviços de suporte e firewall, configura-se como a abordagem mais estratégica, eficiente e em conformidade com os preceitos da Lei nº 14.133/2021. Esta modalidade de contratação não apenas otimiza a aplicação dos recursos públicos, mas também mitiga os riscos inerentes à fragmentação de serviços interdependentes, garantindo a continuidade, a segurança e a qualidade da infraestrutura de TI do órgão.

A centralização da responsabilidade em um único prestador de serviços especializados em TI proporciona uma gestão mais simplificada e eficaz, com clareza na alocação de responsabilidades e maior agilidade na resolução de problemas. A economicidade é alcançada por meio de ganhos de escala, redução de custos administrativos e operacionais, e maior previsibilidade orçamentária. Adicionalmente, a abordagem integrada fortalece a segurança da informação, minimizando vulnerabilidades e garantindo a conformidade com a legislação vigente, como a LGPD.

Em suma, a contratação conjunta é a solução que melhor atende ao interesse público, promovendo a eficiência, a economicidade e a segurança jurídica, pilares da boa gestão pública. Recomenda-se, portanto, a continuidade do processo licitatório sob esta perspectiva integrada, visando a obtenção da proposta mais vantajosa e a garantia de uma infraestrutura de TI robusta e confiável para o CRCES.

## 2. Diretrizes gerais para a contratação:

### 2.1 - DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO, CONSIDERADO O PROBLEMA A SER RESOLVIDO SOB A PERSPECTIVA DO INT PÙBLICO;

O **Conselho Regional de Contabilidade do Espírito Santo (CRCES)** desempenha um papel essencial na sociedade, oferecendo serviços como fiscalização e registro do exercício profissional, orientação técnica e promoção de desenvolvimento profissional da classe contábil. A execução eficiente dessas atividades depende diretamente de uma **infraestrutura de Tecnologia da Informação (TI)** robusta, segura e eficaz, capaz de atender às crescentes demandas internas e externas e garantir a proteção de dados sensíveis, em conformidade com a **Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018)**.

Atualmente, o CRCES conta com apenas **um servidor técnico especializado em TI**, o qual se encontra sobrecarregado com demandas operacionais, administrativas e técnicas. Essa limitação compromete a execução de atividades críticas e complexas, como:

- Manutenção de servidores e redes;
- Monitoramento contínuo da infraestrutura;
- Gestão de incidentes e mudanças;
- Suporte técnico especializado;
- Implementação de políticas de segurança da informação.

Além disso, a **infraestrutura de rede cabeada apresenta falhas recorrentes**, impactando diretamente a conectividade e a produtividade das equipes. A segurança da informação também requer reforços, com a **adoção de soluções modernas e eficazes contra ameaças cibernéticas**.

Atualmente, o CRCES mantém o **Contrato Administrativo nº 40/2024**, firmado com a empresa Smart Fusion Technology Ltda, com vigência até 15/12/2025. Contudo, trata-se de contrato emergencial, **sem possibilidade de prorrogação**, o que torna **necessária a realização de novo procedimento licitatório**, a fim de garantir a contratação regular e contínua dos serviços especializados de gerenciamento de TI.

A nova contratação tem como objetivo **assegurar a continuidade, eficiência e segurança das operações tecnológicas do CRCES**, por meio da prestação dos seguintes serviços especializados:

- Suporte técnico avançado para a infraestrutura tecnológica;
- Manutenção preventiva e corretiva de servidores e redes;
- Gestão de incidentes e implementação de melhorias;
- Monitoramento proativo da infraestrutura de TI;

- Fornecimento, instalação e gestão de **rede Wi-Fi corporativa**;
- Implantação e gestão de **Firewall de Próxima Geração**;
- Implementação e gerenciamento de **solução de backup híbrida** (local e em nuvem), conforme exigências da LGPD.

Além disso, a contratação visa **reduzir a sobrecarga do único servidor de TI**, promovendo maior eficiência e qualidade dos serviços prestados pelo Conselho à sociedade e à classe contábil.

#### Natureza do Objeto – Serviço Comum e Continuado

O objeto desta contratação caracteriza-se como **serviço comum**, nos termos do inciso II do art. 6º da **Lei nº 14.133/2021**, por poder ser descrito de forma objetiva e padronizada, sem necessidade de especificações técnicas complexas ou qualificações exclusivas. São serviços amplamente ofertados no mercado, com condições técnicas e comerciais similares entre fornecedores.

Trata-se, ainda, de **serviço de natureza continuada**, tendo em vista a sua **necessidade permanente e ininterrupta**, indispensável à execução das atividades finalísticas do CRCES. A descontinuidade desses serviços comprometeria a segurança da informação, a funcionalidade dos sistemas internos e a continuidade do atendimento ao público.

Diante do exposto, justifica-se a abertura de procedimento licitatório para a **contratação regular de serviços comuns e continuados de gerenciamento de TI**, garantindo:

- A continuidade das atividades institucionais do CRCES;
- A observância aos princípios da legalidade, eficiência e economicidade;
- A proteção de dados sensíveis, conforme previsto na LGPD;
- A segurança, estabilidade e evolução da infraestrutura tecnológica do Conselho

## 2.2 - PREVISÃO DA CONTRATAÇÃO NO PLANO DE CONTRATAÇÕES ANUAL

A contratação possui previsão no Plano de Contratações Anual do CRCES para o exercício 2026, e no Plano Diretor de Tecnologia da Informação.

## 2.3 - REQUISITOS DA CONTRATAÇÃO

		ITEM 1			
SUBITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01		<b>SOLUÇÃO DE ACESSO VIA WI-FI</b>	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02		<b>FIREWALL (SEDE)</b>	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03		<b>SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3</b>	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	Mês	12
04		<b>BACKUP CORPORATIVO</b>	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

2.3.1 A Contratada deverá prestar **serviços gerenciados de Tecnologia da Informação** que abrangem o **suporte técnico avançado** (remoto e presencial) para a manutenção da infraestrutura tecnológica, garantindo o funcionamento adequado dos sistemas críticos, incluindo a **gestão de incidentes e mudanças**. O escopo prevê a **gestão completa da infraestrutura de redes** (LAN, VLAN e WLAN), com o **fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa**, e a **gestão de todos os ativos de rede, computadores, nobreaks, servidores físicos e virtuais**. Será responsável também pelo **monitoramento contínuo da infraestrutura**, com identificação e mitigação proativa de riscos, pela **manutenção preventiva e corretiva** de todo o parque de TI, pela **gestão e monitoramento dos links de internet**, pela **gestão e manutenção da infraestrutura hiperconvergente** e do **banco de dados em SQL Server**. Além disso, inclui o **fornecimento, instalação e gestão de um Firewall de Próxima Geração** e a **implementação e gestão de solução de backup local e em nuvem**. Os serviços atenderão a única localidade do CRCES, até **60 estações de trabalho** (físicas ou virtuais), **5 servidores físicos** e **12 servidores virtuais**.

2.3.2 A empresa contratada deverá estar plenamente capacitada para **gerenciar toda a estrutura de TI híbrida do CRCES**. Esta estrutura é

complexa e inclui uma **infraestrutura hiperconvergente** (com armazenamento baseado em Software-defined Storage - SDS), uma **infraestrutura com acessos VDI (Virtual Desktop Infrastructure) máquinas virtuais** e uma **infraestrutura tradicional** (com desktops físicos e notebooks). A Contratada será responsável por assegurar a **gestão completa dos backups e restores** de todo esse ambiente, bem como por lidar com qualquer problema, falha, atualização, instalação ou análise inerente a essa integração diversificada de ferramentas, garantindo a **disponibilidade e integridade dos dados** em todas as plataformas.

## 2.4 CARACTERÍSTICAS TÉCNICAS MÍNIMAS OBRIGATÓRIAS

### 2.4.1. SOLUÇÃO DE ACESSO VIA WI-FI.

#### 2.4.1.1. Características da solução.

2.4.1.1.1. Deverá compor a solução equipamentos compatíveis com a planta do órgão;

2.4.1.1.2. Deverá ser fornecido, pela CONTRATADA, todos os equipamentos Wi-Fi necessários para cobertura da sede, totalizando 20 (vinte) unidades, sendo 18 (dezoito) unidades destinadas à instalação nos ambientes da sede, conforme estudo técnico preliminar já realizado e 2 (duas) unidades adicionais a serem mantidas como equipamentos de reserva (spare) e/ou utilizados para cobertura de eventuais zonas de sombra que venham a ser identificadas durante a implantação.

2.4.1.1.3. O posicionamento físico dos Access Points (APs) será de responsabilidade da CONTRATADA, devendo ser definido com base em levantamento técnico de cobertura, densidade de usuários e análise de espectro, assegurando sinal adequado e desempenho compatível com ambientes corporativos.

2.4.1.1.4. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o pleno funcionamento da solução

2.4.1.1.5. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço

2.4.1.1.6. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.

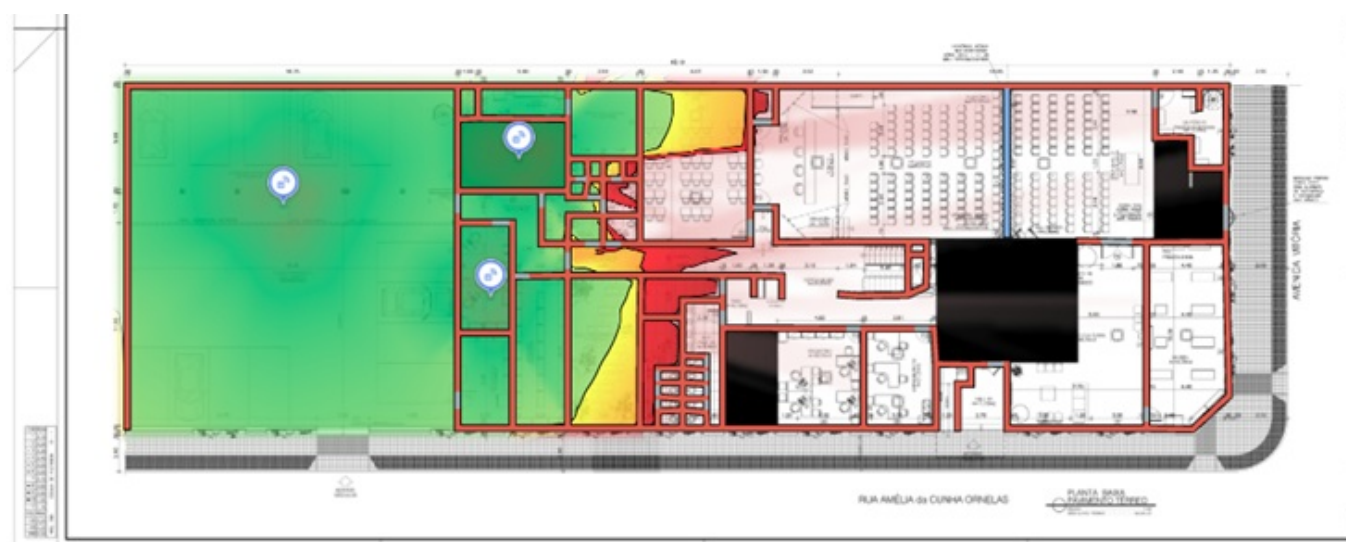
2.4.1.1.7. A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência

#### 2.4.1.1.8. Site Survey Preliminar

Para a definição da quantidade de **equipamentos** necessários, conforme detalhado no item 2.4.1.1.2, o CRCES realizou um **levantamento de campo (site survey)** preliminar, cujos resultados são apresentados a seguir:

a) Pavimento térreo - 09 equipamentos



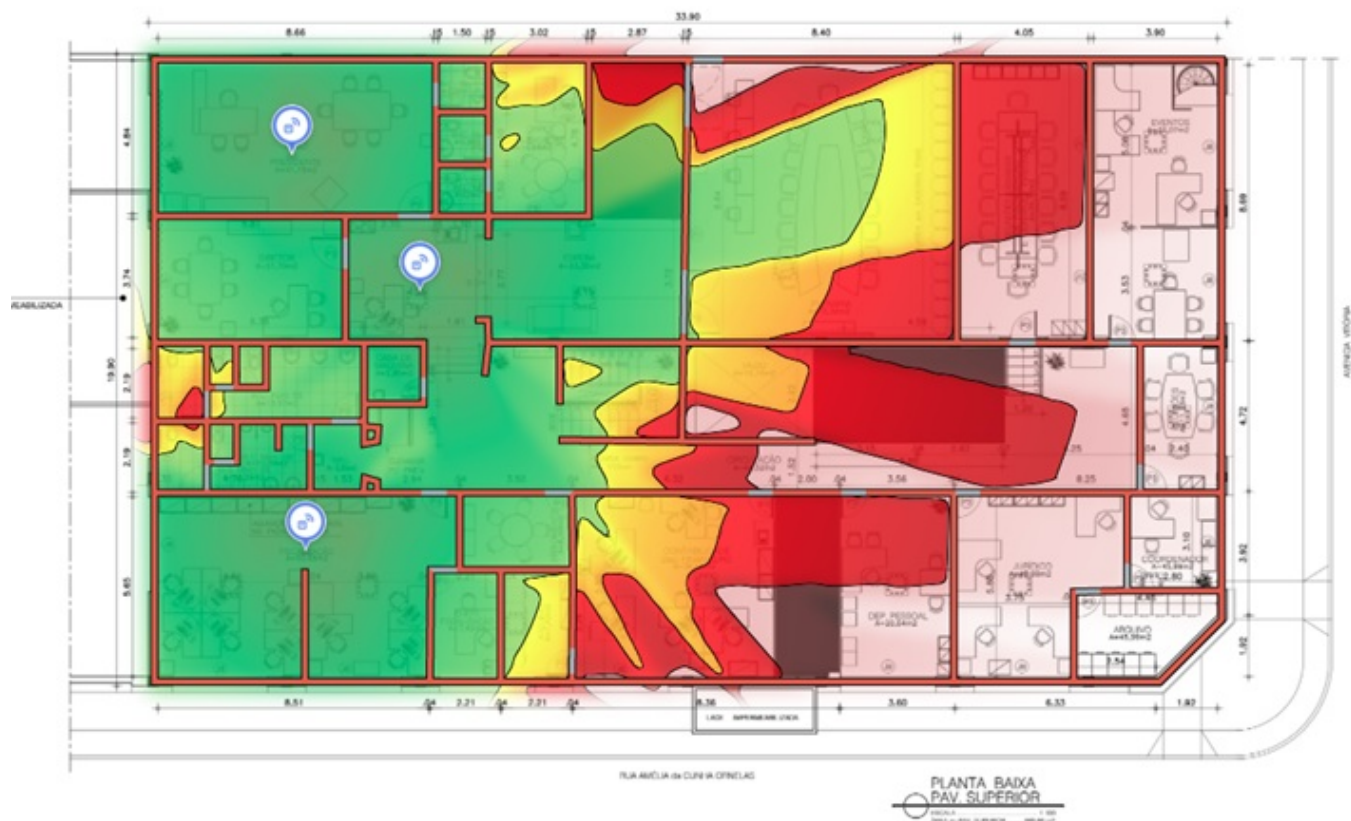


**b) Pavimento superior - 09 equipamentos**









## 2.5 CARACTERÍSTICAS DOS PONTOS DE ACESSO À INTERNET VIA WI-FI.

2.5.1. Características dos pontos de acesso à internet via Wifi. (Equivalente ao seu antigo 1.2)

2.5.1.1. Pontos de acesso (AP) que permita acesso dos dispositivos à rede através da rede sem fio e que possua todas as suas configurações centralizadas em controlador wireless;

2.5.1.2. Deve ser compatível e gerenciado pelo ITENS "Firewall de Próxima Geração (NGFW) – Tipo 0x" deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

2.5.1.3. Deve suportar modo de operação centralizado, ou seja, sua operação depende do controlador wireless que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência;

2.5.1.4. Deve identificar automaticamente o controlador wireless ao qual se conectará;

2.5.1.5. Deve permitir ser gerenciado remotamente através de links WAN;

2.5.1.6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea;

2.5.1.7. Deve possuir capacidade dual-band com rádios 2.4GHz, 5GHz e 6GHz operando simultaneamente, além de permitir configurações independentes para cada rádio;

2.5.1.8. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (WIDS/WIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação;

2.5.1.9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento;

2.5.1.10. Deve permitir a conexão de 512 (quinhentos e doze) clientes wireless simultaneamente;

2.5.1.11. Deve possuir 01 (uma) interface Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

2.5.1.12. Deve possuir 01 (uma) interface Ethernet padrão 10/100/1000/2500 Base-T com conector RJ-45 para permitir a conexão com a rede LAN;

2.5.1.13. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad;

2.5.1.14. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB;

2.5.1.15. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Deve ser fornecido Power



Injector e adicionalmente deve possuir entrada de alimentação 12VDC;

2.5.1.16. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless;

2.5.1.17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

2.5.1.18. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

2.5.1.19. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

2.5.1.20. Deve permitir operação em modo Mesh;

2.5.1.21. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;

2.5.1.22. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;

2.5.1.23. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);

2.5.1.24. Deve suportar OFDMA;

2.5.1.25. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 GHz, 5 GHz e 6GHz servindo clientes wireless 802.11ax;

2.5.1.26. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;

2.5.1.27. Deve suportar BSS Coloring;

2.5.1.28. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;

2.5.1.29. Deve suportar operação em 6GHz com canais de 20, 40, 80 e 160MHz;

2.5.1.30. Deve possuir sensibilidade mínima de -93dBm quando operando em 5GHz com MCS0 (HT20);

2.5.1.31. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz;

2.5.1.32. Deve possuir antenas internas ao equipamento com ganho mínimo de 5dBi em 5GHz e 6GHz;

2.5.1.33. Em conjunto com o controlador wireless, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados;

2.5.1.34. Em conjunto com o controlador wireless, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz;

2.5.1.35. Em conjunto com o controlador wireless, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz;

2.5.1.36. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;

2.5.1.37. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS);

2.5.1.38. Em conjunto com o controlador wireless, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea;

2.5.1.39. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);

2.5.1.40. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;

2.5.1.41. Em conjunto com o controlador wireless, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

2.5.1.42. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

2.5.1.43. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;

2.5.1.44. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

2.5.1.45. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

2.5.1.46. Deve implementar o padrão IEEE 802.11e;

2.5.1.47. Deve implementar o padrão IEEE 802.11h;

2.5.1.48. Deve implementar o padrão IEEE 802.3az;

2.5.1.49. Deve suportar ser gerenciado via SNMP;

2.5.1.50. Deve suportar consultas via REST API;

2.5.1.51. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;

2.5.1.52. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45° C;

2.5.1.53. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;

2.5.1.54. Deve possuir indicadores luminosos (LED) para indicação de status;

2.5.1.55. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;

2.5.1.56. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;

2.5.1.57. Deve possuir certificado emitido pela Wi-Fi Alliance;

2.5.1.58. Deve estar homologado pela ANATEL na data de execução do pregão;

2.5.1.59. Deve ser licenciado para uso pelo período de duração da contratação.

2.5.1.60. Deve possuir garantia para uso pelo período de duração da contratação.

2.5.1.61. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço.

## **2.6. CARACTERÍSTICAS DO EQUIPAMENTO CONTROLADOR DE PONTOS DE ACESSO WIFI**

2.6.1. Características do equipamento controlador de pontos de acesso Wifi (Equivalente ao seu antigo 1.3)

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

2.6.1.2. Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X);

2.6.1.3. Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior;

2.6.1.4. Deverá implementar os padrões IEEE 802.3af (PoE) e IEEE 802.3at (PoE+) com PoE budget de 370W em 24 portas;

2.6.1.5. Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos;

2.6.1.6. Deve possuir 1 (uma) interface USB;

2.6.1.7. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 190 Mpps (milhões de pacotes por segundo);

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

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

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

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

2.6.1.12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (LACP);

2.6.1.13. Deve suportar a comutação de Jumbo Frames;

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

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

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

2.6.1.17. Deve implementar serviço de DHCP Relay;

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

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

2.6.1.20. Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (RSTP) e IEEE 802.1s (MST). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree;

2.6.1.21. Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física;

2.6.1.22. Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra-ataques do tipo "Denial of Service" no ambiente nível 2;

2.6.1.23. Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente;

2.6.1.24. Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado;

2.6.1.25. Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos;

2.6.1.26. Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit;

2.6.1.27. Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID;

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

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

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

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

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

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

2.6.1.34. Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS;

2.6.1.35. Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta;

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

2.6.1.37. Deve suportar MAC Authentication Bypass (MAB);

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

2.6.1.39. Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede;

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

2.6.1.41. Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface;

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

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

2.6.1.44. Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema;

2.6.1.45. Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table);

2.6.1.46. Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface;

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

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

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

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

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

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

- 2.6.1.53. Deve permitir ser gerenciado através de IPv6;
- 2.6.1.54. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- 2.6.1.55. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 2.6.1.56. Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap;
- 2.6.1.57. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 2.6.1.58. Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo;
- 2.6.1.59. Deverá suportar ser configurado e monitorado através de REST API;
- 2.6.1.60. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
- 2.6.1.61. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
- 2.6.1.62. Deve suportar temperatura de operação de até 45º Celsius;
- 2.6.1.63. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
- 2.6.1.64. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
- 2.6.1.65. Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;
- 2.6.1.66. Deve ser licenciado para uso pelo período de duração da contratação.
- 2.6.1.67. Deve possuir garantia para uso pelo período de duração da contratação.
- 2.6.1.68. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço.

## **2.7 REQUISITOS DA INSTALAÇÃO DOS PONTOS DE ACESSO À INTERNET VIA WI-FI.**

- 2.7.1. Requisitos para instalação do item 1.2
- 2.7.2. Serviço de Implementação para rede WLAN
- 2.7.3. A empresa a ser contratada deve realizar mapeamento detalhado no ambiente do CRC, empregando ferramentas de Site Survey, para a definição de posições ideais para o fornecimento do quantitativo de Access Points necessários de forma a atender aos requisitos da solução, visando garantir cobertura total, sendo observada a quantidade mínima estabelecida pela DTIC.
- 2.7.4. Os serviços serão realizados em horário de expediente (07:30 as 16:30) presencialmente nas dependências da CONTRATANTE;
- 2.7.5. Todas as fases de planejamento, instalação e configuração deverão ser realizadas com a presença de técnicos da Contratada, que deverão possuir capacidade técnica necessária à execução do serviço;
- 2.7.6. Requisitos gerais de Implantação
- 2.7.7. A contratada antes da execução deverá obrigatoriamente apresentar um projeto executivo contendo o cronograma detalhado com as atividades adaptadas de acordo com as necessidades do órgão as configurações dos equipamentos da solução devem seguir os requisitos do projeto executivo elaborado.
- 2.7.8. Instalação física
- 2.7.9. Será realizada instalação física conforme a necessidade da contratante.
- 2.7.10. O ponto de acesso wifi deverá ser fixado no teto ou parede.
- 2.7.11. Após a fixação do ponto de acesso wifi, o cabo de rede deverá ser plugado no equipamento para fins de conexão com a rede LAN e energização do dispositivo.

## **2.8 IMPLEMENTAÇÃO LÓGICA**

- 2.8.1. Elaboração do Plano de Implantação da Rede detalhado em conjunto com a equipe de tecnologia da informação do órgão, incluindo os itens de configuração a seguir
- 2.8.2. Aplicar as melhores práticas e configurar para que o equipamento seja gerenciado pela plataforma de gerenciamento unificado.
- 2.8.3. Cadastro das subscrições dos APs na plataforma de gerência;
- 2.8.4. Endereçamento e segmentação das Redes WIRELESS;
- 2.8.5. Qualidade de Serviço (QoS), para fins de aplicação de regras de classificação, priorização e policiamento de acordo com as aplicações a serem utilizadas na rede wireless);
- 2.8.6. Definição de políticas de bloqueio e permissão de acesso;
- 2.8.7. Instalação da versão mais atual de software (firmware) recomendada pelo fabricante;
- 2.8.8. Configuração de Endereços/Interfaces de Gerência:
- 2.8.9. Endereçamento IP, Telnet Seguro (SSH), Web (HTTP/HTTPS),
- 2.8.10. Parâmetros SNMP para monitoração/gerência remota;
- 2.8.11. Configuração de Syslog, quando aplicável;
- 2.8.12. Configuração de redes locais (VLANs);
- 2.8.13. Configuração de redes locais (SSIDs);
- 2.8.14. Configuração de sincronismo de hora NTP ou SNTP;
- 2.8.15. Controle de acesso de usuários a rede através do padrão 802.1x integrado ao Microsoft Active Directory e a plataforma de controle de acesso.
- 2.8.16. Configuração de alarmes e notificações automatizadas via SNMP e/ou SMTP, quando aplicável;
- 2.8.17. Configurar os SSIDs (Locais e Convidados) para as redes conforme planejamento de rede previamente estabelecido;
- 2.8.18. Configurações de grupos de ponto de acesso;
- 2.8.19. Configuração de algoritmo de criptografia a ser utilizado;
- 2.8.20. Configurações de autenticação 802.1x (Active Directory) conforme planejamento de rede previamente estabelecido;
- 2.8.21. Identificar os pontos de acesso por localização conforme survey realizado;
- 2.8.22. Configuração de segurança de rede;
- 2.8.23. Realizar testes de desempenho de RF dos pontos de acesso wireless;
- 2.8.24. Adequar o posicionamento de pontos de acesso da solução instalada;
- 2.8.25. Configuração de alertas ou alarmes críticos, de acordo com definições feitas na fase de planejamento;

2.8.26. Emissão de relatórios de implantação contendo:

- 2.8.27. Mapas de rede,
- 2.8.28. Relação de equipamentos implantados,
- 2.8.29. Configurações feitas nos softwares;
- 2.8.30. Resultado dos testes realizados;

## **2.9 REQUISITOS PARA INSTALAÇÃO DO CONTROLADOR DE PONTOS DE ACESSO WIFI**

2.9.1. Todo o processo de instalação será precedido de um estudo e entendimento de toda a infraestrutura em funcionamento hoje no ambiente englobando sua topologia, todas as configurações em uso (endereçamentos IP, VLANs, rotas, QoS, ACL's, etc),

2.9.2. Para a implementação da solução bem como acompanhamento do projeto proposto, a licitante deverá apresentar profissionais certificados, níveis avançados de conhecimento nas tecnologias ofertadas e necessárias para implantação da solução proposta.

2.9.3. O serviço de instalação, configuração da rede precederá de um cronograma de projeto para implementação das ações abaixo descritas, a ser elaborado de comum acordo.

2.9.4. Todo serviço deverá ser realizado por profissional do fabricante ou certificado por ele para execução dos serviços, para isso deverá ser apresentado junto com a proposta o certificado do profissional que irá executar os serviços de implantação

2.9.5. Planejamento e Projeto para Instalação da Solução

2.9.6. Levantamento e análise da configuração atual da rede;

2.9.7. Elaboração de Projeto de Rede detalhado em conjunto com a equipe de tecnologia da informação, incluindo os itens de configuração a seguir:

2.9.8. Endereçamento e segmentação das Redes LAN e WAN;

2.9.9. Roteamento estativo e dinâmico utilizando protocolos RIPv2 e OSPFv2, se aplicável;

2.9.10. Qualidade de Serviço (QoS): regras de classificação, priorização e policiamento de acordo com as aplicações a serem utilizadas na rede;

2.9.11. Segurança:

2.9.12. Dos ativos: protocolos de comunicação segura, autenticação para acesso e proteção contra ataques;

2.9.13. Da rede: controles a serem implementados para restringir o acesso à rede e reduzir a exposição dos servidores e estações de trabalho;

2.9.14. Instalação da Solução

2.9.15. Instalação dos equipamentos na rede, em local definido pela equipe de tecnologia da informação, fixando-os ao respectivo rack de ativos;

2.9.16. Todo o processo de remoção dos equipamentos legado, migração de serviços para a nova infraestrutura, instalação e configuração dos novos equipamentos é de responsabilidade da empresa contratada, devendo ser realizado por pessoal capacitado, sob a supervisão dos analistas da licitante, que por sua vez deverão fornecer à empresa contratada as informações necessárias para tal;

2.9.17. Instalação da versão mais atual de software (firmware) recomendada pelo fabricante;

2.9.18. Configuração de Endereços/Interfaces de Gerência;

2.9.19. Endereçamento IP;

2.9.20. Telnet, se necessário;

2.9.21. Secure Shell (SSH), se necessário;

2.9.22. Web (HTTP), se necessário;

2.9.23. Restrições (Filtros/ACLs) de Acesso;

2.9.24. Autenticação;

2.9.25. Parâmetros SNMP para monitoração/gerência remota;

2.9.26. Configuração de redes locais (VLANs);

2.9.27. Configuração de sincronismo de hora NTP ou SNTP;

2.9.28. Configuração do protocolo Rapid Spanning Tree (RSTP);

2.9.29. Configuração de BPDU GUARD;

2.9.30. Configuração de Root Spanning Tree;

2.9.31. Interfaces de roteamento IP;

2.9.32. Protocolos de roteamento dinâmico OSPF, conforme Projeto de Rede elaborado;

2.9.33. Implementação de interfaces IP com Virtual Redundancy Router Protocol (VRRP), se aplicável;

2.9.34. Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado;

2.9.35. Otimização da Solução

2.9.36. Aplicar as melhores práticas e configurar para que o equipamento seja gerenciado pela plataforma de gerenciamento unificado.

2.9.37. Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido;

2.9.38. Criação de Vlan, tantas necessárias ao ambiente de acordo com as definições do projeto;

2.9.39. Criação dos Roteamentos de Vlan, tantos necessários de acordo com as definições do projeto

2.9.40. Ativação de recursos para o controle de broadcast storms;

2.9.41. Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado;

2.9.42. Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido;

2.9.43. Controle de acesso a rede através do padrão IEEE 802.1x;

2.9.44. Instalação dos módulos de gerência ofertados, e todos outros componentes necessários para o seu funcionamento;

2.9.45. Configuração de DHCP Snooping;

2.9.46. Configuração de DHCP Relay;

2.9.47. Configuração de interface confiável (trust Interface);

2.9.48. Configuração de alertas ou alarmes críticos, para cada ativo mapeado, de acordo com definições feitas na fase de planejamento.

2.9.49. Configurações dos perfis de acesso à rede baseadas na Política de Segurança;

2.9.50. Criação e ativação de regras de acesso e perfis de acesso à rede;

2.9.51. Configuração de parâmetros de qualidade de serviço (QoS);

2.9.52. Configuração das políticas acesso para a rede dos usuários, integrados com a base LDAP/RADIUS e TACACS existente;

2.9.53. Distribuição, ativação e testes das políticas de acesso nos switches fornecidos;

2.9.54. Criação de filtros e/ou ACLs (Access Control Lists) de acordo com a política;

2.9.55. Ativação e teste das ACLs nos equipamentos fornecidos;

2.9.56. Homologação

2.9.57. Certificação final da solução, mediante testes de comunicação e apresentação de relatórios com os dados gerados.

2.9.58. Documentação em formato PDF contendo os itens a seguir:

2.9.59. As-Built completo do projeto, assinada pelo responsável técnico pela execução e Gerente de Projeto.

2.9.60. Arquivos de configuração dos ativos de rede;

2.9.61. Backup das configurações dos softwares utilizados;

2.9.62. Imagens das versões de software implantadas nos ativos de rede quando de sua entrega;

## **2.10. Requisitos para instalação do cabeamento**

- 2.10.1. Fornecimento e instalação de cabeamento de rede categoria 6 ou superior, certificado para aplicações PoE;
- 2.10.2. Lançamento dos cabos partindo do switch PoE instalado em rack padrão até os pontos de instalação dos APs conforme planta fornecida;
- 2.10.3. Conectorização e crimpagem dos cabos em ambos os extremos;
- 2.10.4. Instalação de caixas de superfície ou embutidas nos pontos de acesso;
- 2.10.5. Fixação dos APs no teto ou parede, de acordo com o projeto de cobertura de sinal;
- 2.10.6. Teste de continuidade e certificação com laudo de todos os pontos instalados;
- 2.10.7. Organização e identificação dos cabos e pontos conforme padrão TIA/EIA-606;
- 2.10.8. Garantia de funcionamento da alimentação elétrica via PoE e comunicação de rede para cada ponto.

## **2.11. Descrição do suporte continuado**

- 2.11.1. A CONTRATADA deverá prestar assistência em horário comercial, das 07:30 às 16:30h na modalidade 8x5;
- 2.11.2. A CONTRATADA deverá providenciar a imediata reposição de equipamentos que estejam indisponíveis, seja por manutenção preventiva, seja por manutenção corretiva, avarias, acidentes ou paralisados por falhas provocadas por falta de suprimento, no prazo máximo de 24 (vinte e quatro) horas;

### **2.11.3. Da Manutenção Preventiva**

A Contratada é a única e exclusiva responsável pela manutenção preventiva dos equipamentos objeto desta contratação; A manutenção deve obedecer às recomendações do fabricante de cada equipamento, porém, sem se limitar a elas e aos serviços abaixo descritos:

- 2.11.4. Providenciar revisão geral de todos os itens previstos de acordo com a recomendação do fabricante;
- 2.11.5. Verificar o estado geral de conservação dos equipamentos e providenciar substituição dos mesmos sempre que for necessário;
- 2.11.6. Efetuar as revisões periódicas, observando as recomendações do fabricante;
- 2.11.7. A Contratada deverá realizar as manutenções preventivas para garantir o pleno funcionamento dos equipamentos e a qualidade dos materiais produzidos.

### **2.11.8. Manutenção Corretiva**

- 2.11.9. A manutenção corretiva deverá ocorrer sempre que a substituição do equipamento for necessária por quebra, assim como quando surgirem falhas;
- 2.11.10. A CONTRATADA deverá iniciar a manutenção corretiva em um prazo máximo de 4 (quatro) horas após a notificação por parte da CONTRATANTE, respeitando os horários definidos pela CONTRATANTE para essa tarefa;
- 2.11.11. A CONTRATADA deverá arcar com todos os custos decorrentes de avarias, exceto os decorrentes do mau uso do equipamento por parte do Contratante; Nesses casos, será de responsabilidade do Contratante arcar com os custos de reparo do equipamento;
- 2.11.12. A CONTRATADA deverá assumir integral e absoluta responsabilidade pelos equipamentos locados, desobrigando a CONTRATANTE de qualquer ônus, encargos, deveres e responsabilidade por defeitos, vícios aparentes ou ocultos, ou funcionamento insatisfatório dos aludidos bens e acidentes.

### **2.11.13. Serviço continuado**

- 2.11.14. CONTRATADA deverá assumir a responsabilidade pelo gerenciamento da WLAN no que tange as seguintes ações:
- 2.11.15. Provisionamento e descoberta de dispositivos;
- 2.11.16. Prestar suporte técnico remoto e presencial;
- 2.11.17. Realizar atualizações de firmware e patches de segurança nos equipamentos;
- 2.11.18. Fazer a gestão de capacidade, espectro e canais da rede wireless;
- 2.11.19. Substituir equipamentos com defeito conforme cláusulas de SLA.
- 2.11.20. Monitorar continuamente a saúde dos dispositivos
- 2.11.21. Monitorar perfil de usuário;
- 2.11.22. Monitorar Autenticação de usuários;
- 2.11.23. Proteção e implementação de WLAN usando os protocolos de segurança descritos no TR;
- 2.11.24. Entregar relatórios mensais com análise de disponibilidade, uso de canais, desempenho e incidentes;
- 2.11.25. Substituir equipamentos com defeito conforme cláusulas de SLA;
- 2.11.26. Corrigir falhas em conectores, cabos, patch panels e pontos RJ45 usados na solução;

## **2.12. ITEM - FIREWALL (SEDE)**

- 2.12.1. Características da solução
  - 2.12.1.1. A solução proposta abrange a contratação de serviços especializados para a implementação e gestão de um firewall de próxima geração (NGFW).
  - 2.12.1.2. O objetivo é assegurar a proteção, o monitoramento e o controle da infraestrutura de TI do CRCES.
  - 2.12.1.3. A solução de firewall de próxima geração (NGFW) será responsável pela proteção da rede, servidores e dados contra acessos não autorizados e ameaças cibernéticas, além de permitir a aplicação de políticas de segurança avançadas. Essa ferramenta oferece funcionalidades como detecção e prevenção de intrusões (IDS/IPS), filtragem de conteúdo, controle de aplicações e gerenciamento centralizado de ameaças. Com isso, o CRCES poderá garantir que todo o tráfego de rede seja devidamente monitorado e que as políticas de segurança sejam aplicadas de forma consistente.
  - 2.12.1.4. Toda a infraestrutura será gerenciada pela empresa contratada, que será responsável pela administração completa da solução, garantindo a atualização contínua das políticas de segurança e monitoramento.
  - 2.12.1.5. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o pleno funcionamento da solução
  - 2.12.1.6. Ressalta-se que todos os equipamentos, produtos, peças ou softwares necessários à contratação devem ser novos, de primeiro uso, não remanufaturados. Ainda, tais itens mencionados integrantes da solução como um todo devem estar em linha de produção, sem previsão de encerramento. No caso de softwares comerciais, é necessário que sejam entregues em sua versão mais atualizada, e estejam cobertos por contratos de suporte à atualização de versão do fabricante durante toda a vigência do respectivo serviço
  - 2.12.1.7. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.
  - 2.12.1.8. A CONTRATADA deverá efetuar visita prévia ao local de instalação para a verificação da tensão elétrica e de toda infraestrutura necessária para viabilizar o funcionamento da solução conforme detalhamentos constantes neste Termo de Referência

### **2.12.2. Requisitos técnicos dos equipamentos que compõe a solução**

- 2.12.2.1. Deve suportar, no mínimo, 1 Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;
- 2.12.2.2. Deve suportar, no mínimo, 1.500.000 (Um milhão e quinhentos mil) de conexões simultâneas;
- 2.12.2.3. Deve suportar, no mínimo, 45.000 (quarenta e cinco mil) novas conexões por segundo;
- 2.12.2.4. Deve Suportar, no mínimo, 65.000 (sessenta e cinco mil) Conexões de throughput IPv4 UDP...



- 2.12.2.4. Deve suportar, no mínimo, 0,5 (seis virgula cinco) Gbps de throughput VPN IPsec;
- 2.12.2.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Gateway-to-Gateway simultâneos;
- 2.12.2.6. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 2500 (dois mil e quinhentos) túneis de VPN IPSEC Client-to-Gateway simultâneos;
- 2.12.2.7. Deve suportar, no mínimo, 1,4 Gbps de throughput de IPS;
- 2.12.2.8. Deve suportar, no mínimo, 1 Gbps de throughput de Inspeção SSL;
- 2.12.2.9. Deve suportar, no mínimo, 900 Mbps de throughput enquanto executa serviços de segurança como IPS, antivírus ou inspeção SSL.
- 2.12.2.10. Deve possuir, pelo menos, 6 (portas) interfaces RJ45 de 1GB;
- 2.12.2.11. Deve possuir, pelo menos, 2 portas de mídia com interfaces SFP de 1GB/ RJ45 1GB;
- 2.12.2.12. Deve possuir, pelo menos, 2 (portas) para gerenciamento de dispositivos do mesmo fabricante do equipamento;
- 2.12.2.13. Deve possuir porta console RJ-45;
- 2.12.2.14. Deve estar licenciado para gerenciar até 96 (Noventa e seis) pontos de acesso sem fio e 24 (Vinte e quatro) switches simultaneamente em um único appliance;
- 2.12.2.15. Deve estar licenciado, sem custo adicional, no mínimo, para 10 (dez) sistemas virtuais lógicos (Contextos) por appliance;
- 2.12.2.16. Deve possuir Fontes redundantes.
- 2.12.2.17. Deve ser possível configurar alta disponibilidade das seguintes formas: Ativo-Ativo, Ativo-Passivo e em Cluster.
- 2.12.2.18. Deve ser licenciado para uso pelo período de duração do contrato.
- 2.12.2.19. Deve possuir garantia para uso pelo período de duração do contrato.
- 2.12.3. Firewalls de próxima geração (NGFW).
- 2.12.3.1. A solução deve consistir em plataforma de proteção e balanceamento inteligente de rede baseada em appliance com funcionalidades de Next Generation Firewall (NGFW), console de gerência e monitoração.
- 2.12.3.2. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- 2.12.3.3. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale;
- 2.12.3.4. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
- 2.12.3.5. As funcionalidades de proteção de rede que compõe a solução de segurança, podem funcionar em múltiplos appliances desde que atendam a todos os requisitos desta especificação;
- 2.12.3.6. Deverá possuir e estar licenciado pelo período de 36 (trinta e seis) meses com as seguintes funcionalidades: Firewall, Traffic Shapping e QoS, Filtro de Conteúdo Web, Antivírus, AntiSpam, Detecção e Prevenção de Intrusos (IPS), VPN IPsec, Controle de Aplicações, Prevenção de Perda de Dados (DLP) e Virtualização.
- 2.12.3.7. Funcionalidades de rede e firewall.**
- 2.12.3.7.1. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
- 2.12.3.7.2. Os dispositivos de proteção de rede devem possuir suporte a Vlans;
- 2.12.3.7.3. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- 2.12.3.7.4. Os dispositivos de proteção de rede devem possuir suporte a DHCP Cliente, Server e Relay;
- 2.12.3.7.5. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- 2.12.3.7.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;
- 2.12.3.7.7. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
- 2.12.3.7.8. Deverá suportar sFlow ou Netflow;
- 2.12.3.7.9. Deve possuir suporte a criação de sistemas virtuais no mesmo appliance e que possam ser administrados por equipes distintas;
- 2.12.3.7.10. Deverá permitir limitar o uso de recursos utilizados por cada sistema virtual;
- 2.12.3.7.11. Deve suportar o protocolo padrão da indústria VXLAN;
- 2.12.3.7.12. Deve implementar o protocolo ECMP;
- 2.12.3.7.13. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
- 2.12.3.7.14. Enviar log para sistemas de monitoração externos;
- 2.12.3.7.15. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
- 2.12.3.7.16. Deve possuir mecanismos de proteção anti-spoofing;
- 2.12.3.7.17. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP4 e OSPFv2);
- 2.12.3.7.18. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);
- 2.12.3.7.19. Suportar OSPF graceful restart;
- 2.12.3.7.20. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
- 2.12.3.7.21. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
- 2.12.3.7.22. Deve suportar Modo Camada - 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
- 2.12.3.7.23. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo;
- 2.12.3.7.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;
- 2.12.3.7.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;
- 2.12.3.7.26. O modo de Alta-Disponibilidade (HA) deve possibilitar monitoração de falha de link;
- 2.12.3.7.27. A solução deve suportar integração nativa com Let's Encrypt, para obtenção de certificados válidos, de forma automática;
- 2.12.3.7.28. A solução deve possuir conectores nativos para integração com nuvens privadas, pelo menos: VMware ESXI, Cisco ACI e Kubernetes;
- 2.12.3.7.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails, notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;
- 2.12.3.7.30. Deverá possuir integração com tokens para autenticação de 02 (dois) fatores;
- 2.12.3.7.31. Deverá suportar controle por zonas de segurança;
- 2.12.3.7.32. Deverá suportar controles de políticas por porta e protocolo;
- 2.12.3.7.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
- 2.12.3.7.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
- 2.12.3.7.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
- 2.12.3.7.36. Controle, inspeção e descryptografia de SSL por política para tráfego de saída (Outbound).

2.12.3.7.36. Controle, inspeção e descryptografia de SSL por política para tráfego de saída (Outbound);  
2.12.3.7.37. Deve descryptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;  
2.12.3.7.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;  
2.12.3.7.39. Suporte a objetos e regras IPV6;  
2.12.3.7.40. Suporte a objetos e regras multicast;  
2.12.3.7.41. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

#### **2.12.3.8. Funcionalidade de controle de aplicações.**

2.12.3.8.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;  
2.12.3.8.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;  
2.12.3.8.3. Reconhecer pelo menos 4.000 (quatro mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;  
2.12.3.8.4. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;  
2.12.3.8.5. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;  
2.12.3.8.6. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;  
2.12.3.8.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;  
2.12.3.8.8. Para tráfego criptografado SSL, deve descryptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;  
2.12.3.8.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;  
2.12.3.8.10. Identificar o uso de táticas evasivas via comunicações criptografadas;  
2.12.3.8.11. Atualizar a base de assinaturas de aplicações automaticamente;  
2.12.3.8.12. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;  
2.12.3.8.13. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;  
2.12.3.8.14. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;  
2.12.3.8.15. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante;  
2.12.3.8.16. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;  
2.12.3.8.17. Deve alertar o usuário quando uma aplicação for bloqueada;  
2.12.3.8.18. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;  
2.12.3.8.19. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;  
2.12.3.8.20. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o YouTube e, ao mesmo tempo, bloquear o streaming em HD;  
2.12.3.8.21. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;  
2.12.3.8.22. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);  
2.12.3.8.23. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: nível de risco da aplicação, tecnologia, fabricante e popularidade;  
2.12.3.8.24. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação;  
2.12.3.8.25. Deve permitir forçar o uso de portas específicas para determinadas aplicações;

#### **2.12.3.9. Funcionalidade de prevenção de intrusão de ameaças.**

2.12.3.9.1. Para proteção do ambiente contra-ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;  
2.12.3.9.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);  
2.12.3.9.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;  
2.12.3.9.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e "quarentenar" IP do atacante por um intervalo de tempo;  
2.12.3.9.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;  
2.12.3.9.6. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;  
2.12.3.9.7. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;  
2.12.3.9.8. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;  
2.12.3.9.9. Deve permitir o bloqueio de vulnerabilidades;  
2.12.3.9.10. Deve permitir o bloqueio de exploits conhecidos;  
2.12.3.9.11. Deve incluir proteção contra-ataques de negação de serviços;  
2.12.3.9.12. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;  
2.12.3.9.13. Detectar e bloquear a origem de portscans;  
2.12.3.9.14. Bloquear ataques efetuados por worms conhecidos;  
2.12.3.9.15. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;  
2.12.3.9.16. Possuir assinaturas para bloqueio de ataques de buffer overflow;  
2.12.3.9.17. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

- 2.12.3.9.18. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
- 2.12.3.9.19. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
- 2.12.3.9.20. Identificar e bloquear comunicação com botnets;
- 2.12.3.9.21. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
- 2.12.3.9.22. Os eventos devem identificar o país de onde partiu a ameaça;
- 2.12.3.9.23. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
- 2.12.3.9.24. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
- 2.12.3.9.25. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.
- 2.12.3.9.26. A solução deve ter capacidade de enviar artefatos suspeitos para serem executados em ambiente controlado na nuvem do fabricante
- 2.12.3.9.27. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS ou controle de aplicação;
- 2.12.3.9.28. Deve permitir que na captura de pacotes por assinaturas de IPS seja definido o número de pacotes a serem capturados ou permitir capturar o pacote que deu origem ao alerta assim como seu contexto, facilitando a análise forense e identificação de falsos positivos;

#### **2.12.3.10. Funcionalidade de filtro de conteúdo web e dns.**

- 2.12.3.10.1. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
- 2.12.3.10.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
- 2.12.3.10.3. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
- 2.12.3.10.4. Deve permitir que os usuários sejam identificados através de consulta em uma base do Active Directory, permitindo que sua autenticação no domínio, não seja solicitada novamente para navegar através da solução;
- 2.12.3.10.5. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
- 2.12.3.10.6. Deve possuir base ou cache de URLs local no appliance ou em nuvem do próprio fabricante, evitando delay de comunicação/validação das URLs;
- 2.12.3.10.7. Possuir pelo menos 70 (setenta) categorias de URLs;
- 2.12.3.10.8. Deve possuir a função de exclusão de URLs do bloqueio;
- 2.12.3.10.9. Permitir a customização de página de bloqueio;
- 2.12.3.10.10. Permitir a restrição de acesso a canais específicos do Youtube, possibilitando configurar uma lista de canais liberado ou uma lista de canais bloqueados;
- 2.12.3.10.11. Deve bloquear o acesso a conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, independentemente de a opção Safe Search estar habilitada no navegador do usuário;
- 2.12.3.10.12. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos e Comando e Controle (C&C) de botnets conhecidas;
- 2.12.3.10.13. Deve possuir filtro de domínio DNS baseado em categorias para inspecionar o tráfego DNS com classificação de domínios continuamente atualizado;

#### **2.12.3.11. Funcionalidade de identificação de usuários.**

- 2.12.3.11.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, eDirectory e base de dados local;
- 2.12.3.11.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 2.12.3.11.3. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2 ou superior;
- 2.12.3.11.4. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;
- 2.12.3.11.5. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 2.12.3.11.6. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 2.12.3.11.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
- 2.12.3.11.8. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
- 2.12.3.11.9. Deve suportar o envio e recebimento de credenciais via RADIUS;
- 2.12.3.11.10. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

#### **2.12.3.12. Funcionalidade de filtro de dados .**

- 2.12.3.12.1. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
- 2.12.3.12.2. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 2.12.3.12.3. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 2.12.3.12.4. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

#### **2.12.3.13. Funcionalidade de geolocalização.**

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

#### **2.12.3.14. Funcionalidade de vpn.**

- 2.12.3.14.1. Suportar VPN Site-to-Site e Cliente-To-Site;
- 2.12.3.14.2. Suportar IPSec VPN;
- 2.12.3.14.3. A VPN IPSEC deve suportar 3DES;
- 2.12.3.14.4. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
- 2.12.3.14.5. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

- 2.12.3.14.6. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- 2.12.3.14.7. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- 2.12.3.14.8. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI
- 2.12.3.14.9. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- 2.12.3.14.10. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPsec IPv6;
- 2.12.3.14.11. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 2.12.3.14.12. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- 2.12.3.14.13. Atribuição de DNS nos clientes remotos de VPN;
- 2.12.3.14.14. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 2.12.3.14.15. Suportar autenticação via AD/LDAP, certificado e base de usuários local;
- 2.12.3.14.16. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 2.12.3.14.17. Deverá manter uma conexão segura com o portal durante a sessão;
- 2.12.3.14.18. O agente de VPN IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bit), Windows 8 (32 e 64 bit), Windows 10 (32 e 64 bit) e Mac OS X (v10.10 ou superior);

#### **2.12.3.15. Funcionalidade de qos, traffic shaping e priorização de tráfego.**

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

#### **2.12.3.16. Funcionalidade de balanceamento inteligente de links.**

- 2.12.3.16.1. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
- 2.12.3.16.2. A solução deve ser capaz de agregar vários links em uma interface virtual;
- 2.12.3.16.3. A solução deve ser possível criar políticas de roteamento inteligente, mediante regras pré-estabelecidas considerando a verificação das seguintes condições: Endereços de origem, Grupos de usuários, Endereços de destino, Serviços na Internet e Aplicações de camada 7 (O365 Exchange, AWS, Dropbox e etc);
- 2.12.3.16.4. A solução deve ser capaz de medir o status de qualidade do link baseando-se em critérios mínimos de latência, jitter e perda de pacotes, onde deve ser possível configurar um valor limite para cada um destes itens que será utilizado como gatilho para fator de decisão nas regras de tráfego de saída e balanceamento inteligente;
- 2.12.3.16.5. A solução deve ser capaz de refletir, de forma manual ou automatizada, suas políticas de balanceamento em condições em que a largura de banda é modificada;
- 2.12.3.16.6. A solução deve ser capaz de monitorar a qualidade e identificar falhas nos links, enviando sinais por meio de cada link para servidores ou aplicações, permitindo utilizar protocolos como Ping, HTTP, TCP ECHO, UDP ECHO, DNS, TCP Connect e TWAMP (Two-way Active Measurement Protocol). Deve suportar ainda um método para mensurar a qualidade do tráfego de voz corporativo baseado em MOS (Mean Opinion Score);
- 2.12.3.16.7. A solução deve possibilitar balanceamento de tráfego entre conexões WAN, de forma em que o algoritmo de balanceamento de carga utilizado possa ser configurado considerando os seguintes parâmetros: Sessões, Volume de tráfego, IP de origem e destino e Transbordo de link (Spillover).
- 2.12.3.16.8. A solução deve possibilitar a criação de regras para seleção das interfaces e suas prioridades que serão utilizadas para encaminhar o tráfego de saída da rede, considerando os seguintes critérios:
- 2.12.3.16.9. Manual: Deve permitir que as interfaces tenham as prioridades atribuídas manualmente.
- 2.12.3.16.10. Melhor Qualidade: Deve permitir que as interfaces recebam uma prioridade com base na qualidade do link no qual a interface está conectada, considerando o monitoramento de um dos seguintes parâmetros com valores customizáveis: latência, jitter, perda de pacotes ou largura de banda;
- 2.12.3.16.11. Menor Custo: Deve permitir que as interfaces recebam uma prioridade com base no custo atribuído a interface, considerando a satisfação dos parâmetros de qualidade do link no qual a interface está conectada;
- 2.12.3.16.12. Balanceamento de Carga: Deve permitir que o tráfego seja distribuído entre todas as interfaces disponíveis com base em algoritmos de balanceamento de carga e satisfação dos parâmetros customizados de qualidade do link no qual a interface está conectada;
- 2.12.3.16.13. A solução de balanceamento inteligente deve suportar marcação de pacotes DSCP nas definições e regras para o tráfego balanceado;
- 2.12.3.16.14. A solução de balanceamento inteligente de links deve suportar Roteamento dinâmico (OSPFv2/v3, BGPv4/BGP4+);
- 2.12.3.16.15. A solução deve realizar o reconhecimento de aplicações, em camada 7, de pelo menos 3.000 (três mil) aplicações, incluindo Aplicações SaaS, em Nuvem e Multimídia (Vimeo, YouTube, Facebook, etc);
- 2.12.3.16.16. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;
- 2.12.3.16.17. A solução deve possibilitar a criação e uso de túneis VPN de forma dinâmica entre unidades remotas, para aplicações sensíveis. Uma vez que as unidades trocam informações entre si, o tráfego deve ser encaminhado diretamente entre as unidades remotas sem passar pela unidade Sede;

2.12.3.16.18. A solução deve permitir a duplicação de pacotes entre dois ou mais links, que atendam os parâmetros de qualidade estabelecidos, objetivando uma melhor experiência de uso de aplicações;

2.12.3.16.19. A solução deve possuir recurso para controlar e corrigir erros (FEC - Forward Error Correction) na transmissão de dados, enviando dados redundantes através de túnel VPN em antecipação à perda de pacotes que pode ocorrer durante o trânsito;

2.12.3.16.20. A solução deve permitir a customização de intervalo de tempo em que é feita a verificação da situação de um link, assim como, permitir definir a quantidade de falhas encontradas no link antes de declará-lo inativo, com objetivo de identificar oscilações nos links, que possam impactar os serviços e a experiência dos usuários;

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

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

2.12.3.16.23. A solução deve prover estatísticas em tempo real a respeito da utilização da largura de banda (upload e download) e nível de qualidade dos links (perda de pacote, jitter e latência);

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

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

2.12.3.16.26. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, três links;

2.12.3.16.27. O appliance físico deve apresentar compatibilidade com modems USB (3G/4G), onde estes sejam capazes de funcionar como circuito ativo em relação à saída principal de Internet, e alternativamente funcionar como circuito Standby, onde apenas seja acionado na eventualidade de falha no link principal;

2.12.3.16.28. Deve ser possível extrair informações de desempenho das verificações de saúde mediante REST API, permitindo assim a consolidação de tais informações em alguma aplicação terceira.

#### **2.12.3.17. Funcionalidade de controlador de rede sem fio.**

2.12.3.17.1. A solução deverá ser capaz de gerenciar os pontos de acesso sem fio deste termo, sendo permitido o atendimento através de composição com outras soluções do mesmo fabricante que possua gerência centralizada, devendo atender aos requisitos descritos abaixo:

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

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

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

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

2.12.3.17.6. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário;

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

2.12.3.17.8. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de \*\*túnel estabelecido entre o ponto de acesso e controlador wireless. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até o controlador wireless. Caso o controlador wireless não seja capaz de operar gerenciando os pontos de acesso e concentrando o tráfego tunelado simultaneamente, então a solução ofertada deve ser composta com elemento adicional para suportar a conexão dos túneis originados dos pontos de acesso;

2.12.3.17.9. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o concentrador através de túnel IPSec;

2.12.3.17.10. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso de Split-Tunneling por SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção;

2.12.3.17.11. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até o controlador wireless;

2.12.3.17.12. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre controladora e ponto de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X;

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

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

2.12.3.17.15. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência;

2.12.3.17.16. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm;

2.12.3.17.17. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso;

2.12.3.17.18. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como \*\*Rogue APs\*\*. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados;

2.12.3.17.19. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN;

2.12.3.17.20. A solução deve detectar os pontos de acesso não autorizados e/ou intrusos através de rádios dedicados para a função de análise ou através de Off-channel/Background scanning. Quando realizada através de Off-channel/Background scanning, a solução deve ser capaz de mensurar a utilização do ponto de acesso para, caso necessário, atrasar a análise e desta forma não prejudicar os clientes conectados;

2.12.3.17.21. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless;

2.12.3.17.22. A solução deve permitir a adição de controlador redundante que deve monitorar a disponibilidade e sincronizar as configurações do controlador principal, além de assumir todas as funções em caso de falha do controlador primário. Desta forma, todos os pontos de acesso devem se associar automaticamente ao controlador redundante que passará a ter função de primário de forma temporária;

2.12.3.17.23. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID



2.12.3.17.23. A solução deve permitir o agrupamento de pontos para que sejam distribuídos múltiplos acessos em um determinado setor, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;

2.12.3.17.24. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado;

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

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

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

2.12.3.17.28. A solução deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming;

2.12.3.17.29. A solução deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos;

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

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

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

2.12.3.17.33. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, Fabricante e sistema operacional do dispositivo, Endereço IP, SSID ao qual está conectado, Ponto de acesso ao qual está conectado, Canal ao qual está conectado, Banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação;

2.12.3.17.34. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering;

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

2.12.3.17.36. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime;

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

2.12.3.17.38. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados;

2.12.3.17.39. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados;

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

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

2.12.3.17.42. A solução deve ser capaz de reconfigurar automaticamente os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências;

2.12.3.17.43. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos;

2.12.3.17.44. A solução deve permitir a configuração de regras de firewall baseadas em identidade, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego;

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

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

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

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

2.12.3.17.49. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada;

2.12.3.17.50. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS;

2.12.3.17.51. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações 802.1X;

2.12.3.17.52. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

2.12.3.17.53. A solução deve implementar recurso para autenticação dos usuários através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede;

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

2.12.3.17.55. A solução deve permitir a customização da página de autenticação, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens;

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

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

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

2.12.3.17.59. A solução deve permitir o cadastramento de contas para usuários visitantes na memória interna. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada;

2.12.3.17.60. A solução deve possuir interface gráfica para administração e gerenciamento das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução;

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

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

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

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

2.12.3.17.65. A solução deve permitir que os usuários sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será

disponibilizado;

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

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

2.12.3.17.68. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no equipamento ao qual os APs estejam fisicamente conectados;

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

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

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

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

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

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

2.12.3.17.75. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD;

2.12.3.17.76. A solução deve apresentar graficamente a topologia lógica da rede, representar os elementos da rede gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles;

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

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

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

2.12.3.17.80. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso, garantindo a gestão e operação simultânea de pontos de acesso com firmwares diferentes;

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

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

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

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

### **2.12.3.18. Funcionalidade de controlador de rede cabeada.**

2.12.3.18.1. Deve operar como ponto central para automação e gerenciamento dos switches deste termo, sendo permitido o atendimento através de composição de solução do mesmo fabricante que possua gerência centralizada para switches, devendo atender aos requisitos descritos abaixo:

2.12.3.18.2. Deve realizar o gerenciamento de inventário de hardware, software e configuração dos Switches;

2.12.3.18.3. Deve possuir interface gráfica para configuração, administração e monitoração dos switches;

2.12.3.18.4. Deve apresentar graficamente a topologia da rede com todos os switches administrados para monitoramento, além de ilustrar graficamente status dos uplinks e dos equipamentos para identificação de eventuais problemas na rede;

2.12.3.18.5. Deve montar a topologia da rede de maneira automática;

2.12.3.18.6. Deve ser capaz de configurar os switches da rede;

2.12.3.18.7. Através da interface gráfica deve ser capaz de configurar as VLANs da rede e distribuí-las automaticamente em todos os switches

gerenciados;

2.12.3.18.8. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;

2.12.3.18.9. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;

2.12.3.18.10. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;

2.12.3.18.11. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;

2.12.3.18.12. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;

2.12.3.18.13. Através da interface gráfica deve ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard;

2.12.3.18.14. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;

2.12.3.18.15. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);

2.12.3.18.16. Deve ser capaz de configurar parâmetros SNMP dos switches;

2.12.3.18.17. A solução deve gerenciar as atualizações de firmware (software) dos switches gerenciados, recomendando versões de software para cada switch, além de permitir a atualização dos switches individualmente;

2.12.3.18.18. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;

2.12.3.18.19. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;

2.12.3.18.20. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;

2.12.3.18.21. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;

2.12.3.18.22. Deve prover indicadores de saúde dos elementos críticos do ambiente;

2.12.3.18.23. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;

2.12.3.18.24. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

### **2.13. Serviço de instalação firewall**

#### **2.13.1. Instalação Estrutura Física**

2.13.1.1. Levantamento de toda estrutura física do ambiente;

2.13.1.2. Levantamento da estrutura Elétrica;

2.13.1.3. Verificação do espaço a ser instalado os equipamentos;

2.13.1.4. Abertura e conferência das caixas dos equipamentos;

2.13.1.5. Instalação do appliance físico;

2.13.1.6. Fixação do equipamento no RACK;

2.13.1.7. Conexão da fonte de alimentação elétrica em régua de tomada;

2.13.1.8. Conexão de cabo UTP utilizando o protocolo TCP/IP para utilização do console de gerenciamento;

2.13.1.9. Conexão das interfaces de rede com os switches;

#### **2.13.2. Configuração do appliance físico:**

2.13.2.1. Parametrização do Licenciamento;

- 2.13.2.2. Parametrização das interfaces de rede;
- 2.13.2.3. Atualização da última versão de Firmware;
- 2.13.2.4. Parametrização das regras de NAT;
- 2.13.2.5. Parametrização do Filtro de Conteúdo (WebFilter);
- 2.13.2.6. Parametrização de Controle de Aplicação;
- 2.13.2.7. Parametrização de VPN (Virtual Private Network);
- 2.13.2.8. Parametrização IDS/IPS;
- 2.13.2.9. Parametrização DNS;
- 2.13.2.10. Parametrização de Gateway Antivírus;
- 2.13.2.11. Parametrização de Objetos de Endereço;
- 2.13.2.12. Parametrização de Grupo de Objetos;
- 2.13.2.13. Parametrização de Load Balancing;
- 2.13.2.14. Parametrização de SSO (Single Sign-on);
- 2.13.2.15. Parametrização de SNMP;
- 2.13.2.16. Parametrização de NTP;
- 2.13.2.17. Parametrização de PortGroups;
- 2.13.2.18. Parametrização de Zones;
- 2.13.2.19. Parametrização de Serviços;
- 2.13.2.20. Parametrização de Rotas;
- 2.13.2.21. Parametrização de DHCP

#### 2.14. Serviços profissionais de suporte técnico na solução de firewall

- 2.14.1. Após a instalação a CONTRATADA deverá manter, monitorar e gerenciar todo o ambiente após a sua instalação na modalidade 8x5;
- 2.14.2. Efetuar toda rotina de backup das configurações semanalmente;
- 2.14.3. Atualizar todos os equipamentos sempre que a versão de software, disponibilizada pelo fabricante, for considerada estável, negociando com a CONTRATANTE janelas de manutenção para efetuar o procedimento;

##### 2.14.4. Realizar as seguintes configurações sempre que solicitadas pela CONTRATANTE:

- 2.14.4.1. Atividades relativas à Solução de Segurança:
- 2.14.4.2. Criação das rotas para links.
- 2.14.4.3. Criação de NAT.
- 2.14.4.4. Liberação de portas.
- 2.14.4.5. Configuração do Filtro de Conteúdo.
- 2.14.4.6. Configuração do Controle de Aplicativos.
- 2.14.4.7. Configuração do Agente para autenticação LDAP.
- 2.14.4.8. Configuração para o Single Sign-On (SSO).
- 2.14.4.9. Configurações dos serviços avançados de segurança (IPS, Antivírus).
- 2.14.4.10. Configuração de VPN client to site.
- 2.14.4.11. Configuração de VPN site to site.
- 2.14.4.12. Criação de regras de Firewall.
- 2.14.4.13. Criação de regras de QoS.
- 2.14.4.14. Emitir relatório de segurança mensal por localidade.
- 2.14.4.15. Criar relatórios e dashboards de acordo com as orientações a serem formuladas.
- 2.14.4.16. Todos os serviços contratados são de realização exclusiva da CONTRATADA, incluindo a implementação, operação, gerenciamento e manutenção do firewall e das plataformas associadas. A CONTRATANTE terá acesso ao Firewall apenas para consulta à plataforma de gerenciamento, monitoramento e logs, com a finalidade de criação e/ou geração de relatórios. Nenhum contato com a fabricante será de responsabilidade da CONTRATANTE, sendo essa atribuição exclusiva da CONTRATADA.
- 2.14.4.17. A empresa contratada deve implementar medidas de segurança da informação compatíveis com as melhores práticas do mercado e normas internacionais, como a ISO/IEC 27001 (Sistema de Gestão de Segurança da Informação), para garantir a proteção contra ameaças cibernéticas, acessos não autorizados e vazamentos de dados.

##### 2.14.5. SLA dos serviços e atendimento

- 2.14.5.1. Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;
- 2.14.5.2. Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;
- 2.14.5.3. Gerar relatórios de acesso e desempenho da solução de firewall.
- 2.14.5.4. Deverá possuir sistema de abertura de chamados pela internet.
- 2.14.5.5. Monitorar latência e uptime dos links configurados.
- 2.14.5.6. A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:
- 2.14.5.7. O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela.
- 2.14.5.8. Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.
- 2.14.5.9. Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela, a seguir:

##### Níveis de Severidade

1	Corresponde a situações em que o ambiente de produção está inoperante, sem disponibilidade de solução alternativa (workaround) imediata. Nesses casos, será exigido que o contratante disponibilize recursos técnicos dedicados para atuar de forma
---	---

	continua na resolução do problema, mantendo-se acessível durante o período de atendimento estabelecido neste contrato, ou seja, em regime de 8x5
2	Ocorre quando uma funcionalidade essencial está significativamente degradada, impactando o desempenho do sistema ou a experiência do usuário. Embora as operações possam prosseguir de forma limitada, há risco de comprometimento da produtividade ao longo do tempo. Nessa situação, existe uma solução alternativa (workaround) temporária disponível, permitindo a continuidade parcial das atividades até a resolução definitiva do problema.
3	Refere-se à perda parcial e não crítica de funcionalidades no ambiente. Determinados componentes apresentam falhas ou desempenho reduzido, mas o sistema permanece operante, permitindo ao usuário continuar utilizando suas funções principais. Há risco mínimo de interrupção total do ambiente produtivo.
4	Corresponde a solicitações relacionadas ao uso geral do sistema, ajustes de configuração rotineiros, questões de otimização ou problemas de natureza estética ("cosméticos"), que não impactam a operação, o desempenho ou a disponibilidade do ambiente produtivo.

### 2.15. Níveis de Severidade

2.15.1. Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.

2.15.2. Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime 8x5 (on-site ou remota), com atendimento no local em até 4 (quatro) horas úteis após o registro do chamado.

2.15.2.1. Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 8 (oito) horas úteis, após o registro do chamado.

2.15.2.2. Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 4 (quatro) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

2.15.3. Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime 8x5 (remota ou on-site), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

2.15.3.1. Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 12 (doze) horas úteis, a assistência técnica deverá ser on-site e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao próximo dia útil, após o registro do chamado.

2.15.3.2. Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

2.15.4. Para os chamados classificados como severidade 3 (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

2.15.4.1. A CONTRATADA terá, no máximo, 24 (Vinte e quatro) horas úteis, após registro do chamado, para implantar uma solução definitiva ou de contingência.

2.15.4.2. Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias corridos após o registro do chamado, a não ser que envolva a troca do equipamento.

2.15.5. Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

2.15.5.1. A CONTRATADA terá, no máximo, 8 (oito) dias corridos para solucionar o chamado, após o seu registro.

2.15.5.2. Não poderá haver limites no quantitativo de abertura de chamados.

### 2.16 Qualificação Técnica

2.16.1. Declaração formal de disponibilidade técnica, assinada por seu representante legal, em papel timbrado da licitante, atestando que possui estrutura adequada e terá disponível, em seu quadro de pessoal, quando da assinatura do contrato e o consequente início da prestação dos serviços, equipe de profissionais com as qualificações técnicas obrigatórias e necessárias à execução dos serviços, incluindo atendimento a requisitos de suporte técnico e gestão de incidentes de segurança, devendo comprovar, no mínimo:

2.16.2. 1 (um) profissional com certificação em tecnologias de firewall e segurança de rede (ex: certificações fornecidas pelos fabricantes de NGFW como Fortinet, Palo Alto, Cisco, entre outros);

2.16.3. Apresentar catálogos, prospectos, folders, manuais e outros documentos e informações sob a marca, fabricante, modelo e outros dados pertinentes que permitam a clara e segura identificação do produto ofertado, em idioma português ou inglês, em original ou cópia, não sendo aceitos documentos impressos de qualquer natureza produzidos com a finalidade específica de possibilitar e qualificar tecnicamente a proposta da licitante. Os documentos poderão ser entregues em formato eletrônico;

2.16.4. Documentos obtidos pela Internet no site do fabricante do software, cujas páginas deverão ter indicação do endereço URL em que foram obtidas;

2.16.5. Visando comprovar o atendimento aos requisitos técnicos, deverá ser fornecido juntamente com a proposta documento comprobatório de cada ponto solicitado neste termo de referência com base nos descritivos técnicos do firewall/Sdwan, sendo que os trechos da documentação que comprovem os respectivos requisitos devem estar explícitos contendo nome do documento e página, de forma a facilitar sua identificação e visualização.

## 3. SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3

### 3.1. Definição do objeto

3.1.1. Contratação emergencial de empresa especializada em serviços gerenciados em Tecnologia da Informação para: Gestão de infraestrutura de redes (LAN, VLAN e WLAN), ativos de rede, computadores, nobreaks, Suporte técnico remoto e presencial para 1 (uma) localidade, até 50 (cinquenta) estações de trabalho (Físicas ou virtuais), até 7 (sete) Servidores Físicos, e 12 (doze) servidores virtuais, abrangendo ativos de rede,

firewall (SonicWall), nobreaks e monitores. Manutenção preventiva e corretiva em nobreaks, estações de trabalho e monitores; Gestão e monitoramento de Links de internet, além da gestão e manutenção da infraestrutura hiperconvergente. visando atender às necessidades do CRCES em sua sede em Bento Ferreira, Vitória/ES, conforme condições e exigências estabelecidas neste instrumento.

**3.1.2.** O prazo de vigência da contratação é de 12 (doze) meses, na forma do artigo 75, VIII, da Lei 14.133/21da Lei nº 14.133, de 2021.

**3.1.3.** O presente serviço é enquadrado como continuado tendo em vista as especificações constantes em Estudo Técnico Preliminar.

**3.1.4.** O detalhamento necessário quanto ao período de vigência constará em instrumento contratual. A avaliação prévia do local de execução dos serviços é imprescindível para o conhecimento pleno das condições e peculiaridades do objeto a ser contratado, sendo assegurado ao interessado o direito de realização de vistoria prévia, acompanhado por servidor designado para esse fim, de segunda à sexta-feira das 09 horas às 15 horas, devendo ser solicitado agendamento através do e-mail [administrativo@crces.org.br](mailto:administrativo@crces.org.br).

**3.1.5.** Serão disponibilizados data e horário diferentes aos interessados em realizar a vistoria prévia.

**3.1.6.** Para a vistoria, o representante legal da empresa ou responsável técnico deverá estar devidamente identificado, apresentando documento de identidade civil e documento expedido pela empresa comprovando sua habilitação para a realização da vistoria.

### **3.2. Características da solução**

**3.2.1.** A execução do objeto seguirá a seguinte dinâmica:

**3.2.2.** Início da execução do objeto: 05 (cinco) dias úteis da emissão da ordem de serviço;

**3.2.3.** Descrição detalhada:

ITEM	CATSER	Descrição	Descrição complementar	Unidade de medida	Quantidade
01		<b>SOLUÇÃO DE ACESSO VIA WI-FI</b>	Fornecimento, instalação e gestão de uma rede corporativa Wi-Fi completa, visando superar as limitações da rede cabeada atual e garantir conectividade de alta qualidade em toda a sede do CRCES	Mês	12
02		<b>FIREWALL (SEDE)</b>	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	Mês	12
03		<b>SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3</b>	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo da infraestrutura, e manutenção preventiva e corretiva de todo o parque de TI.	Mês	12
04		<b>BACKUP CORPORATIVO</b>	Implementação e gestão de solução de backup local e em nuvem, garantindo a disponibilidade e a integridade dos dados críticos em caso de falhas, desastres ou ataques cibernéticos, essencial para a continuidade dos negócios e conformidade com a LGPD.	Mês	12

**3.2.4.** Contratada deve prestar os serviços gerenciados em Tecnologia da Informação para: Gestão de infraestrutura de redes (LAN, VLAN e WLAN), ativos de rede, computadores, nobreaks, Suporte técnico remoto e presencial para 1 (uma) localidade, até 50 (cinquenta) estações de trabalho (físicas ou virtuais), até 7 (sete) Servidores Físicos, e 12 (doze) servidores virtuais, ativos de rede, nobreaks e monitores. Manutenção preventiva e corretiva em nobreaks, estações de trabalho e monitores; Gestão e monitoramento de Links de internet, além da gestão e manutenção da infraestrutura hiperconvergente.

**3.2.5.** A empresa deverá estar pronta para gerir toda a estrutura hiperconvergente, que conta atualmente com dois clusters gerenciados de forma separada (com armazenamento baseado em Software-defined storage -SDS), uma infraestrutura com base em acessos VDI, máquinas virtuais. A empresa contratada deve estar pronta para lidar com seus backups, restores, e qualquer problema, falha, atualização, instalação ou análise oriunda desta relação de ferramentas integradas.

### **3.3. Requisitos técnicos**

#### **3.3.1. Monitoramento e suporte técnico**

**3.3.2.** Realizar o monitoramento proativo das estações de trabalho, identificando preventivamente falhas e promovendo ações corretivas;

**3.3.3.** Prestar suporte técnico remoto ilimitado aos usuários, conforme os seguintes níveis:

**3.3.4.** Nível 1 (N1): Atendimento de primeiro nível (dúvidas operacionais e incidentes comuns);

**3.3.5.** Nível 2 (N2): Suporte intermediário, com resolução de problemas técnicos e administrativos;

**3.3.6.** Nível 3 (N3): Suporte avançado, envolvendo infraestrutura, servidores e sistemas críticos;



**3.3.7.** Executar o monitoramento completo do ambiente de TI, por meio de ferramentas especializadas de mercado.

**3.3.8. Manutenção, gestão de ativos e rede**

**3.3.9.** Executar manutenção corretiva e preventiva em todos os ativos tecnológicos listados no item 6.1.1, sem custo adicional;

**3.3.10.** Realizar gestão e manutenção da estrutura hiperconvergente, garantindo operação contínua e eficiente dos recursos virtualizados;

**3.3.11.** Garantir o pleno funcionamento da solução de telefonia IP local, assegurando a operação contínua dos ramais, controladoras, interfaces e dispositivos vinculados, bem como a correção de falhas e apoio na configuração dos dispositivos conforme diretrizes da CONTRATANTE.

**3.3.12.** Executar a gestão técnica da infraestrutura de rede, abrangendo:

**3.3.13.** Administração de lans, vlans e sub-redes, com segmentação lógica adequada ao ambiente corporativo;

**3.3.14.** Configuração de protocolos de segurança de rede, como acls, 802.1X, VLAN tagging e controle de broadcast;

**3.3.15.** Implementação de boas práticas para prevenção de incidentes, como isolamento de tráfego e controle de acesso;

**3.3.16.** Apoio à CONTRATANTE na atualização de topologias, mapeamento de rede e análise de performance.

**3.3.17.** Executar serviços de instalação e gerenciamento de cabeamento de rede, incluindo as interligações entre os diversos setores da sede e o servidor central.

**3.3.18. Serviços gerenciados**

**3.3.19.** Prestar serviços gerenciados de segurança da rede e ativos de TI, incluindo políticas de proteção e respostas a incidentes;

**3.3.20.** Realizar a aplicação gerenciada de atualizações de segurança (patches) em estações de trabalho e servidores;

**3.3.21.** Gerenciar e administrar o ambiente de Office 365, incluindo usuários, licenças e segurança da informação;

**3.3.22.** Realizar a gestão e manutenção do banco de dados SQL Server, incluindo monitoramento de performance, backups e segurança.

**3.3.23. Controle, inventário e chamados**

**3.3.24.** Manter atualizado o inventário de hardware e software, contendo marca, modelo, especificações, localização e situação operacional dos ativos;

**3.3.25.** Efetuar a gestão de chamados por meio de sistema de tickets, com categorização por tipo de incidente, severidade, prazo e status de resolução.

**3.3.26. Logística e apoio à contratação**

**3.3.27.** Executar a logística de coleta e entrega de equipamentos entre a sede da CONTRATANTE e os locais de atendimento;

**3.3.28.** Prestar assessoria técnica nas aquisições de bens e serviços relacionados à TI, incluindo:

**3.3.29.** Elaboração de especificações técnicas;

**3.3.30.** Análise de propostas técnicas;

**3.3.31.** Apoio em processos licitatórios;

**3.3.32.** O prazo para entrega de pareceres técnicos será de até 5 (cinco) dias úteis, a partir de solicitação formal da CONTRATANTE.

**3.3.33. Atendimento presencial**

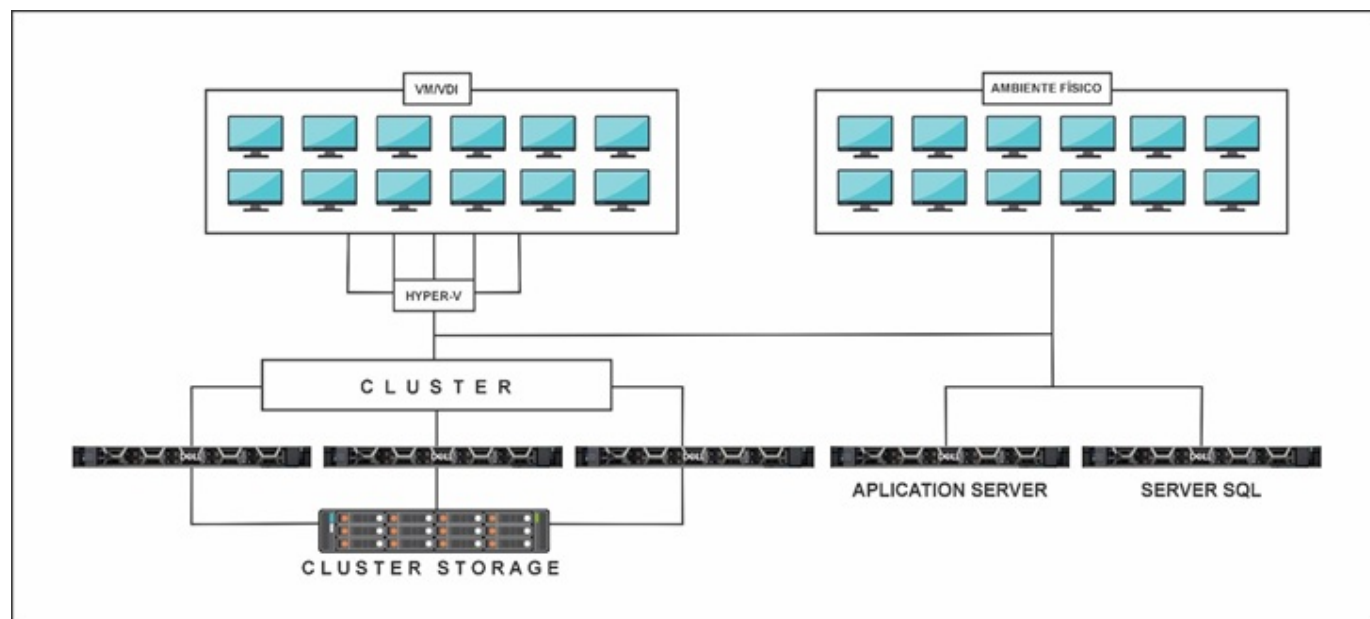
**3.3.34.** Disponibilizar 02 (duas) visitas técnicas presenciais por semana, com duração mínima de 8 (oito) horas por visita, para execução de tarefas presenciais corretivas, preventivas e de alinhamento com a equipe técnica da CONTRATANTE.

**3.3.35. Parque de informática do CRCES:**

TIPO	DESCRIÇÃO	QUANTIDADE
Equipamento de segurança	Firewall a ser contratado neste termo de referência	01
Pontos de acesso	Pontos de acesso a serem contratados neste termo de referência	A depender da solução contratada
Virtualizador	Hyper-V	05
Servidor Windows 2022 Server	Dell PowerEdge R640	02
Servidor Windows 2022 Server	Dell PowerEdge R650	03
Windows 2008 Server SQLSERVER 2008	Servidor Dell PowerEdge R710	01
Windows 2008 Server	Servidor Dell PowerEdge R710	01
Estação de Trabalho	Dell Optiplex 780	05
Estação de Trabalho	HP ProDesk 600 G1	01

Estação de Trabalho	Dell Optiplex 3040	01
Desktops virtualizados - VDI	ThinClient Dell Wyse 3040	35
Switch de agregação	Dell x4012 10x	02
Switch Core	Dell Networking N3048 L3 48x	02
NoBreak	NHS Premium OL (Rack/3000VA/8b.9Ah)	03
Monitor	HP V22B 21,5"	20
Monitor	Monitor 23.8" Philips LED 242V8A	14
Monitor	Monitor 23.8" Acer CB242YDBMIPRCX	42
Notebook	Dell Vostro 15 3500	05
Acesso remoto	SonicWall SMA 550V Standard	20
Projetor de imagem	Epson Powerlite W42	05
Scanner de mesa	Avision AV186+	03
Impressora térmica	Argox	01
Impressora matricial	Epson LX-350	01
Telefone IP SIP	Yalink T19PE2	25
Telefone IP Gigabit	Yalink T27G	01

**3.3.36. A hiperconvergência do CRCES está funcionando atualmente no seguinte cenário:**



### 3.3.36. Manutenção Preventiva e Corretiva

#### 3.3.36.1. Manutenção Preventiva

3.3.36.1.1. A manutenção preventiva consiste na execução periódica de atividades planejadas com o objetivo de garantir o funcionamento contínuo, seguro e eficiente dos equipamentos e sistemas de TIC do CRCES, visando a prevenção de falhas, degradações de desempenho e indisponibilidades.

3.3.36.1.2. Tais atividades incluem, mas não se limitam a:

3.3.36.1.2.1. Verificação de funcionamento dos componentes físicos e lógicos;

- 3.3.36.1.2.2. Limpeza técnica interna e externa;
- 3.3.36.1.2.3. Aferição e calibração de dispositivos, quando aplicável;
- 3.3.36.1.2.4. Atualização de firmwares, BIOS e softwares;
- 3.3.36.1.2.5. Verificação e otimização de configurações;
- 3.3.36.1.2.6. Avaliação do desempenho geral e análise de logs;
- 3.3.36.1.2.7. Testes de funcionalidade e conectividade.
- 3.3.36.1.3. Os equipamentos e ativos de tecnologia que deverão ser contemplados no plano de manutenção preventiva incluem:
  - 3.3.36.1.3.1. Servidores físicos;
  - 3.3.36.1.3.2. Servidores virtuais;
  - 3.3.36.1.3.3. Infraestrutura de rede (switches, cabeamento, racks, patch panels, etc.);
  - 3.3.36.1.3.4. Ativos de rede (roteadores, access points, controladoras, etc.);
  - 3.3.36.1.3.5. Estações de trabalho tipo desktop;
  - 3.3.36.1.3.6. Nobreaks e sistemas de energia ininterrupta;
  - 3.3.36.1.3.7. Terminais de desktop virtualizado (Thin Clients);
  - 3.3.36.1.3.8. Firewalls e appliances de segurança;
  - 3.3.36.1.3.9. Notebooks;
  - 3.3.36.1.3.10. Scanners (digitalizadores) de mesa e portáteis;
  - 3.3.36.1.3.11. Projetores multimídia;
  - 3.3.36.1.3.12. Monitores LCD/LED;
  - 3.3.36.1.3.13. Telefones IP e demais dispositivos de comunicação.
- 3.3.36.1.4. A CONTRATADA deverá elaborar e apresentar, no prazo máximo de 15 (quinze) dias após a assinatura do contrato, um Plano de Manutenção Preventiva, contendo a periodicidade, o escopo das atividades para cada tipo de equipamento e a metodologia empregada, o qual deverá ser aprovado pela CONTRATANTE.
- 3.3.36.1.5. A execução da manutenção preventiva deverá ser previamente agendada com a CONTRATANTE, de modo a não impactar as atividades institucionais. Caso haja necessidade de interrupção de serviço, deverá haver comunicação com no mínimo 48 (quarenta e oito) horas de antecedência.
- 3.3.36.1.6. Ao término de cada manutenção preventiva realizada, deverá ser emitido Relatório Técnico, contendo a descrição das atividades executadas, o diagnóstico dos equipamentos, recomendações de melhorias (quando houver) e a assinatura do responsável técnico da CONTRATADA, bem como do servidor responsável pela fiscalização do contrato.
- 3.3.36.1.7. A CONTRATADA deverá manter o histórico atualizado de todas as manutenções preventivas executadas, o qual deverá estar disponível para auditoria e fiscalização da CONTRATANTE sempre que solicitado.
- 3.3.36.2. Manutenção Corretiva
  - 3.3.36.2.1. Em caso de problema técnico, a contratada deverá providenciar laudo técnico e orçamento prévio das peças no prazo máximo de 5 (cinco) dias úteis, de forma detalhada, abrangendo quantidade, marca e modelo a serem consertados ou adquiridos. Os equipamentos que forem retirados para manutenção deverão ser devolvidos aos mesmos locais onde estavam nas dependências do CRCES.
  - 3.3.36.2.2. A CONTRATADA deverá conduzir as suas ações em conformidade com os requisitos legais e regulamentos aplicáveis, observando ainda a legislação ambiental aplicável, designando adequadamente todos os materiais e equipamentos utilizados na execução do contrato.
  - 3.3.36.2.3. A empresa deve apresentar cronograma de retirada dos equipamentos para manutenção externa (se necessário) e fornecer equipamentos substitutos, de mesmo tipo e capacidade, que estejam em condições de uso e com identificação do fornecedor, para garantir o funcionamento regular das atividades do CRCES.
  - 3.3.36.2.4. A empresa contratada é obrigada a programar a coleta dos equipamentos com no mínimo um dia útil de antecedência, assegurando a disponibilização de unidades substitutas até que os equipamentos da contratante sejam devidamente preparados para uso e reinstalados em seus locais originais.
  - 3.3.36.2.5. Todos os custos de aquisição de peças serão arcados pela CONTRATANTE, e a contratada deverá enviar especificação técnica após a identificação do problema para as cotações necessárias e posterior instalação das peças adquiridas pela empresa contratada.
  - 3.3.36.2.6. Em caso de necessidade de aquisição de peças por parte do CRCES, a contratada deverá providenciar a instalação das peças adquiridas pelo CRCES em até 5 (cinco) dias úteis após o recebimento dos novos equipamentos/peças.
  - 3.3.36.2.7. Os prazos acima poderão ser revistos, mediante a apresentação de justificativa válida e aceita pela contratante.
  - 3.3.36.2.8. Durante a execução do serviço externo, a empresa contratada deverá:
    - 3.3.36.2.8.1. Se responsabilizar pelo transporte dos equipamentos que serão retirados;
    - 3.3.36.2.8.2. Providenciar termo de responsabilidade de retirada;
    - 3.3.36.2.8.3. Cumprir todas as obrigações constantes e assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.
  - 3.3.36.2.9. O material deverá ser entregue sem avarias, devendo ser identificado com informações precisas, corretas, claras, em língua portuguesa sobre suas características, quais sejam: quantidade e descrição do produto;
  - 3.3.36.2.10. O descarregamento do produto ficará a cargo da Contratada, devendo ser providenciada a devida mão de obra;
  - 3.3.36.2.11. A Contratada deverá comunicar a data de entrega com 2 (dois) dias úteis de antecedência ao CRCES;
  - 3.3.36.2.12. Os produtos serão recebidos por empregado do CRCES e, no caso de recebimento provisório, não implicará em aceitação dos mesmos;
  - 3.3.36.2.13. O recebimento definitivo não transfere a responsabilidade futura perante a qualidade do produto entregue.

- 3.3.36.2.13. O recebimento definitivo não isenta a empresa de responsabilidades futuras quanto a qualidade do produto entregue;
- 3.3.36.2.14. Todas as peças que apresentaram problemas e foram substituídas deverão ser identificadas e entregues ao departamento de T.I do CRCES.
- 3.3.37. SLA dos Serviços e Atendimento**
- 3.3.37.1. Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;
- 3.3.37.2. Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;
- 3.3.37.3. O ambiente de TI do CRCES deverá ser continuamente monitorado por ferramentas especializadas, com alertas automáticos e registro de falhas, a fim de garantir o funcionamento adequado e a disponibilidade dos recursos.
- 3.3.37.4. Deverá gerar e fornecer, mediante solicitação, relatórios técnicos de desempenho e disponibilidade, incluindo estatísticas de uptime, latência de links, falhas críticas e acessos aos dispositivos.
- 3.3.37.5. Deverá possuir sistema de abertura de chamados pela internet.
- 3.3.37.6. Monitorar latência e uptime dos links configurados.
- 3.3.37.7. A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:
- 3.3.37.7.1. O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela (a ser fornecida ou referenciada no documento original).
- 3.3.37.7.2. Os níveis de atendimento técnico (N1, N2 e N3) deverão seguir o escopo descrito no item 3.3, com suporte remoto ilimitado e visitas técnicas presenciais duas vezes por semana (conforme cláusula 3.3.34).
- 3.3.37.7.3. Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.
- 3.3.37.8. Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela (a ser fornecida ou referenciada no documento original).

Níveis de Severidade	
1	Corresponde a situações em que o ambiente de produção está inoperante, sem disponibilidade de solução alternativa (workaround) imediata. Nesses casos, será exigido que o contratante disponibilize recursos técnicos dedicados para atuar de forma contínua na resolução do problema, mantendo-se acessível durante o período de atendimento estabelecido neste contrato, ou seja, em regime de 8x5
2	Ocorre quando uma funcionalidade essencial está significativamente degradada, impactando o desempenho do sistema ou a experiência do usuário. Embora as operações possam prosseguir de forma limitada, há risco de comprometimento da produtividade ao longo do tempo. Nessa situação, existe uma solução alternativa (workaround) temporária disponível, permitindo a continuidade parcial das atividades até a resolução definitiva do problema.
3	Refere-se à perda parcial e não crítica de funcionalidades no ambiente. Determinados componentes apresentam falhas ou desempenho reduzido, mas o sistema permanece operante, permitindo ao usuário continuar utilizando suas funções principais. Há risco mínimo de interrupção total do ambiente produtivo.
4	Corresponde a solicitações relacionadas ao uso geral do sistema, ajustes de configuração rotineiros, questões de otimização ou problemas de natureza estética (“cosméticos”), que não impactam a operação, o desempenho ou a disponibilidade do ambiente produtivo.

**3.3.38 Níveis de Severidade**

- **3.3.38.1.** Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.
- **3.3.38.2.** Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime **8x5 (on-site ou remota)**, com atendimento no local em até **4 (horas) horas úteis** após o registro do chamado.
  - **3.3.38.2.1.** Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a **8 (oito) horas úteis**, após o registro do chamado.
  - **3.3.38.2.2.** Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar **4 (quatro) dias úteis** após o registro do chamado, a não ser que envolva a troca do equipamento.
- **3.3.38.3.** Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime **8x5 (remota ou on-site)**, com atendimento em até **8 (oito) horas úteis** após o registro do chamado.
  - **3.3.38.3.1.** Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após **12 (doze) horas úteis**, a assistência técnica deverá ser onsite e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao **próximo dia útil**, após o registro do chamado.
  - **3.3.38.3.2.** Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar **8 (oito) dias úteis** após o registro do chamado, a não ser que envolva a troca do equipamento.

- **3.3.38.4.** Para os chamados classificados como severidade 3 (tres), a assistência técnica será prestada em **horário comercial, em regime 8 x 5 (remota)**, com atendimento em até **8 (oito) horas úteis** após o registro do chamado.
  - **3.3.38.4.1.** A CONTRATADA terá, no máximo, **24 (Vinte e quatro) horas úteis**, após registro do chamado, para implantar uma solução definitiva ou de contingência.
  - **3.3.38.4.2.** Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar **8 (oito) dias corridos** após o registro do chamado, a não ser que envolva a troca do equipamento.
- **3.3.38.5.** Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em **horário comercial, em regime 8 x 5 (remota)**, com atendimento em até **8 (oito) horas úteis** após o registro do chamado.
  - **3.3.38.5.1.** A CONTRATADA terá, no máximo, **8 dias corridos** para solucionar o chamado, após o seu registro.
  - **3.3.38.5.2.** Não poderá haver limites no quantitativo de abertura de chamados.

### 3.3.39 Qualificação Técnica

- **3.3.39.1.** A complexa infraestrutura de TI do CRCES, composta por diversos componentes interligados e tecnologias de ponta, exige um alto nível de detalhamento no Termo de Referência para garantir a efetividade da contratação e a correta execução dos serviços. Sem esse detalhamento, torna-se inviável:
- **3.3.39.2.** Experiência em Hiperconvergência: A empresa contratada deve comprovar experiência em implementação, operação e manutenção de infraestruturas hiperconvergentes, incluindo profundo conhecimento em tecnologias como VMware vSAN, Nutanix AHV e HPE Simplivity.
- **3.3.39.3.** Gerenciamento de Clusters de Servidores: Expertise na gestão de clusters de servidores de grande porte, incluindo balanceamento de carga, otimização de recursos, failover e alta disponibilidade, é fundamental para garantir a performance e confiabilidade dos sistemas.
- **3.3.39.4.** Virtualização com Hyper-V: A empresa deve demonstrar conhecimento avançado na virtualização de desktops com Hyper-V, incluindo provisionamento de desktops virtuais, gerenciamento de imagens, otimização de desempenho e segurança da rede virtual.
- **3.3.39.5.** Administração de Banco de Dados SQL: Expertise em administração de bancos de dados SQL, incluindo otimização de desempenho, segurança da informação, backup e recuperação de desastres, é crucial para garantir a integridade dos dados críticos do CRCES.
- **3.3.39.6.** Integração com SEFAZ ES e CFC: A empresa precisa comprovar experiência em integração de sistemas com órgãos governamentais, incluindo protocolos de comunicação, segurança da informação e monitoramento constante da integração.
- **3.3.39.7.** Gerenciamento de Serviços Online: Expertise em administração de sistemas, redes e segurança da informação é essencial para garantir o funcionamento adequado dos serviços online do CRCES, com alta disponibilidade, performance e segurança.
- **3.3.39.8.** Certificação ITIL v3 ou superior;
- **3.3.39.9.** Certificação MCSA Windows Server 2012 ou superior;
- **3.3.39.10.** A empresa deverá comprovar, mediante atestados de capacidade técnica emitidos por pessoas jurídicas de direito público ou privado, já ter atuado com:
  - **3.3.39.10.1.** Gestão de ambientes com infraestrutura virtualizada e VDI com pelo menos 30 estações virtuais;
  - **3.3.39.10.2.** Suporte a infraestruturas com mais de 5 servidores físicos e 10 servidores virtuais simultâneos;
  - **3.3.39.10.3.** Monitoramento e gestão de ambientes com hiperconvergência e armazenamento definido por software (SDS);

## 4. BACKUP CORPORATIVO

### 4.1. Software de Backup

- **4.1.1.** Deverá ser disponibilizado 14 licenças para backup de máquinas virtuais,
- **4.1.2.** Backup Local e em Nuvem: O software deve oferecer a capacidade de fazer backups locais no appliance de backup e permitir o envio de backups para a nuvem pública (ex. Amazon S3, Azure Blob Storage). Isso garante redundância e recuperação em casos de desastres.
- **4.1.3.** Gerenciamento Centralizado: Interface centralizada para gerenciar backups tanto locais quanto na nuvem, possibilitando uma visualização única de todos os dados armazenados.
- **4.1.4.** Deduplicação Avançada: A deduplicação deve ocorrer tanto no lado fonte (antes do envio dos dados) quanto no lado destino, para reduzir o consumo de armazenamento. Isso é fundamental para economizar espaço em disco e largura de banda ao transferir para a nuvem.
- **4.1.5.** Taxas de Deduplicação: Suporte para taxas de deduplicação eficazes, como 3:1 ou 2:1, garantindo que os dados sejam armazenados de maneira eficiente e que menos espaço seja utilizado tanto localmente quanto na nuvem.
- **4.1.6.** Compressão de Dados: A compressão deve ser personalizável para otimizar o desempenho conforme as necessidades da infraestrutura, especialmente em volumes de escrita diários significativos.
- **4.1.7.** Crescimento Modular: O software precisa suportar o aumento de dados, permitindo expandir o volume de backup. Ele deve ser capaz de lidar com o crescimento anual projetado com base na taxa de escrita dos servidores.
- **4.1.8.** Suporte a Multinuvem: Deve permitir integração com diferentes provedores de nuvem, como Amazon S3, Azure, Google Cloud, para garantir flexibilidade na escolha e custos competitivos.
- **4.1.9.** Criptografia de Dados em Trânsito e em Repouso: Deve suportar criptografia robusta, como AES-256, para proteger os dados tanto enquanto eles estão sendo transferidos para a nuvem quanto enquanto estão armazenados, garantindo conformidade com a LGPD.
- **4.1.10.** Autenticação Multifator (MFA): Integração com sistemas de autenticação multifator para acessar o software e as configurações de backup, assegurando que somente usuários autorizados possam modificar as políticas de backup.
- **4.1.11.** Proteção contra Ransomware: Deve incluir funcionalidades para proteger contra ataques de ransomware, garantindo que os backups não sejam corrompidos ou excluídos por agentes maliciosos. Deve suportar recursos de "Imutabilidade" em backups em nuvem.
- **4.1.12.** Suporte para Ambientes Virtuais e Físicos: O software deve ser capaz de realizar backups tanto de máquinas físicas quanto de ambientes virtualizados (VMware, Hyper-V, etc.), garantindo cobertura total do ambiente.



- 4.1.13. Backup de Máquinas Virtuais com Consistência de Aplicações:** O backup de máquinas virtuais deve ser realizado com consistência de aplicativos, garantindo que bancos de dados e outros sistemas transacionais sejam corretamente salvos.
- 4.1.14. Backup Incremental e Diferencial:** Para otimizar o tempo e o espaço de armazenamento, o software deve suportar backups incrementais e diferenciais, armazenando apenas as mudanças desde o último backup completo.
- 4.1.15. Cópias de Backup Imutáveis:** Recursos que garantam a imutabilidade dos backups, evitando alterações ou exclusões até que o período de retenção termine, principalmente em caso de ataques de ransomwares.
- 4.1.16. Retenção Personalizável:** O software deve oferecer flexibilidade na configuração de políticas de retenção, permitindo retenção de longo prazo em discos locais e retenção de curto prazo para backups de nuvem.
- 4.1.17. Arquivamento Inteligente:** Capacidade de arquivar backups antigos na nuvem para economizar espaço local, enquanto mantém acessível para restauração conforme necessário.
- 4.1.18. Monitoramento e Alertas:** O software precisa oferecer monitoramento contínuo de todos os trabalhos de backup, com alertas para falhas, desempenho abaixo do esperado ou outros problemas.
- 4.1.19. Dashboard Intuitivo:** Um painel de controle que permita a visualização em tempo real do status dos backups e do uso de recursos, como IOPS, Throughput e latência.
- 4.1.20. Otimização de Recursos (IOPS e Throughput):** O software deve ser capaz de ajustar automaticamente o uso de recursos de acordo com as características da infraestrutura, respeitando o throughput e IOPS máximos dos servidores.
- 4.1.21. Restauração Granular:** Capacidade de restaurar desde arquivos individuais até máquinas inteiras (físicas ou virtuais), com velocidade e flexibilidade.
- 4.1.22. Recuperação Bare-Metal:** Capacidade de restaurar máquinas físicas diretamente para novas instâncias ou hardware, sem a necessidade de configuração manual de cada sistema.
- 4.1.23. Testes de Restauração Automática:** Testes automáticos de restauração para garantir que os backups estão íntegros e prontos para serem restaurados se necessário.
- 4.1.24. Integração Nativa com Provedores de Nuvem:** Suporte para integrações nativas com serviços de armazenamento de nuvem como Amazon S3, Microsoft Azure Blob Storage e Google Cloud Storage, no mínimo.
- 4.1.25. Economia de Largura de Banda:** Uso inteligente da largura de banda durante backups para a nuvem, para otimizar as transferências de dados para a nuvem.
- 4.1.26. Perfis de Acesso Personalizáveis:** O software deve permitir a criação de perfis de usuários com permissões personalizáveis, garantindo que apenas pessoal autorizado possa gerenciar ou restaurar os dados de backup.
- 4.1.27. Controle de Acessos Granular:** Capacidade de definir permissões específicas para diferentes tipos de dados e volumes de backup, garantindo que acessos indevidos sejam evitados.
- 4.1.28. Suporte a LGPD e Outras Normas:** O software deve estar em conformidade com regulamentações, como a LGPD, e deve permitir auditorias completas e geração de relatórios detalhados sobre os backups e o uso de dados.
- 4.1.29. Auditorias e Relatórios:** Geração de relatórios automáticos sobre o status dos backups e a conformidade com as políticas de retenção e segurança, facilitando a auditoria e a resposta a exigências legais.
- 4.1.30. Automatização de trabalhos de Backup:** Capacidade de automatizar os processos de backup, permitindo agendamentos e execuções automáticas conforme as necessidades do ambiente.
- 4.1.31. Integração com Ferramentas de Orquestração:** Suporte para integração com ferramentas de orquestração e automação (ex: scripts PowerShell, APIs).
- 4.1.32. Cobertura Completa:** O software deve oferecer suporte abrangente para backup de Exchange Online, OneDrive for Business, SharePoint Online, e Microsoft Teams, assegurando que todos os componentes da solução Microsoft 365 sejam cobertos.
- 4.1.33. Recuperação Granular:** Deve permitir a restauração granular de itens individuais (emails, arquivos, sites de SharePoint, conversas do Teams) além de permitir a restauração de volumes maiores, como caixas de e-mail completas ou sites inteiros.
- 4.1.34. Agendamento e Automação:** A capacidade de definir backups automáticos regulares para o Microsoft 365, garantindo que os dados estejam sempre atualizados e protegidos sem intervenção manual constante.

## **4.2. Appliance de Backup Local**

- 4.2.1.** A contratada deverá ser responsável pela gestão, configuração, operação e manutenção do servidor local de backup fornecido pelo CRC-ES, modelo Dell PowerEdge R710, composto inicialmente por 05 (cinco) discos rígidos com capacidade de 1 TB cada.
- 4.2.2.** Deverá realizar visita técnica presencial no local onde se encontra o servidor, para fins de vistoria e validação do estado físico e funcional do equipamento.
- 4.2.3.** Será responsável por configurar o sistema de armazenamento local do equipamento, devendo:
- 4.2.3.1.** Criar e configurar o arranjo de discos em RAID 5;
- 4.2.3.2.** Instalar e configurar sistema operacional baseado em Linux (com preferência por versões LTS, como Ubuntu Server ou Debian Stable);
- 4.2.3.3.** Provisionar o volume lógico para armazenamento dos dados de backup, com diretórios e permissões apropriadas
- 4.2.4.** Deverá realizar as configurações de rede e segurança necessárias para permitir o tráfego seguro dos dados de backup entre os ambientes locais e em nuvem.
- 4.2.5.** Será responsável por configurar o software de backup na infraestrutura local, integrando-o com o ambiente em nuvem, devendo:
- 4.2.5.1.** Garantir que os dados de backup armazenados localmente estejam sincronizados com os dados de backup na nuvem;
- 4.2.5.2.** Gerar e manter registros e relatórios de status dos backups locais e remotos;
- 4.2.5.3.** Implementar política de retenção e descarte conforme diretrizes estabelecidas pelo CRC-ES.

4.2.5.5. Implementar política de retenção e descarte conforme diretrizes estabelecidas pelo CRC-ES;

4.2.6. Deverá realizar monitoramento contínuo do servidor de backup local, incluindo:

4.2.6.1. Acompanhamento da integridade dos discos e volumes lógicos;

4.2.6.2. Monitoramento do uso de espaço em disco e alertas proativos;

4.2.6.3. Verificação da consistência dos arquivos de backup e testes periódicos de restauração.

4.2.7. Será responsável pelo suporte técnico completo ao servidor de backup local, devendo atuar:

4.2.7.1. De forma remota, em primeira instância, e presencialmente, caso não seja possível resolver o incidente de forma remota;

4.2.7.2. Dentro dos prazos estabelecidos no Acordo de Nível de Serviço (ANS/SLA).

4.2.8. deverá garantir que a solução de backup seja escalável. No caso de crescimento da volumetria de backup e esgotamento da capacidade atual, caberá à CONTRATADA:

4.2.8.1. Notificar formalmente a CONTRATANTE sobre a necessidade de expansão;

4.2.8.2. Realizar a instalação de novos discos no equipamento, previamente adquiridos pela CONTRATANTE ou fornecidos pela CONTRATADA, conforme contratação;

4.2.8.3. Reconfigurar o RAID e volumes lógicos, preservando os dados existentes e a integridade do ambiente;

4.2.8.4. Ajustar as políticas de backup e monitoramento para o novo ambiente.

4.2.9. Toda e qualquer alteração na infraestrutura de backup local deverá ser previamente comunicada e autorizada pelo CRC-ES.

#### **4.3. Armazenamento de backup em nuvem**

4.3.1. Deverá ser disponibilizado, no mínimo, 25 (vinte e cinco) terabytes de capacidade de armazenamento utilizável, respeitando os níveis de desempenho e retenção definidos neste Termo de Referência.

4.3.2. O armazenamento em nuvem deve ser compatível com o software de backup fornecido.

4.3.3. Deverá ser fornecido serviço de armazenamento em nuvem pública compatível com soluções de backup corporativas que utilizem armazenamento em formato objeto (object storage), com suporte a repositórios escaláveis e integração por API.

4.3.4. O armazenamento deverá ser compatível com recursos como cópia de backup em nuvem, retenção imutável de dados, e suporte a múltiplas camadas de armazenamento de acordo com o tempo de retenção e a criticidade dos dados.

4.3.5. O serviço deverá permitir o envio automático de dados a partir de repositórios locais, conforme regras de ciclo de vida e retenção configuradas pela CONTRATANTE, bem como a utilização de políticas de arquivamento e movimentação entre camadas de armazenamento.

4.3.6. A integração deverá garantir a utilização plena de todas as funcionalidades da ferramenta de backup, incluindo repositórios externos, retenções avançadas, restauração granular, movimentação entre camadas e proteção imutável.

4.3.7. A solução deverá oferecer proteção contra exclusões acidentais e ataques de ransomware, por meio de funcionalidade de imutabilidade de dados (object lock ou equivalente), respeitando os prazos de retenção definidos pelo CRC.

4.3.8. Permite que múltiplas versões de um arquivo sejam mantidas no caso de necessidade de recuperação de dados antigos.

4.3.9. O armazenamento deverá ser compatível com recursos como cópia de backup em nuvem, retenção imutável de dados, e suporte a múltiplas camadas de armazenamento de acordo com o tempo de retenção e a criticidade dos dados.

4.3.10. O armazenamento em nuvem deve fornecer criptografia de dados em trânsito (durante a transferência) e em repouso (armazenados).

4.3.11. TLS/SSL deve ser usado para proteger os dados durante a transferência.

4.3.12. Criptografia em repouso é necessária para proteger os dados armazenados, utilizando algoritmos como AES-256.

4.3.13. Chaves de criptografia devem ser gerenciadas de forma segura, seja pelo cliente ou pelo provedor de nuvem.

4.3.14. O serviço deverá oferecer alta disponibilidade de pelo menos 99,99% e garantir SLA mínimo de 99,9% para o acesso ao armazenamento.

4.3.15. O armazenamento deve possuir capacidade de escala praticamente ilimitada, sem necessidade de intervenção manual, manutenção ou monitoramento contínuo por parte da CONTRATANTE.

4.3.16. Os dados devem ser armazenados com redundância física, em múltiplos equipamentos e zonas de disponibilidade distintas, de forma a garantir a persistência e a tolerância a falhas de hardware.

4.3.17. A CONTRATADA deverá assegurar que os dados permaneçam exclusivamente em território brasileiro durante todo o período de vigência contratual, inclusive cópias e réplicas.

4.3.18. O provedor de nuvem precisa oferecer APIs RESTful que permitam a integração com o software de backup para realizar as operações de gravação, leitura, e exclusão de dados de forma automatizada.

4.3.19. Toda e qualquer atividade de acesso à API de armazenamento deverá ser registrada, auditável e consultável por meio de relatórios de trilha de auditoria, incluindo acessos, alterações e exclusões de objetos.

4.3.20. Deve fornecer mecanismos robustos de controle de acesso com perfis de usuário e controle baseado em funções (RBAC), permitindo que diferentes níveis de acesso sejam concedidos conforme a função do usuário (administração, auditoria, leitura, etc.).

4.3.21. O uso de políticas de acesso detalhadas como o IAM (Identity and Access Management) é essencial para garantir que apenas usuários autorizados possam acessar os backups.

4.3.22. A solução de armazenamento deve oferecer monitoramento contínuo com métricas e alertas configuráveis, permitindo que a equipe de TI monitore a utilização do espaço, desempenho, e possíveis falhas.

4.3.23. Ferramentas de monitoramento nativas devem estar integradas.

4.3.24. Os custos devem estar inclusos na cobrança mensal do armazenamento.

#### **4.4. SLA dos serviços e atendimento**

- 4.4.1.** Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;
- 4.4.2.** Deverá monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;
- 4.4.3.** deverá gerar e fornecer, mediante solicitação, relatórios técnicos de desempenho e disponibilidade, incluindo estatísticas de uptime e falhas críticas.
- 4.4.4.** Deverá possuir sistema de abertura de chamados pela internet.
- 4.4.5.** A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:
- 4.4.6.** O tratamento dos chamados abertos junto à CONTRATADA visa à disponibilidade e à qualidade da operação do equipamento contratado. Para tanto, a CONTRATADA deverá garantir os atendimentos aos chamados dentro dos prazos e grau de severidade explicitados na tabela.
- 4.4.7.** Para a realização de manutenções corretivas ou preventivas programadas, a CONTRATADA deverá planejar e negociar com a equipe de gestão de mudanças da CONTRATANTE, para obter a autorização do melhor período para as paralisações necessárias.
- 4.4.8.** Para apuração do índice de tempo de atendimento para solução de problemas, os chamados são classificados em 4 (quatro) Níveis de Severidade, de acordo com a tabela , a seguir:

Níveis de Severidade	
1	Corresponde a situações em que haja Interrupção total do sistema de backup (local e/ou nuvem); perda de capacidade de restauração; falha de sincronização completa.
2	Ocorre quando há falha em backup de sistemas críticos; perda parcial da comunicação com a nuvem; degradação severa.

3	Refere-se à problemas com backups não críticos, alertas de desempenho, erros isolados de backup..
4	Solicitações de configuração, dúvidas, relatórios, auditoria.

#### **4.4.9. Níveis de Severidade**

**4.4.10.** Um chamado somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE.

**4.4.11.** Para os chamados classificados como de severidade 1 (um), a assistência técnica será prestada em regime 8x5 (on-site ou remota), com atendimento no local em até 4 (horas) horas úteis após o registro do chamado.

**4.4.11.1.** Em caso de adoção de uma solução de contingência ou de contorno, esta não poderá ser implementada em prazo superior a 8 (oito) horas úteis, após o registro do chamado.

**4.4.11.2.** Em sendo utilizada uma solução de contingência, a solução definitiva não poderá ultrapassar 4 (quatro) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

**4.4.12.** Para os chamados classificados como severidade 2 (dois), a assistência técnica será prestada em regime 8x5 (remota ou on-site), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

**4.4.12.1.** Após a abertura de chamado, caso o problema não tenha sido contingenciado remotamente após 12 (doze) horas úteis, a assistência técnica deverá ser onsite e a solução de contingência ou de contorno não poderá ser implementada em prazo superior ao próximo dia útil, após o registro do chamado.

**4.4.12.2.** Em sendo utilizada uma solução de contingência ou contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias úteis após o registro do chamado, a não ser que envolva a troca do equipamento.

**4.4.13.** Para os chamados classificados como severidade 3 (três), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

**4.4.13.1.** A CONTRATADA terá, no máximo, 24 (Vinte e quatro) horas úteis, após registro do chamado, para implantar uma solução definitiva ou de contingência

**4.4.13.2.** Em sendo utilizada uma solução de contingência ou de contorno, a solução definitiva não poderá ultrapassar 8 (oito) dias corridos após o registro do chamado, a não ser que envolva a troca do equipamento.

**4.4.14.** Para os chamados classificados como severidade 4 (quatro), a assistência técnica será prestada em horário comercial, em regime 8 x 5 (remota), com atendimento em até 8 (oito) horas úteis após o registro do chamado.

**4.4.14.1.** A CONTRATADA terá, no máximo, 8 dias corridos para solucionar o chamado, após o seu registro.

**4.4.14.2.** Não poderá haver limites no quantitativo de abertura de chamados.

#### **4.3.3.17. Certificações**

Será necessário solicitar algumas certificações, com isso o CRCES está garantindo que a empresa contratada possui o conhecimento e as habilidades necessárias para prestar um serviço de alta qualidade, alinhado com as melhores práticas do mercado e com as recomendações de segurança de órgãos como o NIST e o CIS.

**Abaixo, vamos citar cada uma delas, ampliando as justificativas:**

**a) Certificação Microsoft Certified Solutions Associate (MCSA) Windows Server 2012 (no mínimo)**

**Domínio do Sistema Operacional:** A certificação MCSA garante que o profissional possui um conhecimento profundo do Windows Server 2012,

que é a base do nosso ambiente corporativo hiperconvergente. Isso inclui domínio em instalação, configuração, administração e troubleshooting do sistema operacional, além de serviços como Active Directory, DNS, DHCP e outros.

**Integração com Outros Serviços:** O Windows Server é integrado a outros serviços da Microsoft, como Exchange, SharePoint e SQL Server. Um profissional com a certificação MCSA terá mais facilidade em integrar e gerenciar esses serviços em um ambiente unificado.

**Padrão de Qualidade e Alinhamento com Boas Práticas:** A certificação MCSA é reconhecida mundialmente como um padrão de qualidade para profissionais de infraestrutura. Ela demonstra que o profissional possui as habilidades necessárias para lidar com as complexidades de um ambiente como o nosso, que possui dois clusters e funciona no modelo de hiperconvergência, além de estar alinhado com as melhores práticas do mercado.

#### **b) Certificação para Instalação e Configuração de Switches DELL ou similar**

**Infraestrutura de Rede e Otimização:** Switches são equipamentos essenciais para a interconexão de dispositivos em uma rede. A certificação garante que o profissional possui conhecimento sobre os princípios de funcionamento de switches, além de saber como configurá-los para atender às necessidades específicas da rede do CRCES, que utiliza switches complexos de alta tecnologia (tanto o core quanto o de agregação da hiperconvergência). Isso permite otimizar o desempenho da rede, reduzindo a latência e aumentando a disponibilidade.

**Escalabilidade e Flexibilidade:** À medida que a rede cresce, é necessário adicionar novos switches. Um profissional certificado terá as habilidades necessárias para integrar novos switches à rede existente, garantindo a escalabilidade da infraestrutura e a flexibilidade para atender às futuras demandas do CRCES.

**Alinhamento com as Melhores Práticas:** A certificação garante que o profissional está familiarizado com as melhores práticas de configuração e gerenciamento de redes, o que contribui para a estabilidade e a segurança da infraestrutura.

As certificações solicitadas demonstram que a empresa contratada possui o conhecimento e as habilidades necessárias para prestar um serviço de alta qualidade para o CRCES. Elas garantem que os profissionais terão a capacidade de:

**Gerenciar e manter a infraestrutura de TI** de forma eficiente, segura e alinhada com as melhores práticas do mercado.

**Resolver problemas** de forma rápida e eficaz, minimizando o tempo de inatividade do sistema.

**Implementar novas tecnologias** de forma adequada e segura.

**Acompanhar as melhores práticas** do mercado e as recomendações de segurança de órgãos como o NIST e o CIS.

#### **4.3.3.17.1. Justificativa**

Diante da complexa e crítica infraestrutura de TI do CRCES, composta por tecnologias de ponta e interligadas, a contratação de uma empresa especializada para gerar todos esses serviços de TI se torna imprescindível para garantir a segurança, confiabilidade, disponibilidade e bom funcionamento dos sistemas da instituição.

A simples contratação de "qualquer um" para este serviço, sem o devido detalhamento no Termo de Referência, coloca em risco a efetividade da gestão da TI, a segurança dos dados e a própria continuidade das operações do CRCES.

O detalhamento no Termo de Referência, como demonstrado acima, é crucial para:

**a) Assegurar a contratação da empresa mais qualificada e experiente para o serviço.**

**b) Definir claramente as expectativas e responsabilidades de ambas as partes.**

**c) Permitir a avaliação objetiva das propostas e a escolha da melhor solução.**

**d) Facilitar o acompanhamento e a fiscalização do contrato.**

**e) Mitigar riscos e garantir o sucesso da contratação.**

**f) Atender aos princípios da Lei 14.133 e da Administração Pública.**

Portanto, a contratação de um profissional ou empresa sem a devida qualificação e sem o detalhamento adequado no Termo de Referência pode gerar diversos problemas, como:

**a) Falhas na prestação do serviço, comprometendo a segurança, confiabilidade e disponibilidade dos sistemas.**

**b) Aumento de custos com retrabalho, correções e possíveis perdas.**

**c) Dificuldades na comunicação e na resolução de conflitos.**

**d) Dificuldades na fiscalização do contrato e na cobrança de resultados.**

**e) Riscos de inadimplência e de litígios.**

A contratação de uma empresa especializada em gerenciamento de TI para o CRCES exige um Termo de Referência detalhado e abrangente, que defina claramente os requisitos técnicos, as responsabilidades e os níveis de serviço esperados. Essa medida garante a efetividade da contratação, a qualidade dos serviços prestados e a proteção dos interesses da instituição.

#### **4.3.3.18. Softwares que deverão ser disponibilizados**

As ferramentas listadas abaixo (monitoramento e de abertura de chamados) deverão ser disponibilizadas e totalmente configuradas pela CONTRATADA sem custo adicional para o CRCES, e deverão apresentar as seguintes especificações (mínimas):

##### **4.3.3.18.1. Ferramenta de monitoramento.**

**Monitoramento de Rede:** Roteadores, switches, impressoras, etc., utilizando protocolos como SNMP (v1/v2c/v3), ICMP (ping) e verificações de portas TCP/UDP.

**Monitoramento de Servidores:** Desempenho de CPU, uso de memória, espaço em disco, tráfego de rede, processos, serviços e logs.

**Monitoramento de Aplicações e Serviços:** Bancos de dados (MySQL, PostgreSQL, Oracle, etc.), servidores web (Apache, Nginx, IIS), Java applications (JMX), serviços específicos e outros.

**Monitoramento de Virtualização:** Serviços em nuvem, contêineres, máquinas virtuais.

**Monitoramento Web (Web Scenarios):** Simula a navegação de usuários em aplicações web, verificando a disponibilidade, o tempo de resposta e o conteúdo das páginas.

**Monitoramento de Dispositivos IoT e Sensores:** Coleta dados de uma variedade de sensores e dispositivos IoT.

**Monitoramento de Logs e Eventos:** Analisa arquivos de log em busca de padrões, erros, avisos ou atividades suspeitas.

**Extensibilidade:** Permitir a coleta de dados qualquer fonte através de scripts externos personalizados, APIs e extensões.

**Limiares Flexíveis:** Definição de condições personalizadas para identificar problemas (triggers).

**Previsão de Tendências e Machine Learning:** Funções preditivas que permitem prever quando um limiar será atingido, possibilitando ações proativas antes que um problema ocorra.

**Níveis de Severidade:** Classificação dos problemas por níveis de severidade (informação, aviso, médio, alto, desastre), facilitando a priorização.

**Análise de Causa Raiz:** Ajuda a identificar a causa subjacente dos problemas.

**Canais de Notificação Diversos:** Envio de alertas por e-mail, SMS, aplicativos de mensagens (Telegram, Slack, etc.), webhooks e scripts personalizados.

**Escalonamento de Alertas:** Configuração de fluxos de escalonamento para garantir que os alertas cheguem aos destinatários corretos em diferentes etapas.

**Ações Automáticas (Auto-remediação):** Possibilidade de executar comandos remotos automaticamente em resposta a um problema (ex: reiniciar um serviço, executar um script de correção).

**Notificações Customizáveis:** Mensagens de alerta personalizadas com informações relevantes sobre o problema.

**Dashboards Personalizáveis:** Criação de painéis de controle interativos com widgets para exibir métricas em tempo real, status de hosts, problemas, mapas de rede, gráficos e muito mais.

**Gráficos Flexíveis:** Geração de gráficos detalhados para visualizar dados históricos e tendências, com opções de personalização de tempo e exibição.

**Mapas de Rede (Network Maps):** Criação de representações visuais da infraestrutura, mostrando o status dos dispositivos e as interconexões.

**Relatórios:** Geração de relatórios de disponibilidade, desempenho e outros dados relevantes.

**Visão de Negócio (SLA/KPI):** Possibilidade de monitorar o desempenho dos serviços de TI em relação aos Acordos de Nível de Serviço (SLAs) e Indicadores Chave de Desempenho (KPIs).

**Descoberta Automática de Rede (Network Discovery):** Detecta automaticamente novos dispositivos na rede, facilitando a configuração inicial.

**Auto-registro de Agentes (Agent Autoregistration):** Permite que os agentes Zabbix se registrem automaticamente no servidor Zabbix, simplificando a implantação em grande escala.

**Descoberta de Baixo Nível (Low-Level Discovery - LLD):** Descobre automaticamente componentes de um host (ex: interfaces de rede, sistemas de arquivos, CPUs, partições de disco) e cria itens de monitoramento, triggers e gráficos para eles.

**Modelos (Templates):** Reutilização de configurações de monitoramento para diferentes tipos de hosts, agilizando a implantação e padronizando o monitoramento.

**Sistema de Permissões:** Controle granular de acesso baseado em funções e grupos de usuários.

**Autenticação:** Suporte a diferentes métodos de autenticação (interna, LDAP, SAML).

**criptografia:** Criptografia de todo o tráfego de monitoramento para garantir a segurança dos dados.

**Alta Disponibilidade:** Monitoramento contínuo.

#### 4.3.3.18.2. Ferramenta de abertura e gestão de chamados de T.I

**Abertura de chamados por e-mail:** Integração com e-mail para que os chamados sejam criados automaticamente a partir de mensagens enviadas para um endereço específico.

**Categorização e Priorização Automática:** Possibilidade de pré-definir categorias (ex: "Problema de Software", "Solicitação de Hardware", "Acesso"), subcategorias e níveis de prioridade (ex: "Baixa", "Média", "Alta", "Crítica") com base no tipo de solicitação ou no usuário.

**Anexos:** Capacidade de anexar arquivos (screenshots, logs, documentos) para fornecer mais contexto ao chamado.

**Atribuição Automática e Manual:** Atribuição de chamados a agentes ou equipes com base em regras predefinidas (categoria, prioridade, departamento do usuário) ou atribuição manual pelos gerentes.

**Filas de Atendimento:** Organização dos chamados em filas específicas para cada equipe ou tipo de serviço.

**Fluxos de Trabalho (Workflows):** Definição de etapas e ações automatizadas para o ciclo de vida de um chamado (ex: Aberto -> Em Andamento -> Aguardando Usuário -> Resolvido -> Fechado).

**Notificações Automáticas:** Envio de e-mails ou notificações push para o usuário e para os agentes sobre o status do chamado, novas mensagens, resolução, etc.

**Colaboração em Equipe:** Permite que múltiplos agentes trabalhem em um mesmo chamado, com compartilhamento de informações e anotações.

**Macros/Respostas Predefinidas:** Modelos de respostas para perguntas frequentes, agilizando o atendimento.

**Artigos e FAQs:** Repositório central de artigos de solução de problemas, FAQs (perguntas frequentes), guias e procedimentos.

**Busca Inteligente:** Ferramenta de busca robusta que permite aos usuários e agentes encontrar informações relevantes rapidamente.

**Sugestão de Soluções:** Apresentar artigos da base de conhecimento aos usuários enquanto eles digitam seu problema no portal self-service, incentivando a auto-resolução.

**Dashboards e Métricas:** Visualização em tempo real de KPIs (Key Performance Indicators) como número de chamados abertos, chamados resolvidos, tempo médio de resposta, tempo médio de resolução, etc.

resolvidos, tempo médio de resposta, tempo médio de resolução, etc.

**Relatórios Customizáveis:** Geração de relatórios sobre desempenho da equipe, tipos de chamados mais comuns, cumprimento de SLAs, tendências, etc.

**Integração com a ferramenta de Monitoramento:** Integração com a ferramenta de monitoramento proposto pela CONTRATADA, para que alertas de monitoramento possam gerar chamados automaticamente.

**Controle de Acesso Baseado em Funções:** Definição de permissões diferentes para usuários, agentes e administradores.

**Acessibilidade:** Interface amigável e acessível em diferentes dispositivos (desktop, mobile).

#### **SLA (Service Level Agreement) Management:**

Definição de SLAs para diferentes tipos de chamados, especificando tempo de resposta e tempo de resolução esperados.

Monitoramento automático do cumprimento dos SLAs, com alertas e escalonamentos caso os prazos estejam sendo excedidos.

Escalonamento automático para gerentes ou equipes superiores quando os SLAs estão em risco.

Histórico Completo do Chamado: Registro detalhado de todas as interações, atualizações, comentários e mudanças de status em um chamado.

Pesquisa Avançada: Facilidade para buscar chamados por ID, usuário, categoria, palavras-chave, etc.

#### **4.3.3.19. Serviços externos que deverão ser acompanhados pela contratada**

A CONTRATADA será um ponto focal e estratégico para o CRCES, atuando como o principal **elo de coordenação e intermediação** entre nossa instituição e as demais prestadoras de serviços de TI. Dada a complexidade e a interdependência de nossas operações tecnológicas, a **intervenção e o acompanhamento proativo** da CONTRATADA serão cruciais para garantir a fluidez e a eficácia de todas as interações e projetos. Atualmente, gerenciamos diversos contratos com terceiros, e essa carteira de fornecedores poderá se expandir conforme nossas necessidades evoluírem. Abaixo vamos listar alguns dos contratos:

- Serviço de fornecimento de software de gestão integrada (SpiderWare);
- Serviço de hospedagem do website e webservice do CRCES;
- Serviço de fornecimento de link de internet;
- Serviço de fornecimento de e-mail corporativo;
- Serviço de fornecimento de link SIP Trunk;
- Serviço de fornecimento de validador de assinaturas digitais;
- Serviço de fornecimento de atendente virtual por whatsapp;
- Serviço de outsourcing de impressão;
- Serviço de fornecimento de ePABX;

### **5. ESTIMATIVAS DAS QUANTIDADES PARA A CONTRATAÇÃO, ACOMPANHADAS DAS MEMÓRIAS DE CÁLCULO E DOS DOCUMENTOS QUE DÃO SUPORTE;**

5.1 A estimativa de quantidade foi baseada na estrutura de tecnologia atual do CRCES, conforme descrito ao longo deste documento.

### **6. LEVANTAMENTO DE MERCADO, ANÁLISE DAS ALTERNATIVAS POSSÍVEIS E JUSTIFICATIVA TÉCNICA E ECONÔMICA DA ESCOLHA DO T I SOLUÇÃO A CONTRATAR;**

**6.1** O levantamento de mercado para contratação de empresa que preste serviço de gerenciamento de T.I e um processo que requer atenção, cuidado e critério, pois envolve a confiança e a parceria entre o contratante e o contratado.

**6.2** Atualmente, o CRCES enfrenta um cenário desafiador na gestão de T.I, com apenas um funcionário dedicado a essa área. Esta escassez representa um risco significativo para a continuidade dos serviços e para a qualidade do atendimento oferecido aos usuários.

**6.3** Ademais, o CRCES se depara com desafios crescentes, como a necessidade premente de adaptação às normas de governança, a demanda por inovação e modernização tecnológica, bem como a crescente complexidade dos processos e projetos de T.I.

**6.4** Em um ambiente em constante evolução tecnológica, é essencial que o CRCES esteja alinhado com as mais recentes tendências e práticas em T.I. A falta de recursos e expertise interna dificulta a implementação de soluções inovadoras que possam impulsionar a eficiência e a eficácia das operações.

**6.5** O serviço de gerenciamento de T.I são considerados serviços comuns, pois se enquadram na definição de atividades que podem ser prestadas por qualquer pessoa jurídica, sem exigência de qualificação específica ou exclusividade.

**6.6** Uma vez que há diversas empresas que oferecem este serviço, optamos por consultar empresas que já têm experiência com a infraestrutura tecnológica do CRCES, o que nos permite obter uma pesquisa mais adequada à realidade e à necessidade do suporte e serviço que solicitamos no processo, com isso, alcançamos a estimativa descrita abaixo:

	VALOR ITEM I
Mensal	R\$40.000,00
Anual	R\$480.000,00

**6.7** Analisando os orçamentos apresentados, o valor mensal para esta contratação ficou estimado em R\$ 40.000,00 (quarenta mil reais), sendo que o valor total para os 12 (doze) meses resulta no valor de R\$480.000,00 (quatrocentos e oitenta mil reais) para os serviços gerenciados em Tecnologia da Informação.

CC-0. Além disso, a Comissão Permanente de Contabilidade da Prefeitura Santa Helena, com o nº 001/2025, tem a responsabilidade de elaborar o plano de

6.9 Além disso, o Conselho Regional de Contabilidade do Espírito Santo, como órgão público, tem a responsabilidade de zelar pelo uso eficiente dos recursos financeiros. Portanto, a busca pelo menor preço em processos de contratação é uma prática comum para garantir a economicidade e maximizar o retorno sobre o investimento público.

6.10 Outro aspecto relevante é a transparência e a simplificação do processo de licitação proporcionadas pelo critério de "menor preço". Por ser um critério objetivo de verificação, ele facilita a análise das propostas pelos licitantes e pelos responsáveis pela fiscalização, promovendo assim a lisura e a competitividade do certame.

6.10 Por fim, considerando que os **Serviços gerenciados em Tecnologia da Informação** são essenciais para garantir a saúde e a segurança dos ocupantes das instalações do Conselho Regional de Contabilidade, a escolha do critério de "menor preço" permite contar com uma infraestrutura de tecnologia da informação (T.I) eficiente, segura e atualizada, que garanta o bom funcionamento dos sistemas internos e externos, a comunicação com os diversos públicos e a proteção dos dados sensíveis.

6.11 Dessa forma, o uso do critério de "menor preço" no processo de licitação para a contratação de serviços **Tecnologia da Informação** completa é uma escolha justificada e alinhada aos princípios da administração pública, visando garantir a eficiência, a transparência e o melhor aproveitamento dos recursos disponíveis.

## 7. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Conforme documentos acostados aos autos, o valor estimado da contratação mensal é de R\$40.000,00 (quarenta mil reais) perfazendo o valor total de R\$480.000,00 (quatrocentos e oitenta mil reais).

Para fins de estimativa da presente contratação, procedeu-se à pesquisa direta com fornecedores, por meio de solicitação de proposta de preço por e-mail, cujo valor médio é apresentado acima.

A pesquisa está em conformidade com o art. 6º da Instrução Normativa SEGES/ME n.º 65/2021, realizamos a média dos orçamentos.

## 8. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO, INCLUSIVE DAS EXIGÊNCIAS RELACIONADAS À MANUTENÇÃO E À ASSISTÊNCIA TÉCNICA, QUANDO FOR O CASO;

Contratação de empresa especializada na prestação de serviços gerenciados de Tecnologia da Informação para atender às necessidades do Conselho Regional de Contabilidade do Espírito Santo (CRCES) em sua sede em Bento Ferreira, Vitória/ES. Os serviços incluem o fornecimento, instalação e gestão de solução Wi-Fi, instalação e gestão de Firewall de próxima geração, e fornecimento e gestão de backup local e em nuvem. A empresa será responsável pela gestão completa da infraestrutura de redes (LAN, VLAN e WLAN), abrangendo ativos de rede, computadores, nobreaks, servidores e monitores. O escopo contempla suporte técnico remoto e presencial para uma localidade, até 60 estações de trabalho (físicas ou virtuais), até 5 servidores físicos e 12 servidores virtuais. Adicionalmente, serão realizados a gestão e manutenção do banco de dados em SQL Server, a manutenção preventiva e corretiva de todo o parque de TI, a gestão e o monitoramento dos links de internet, e a gestão e manutenção da infraestrutura hiperconvergente.

Na descrição da solução, já estão incluídos todos os procedimentos, equipamentos, instalação e manutenções corretivas para a perfeita execução dos serviços.

## 9. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO;

A não viabilidade de parcelamento da solução se fundamenta na natureza integrada do objeto, que demanda uma abordagem unificada para garantir eficiência e consistência. Optar por consolidar os serviços em um único item considerou a coesão dos elementos a serem licitados e a sequência lógica de sua execução.

Adicionalmente, a fragmentação deste processo acarretaria à Administração um risco significativo, pois diferentes empresas, embora possam operar no mesmo setor, apresentam disparidades estruturais, logísticas e econômico-financeiras. Tal divisão resultaria em capacidades discrepantes de prestação de serviço, comprometendo a supervisão e expondo a execução dos contratos a possíveis desvios dos padrões estabelecidos.

Portanto, a decisão de não parcelar a contratação busca assegurar a coerência e a qualidade na entrega dos serviços, minimizando potenciais incongruências e garantindo a conformidade na execução do objeto.

## 10. RESULTADOS PRETENDIDOS EM TERMOS DE ECONOMICIDADE E DE MELHOR APROVEITAMENTO DOS RECURSOS HUMANOS, MATERIAIS E FINANCEIROS;

Pretende-se com a presente contratação, os resultados abaixo descritos:

- Aumentar a eficiência e a segurança dos sistemas de informação do CRCES, reduzindo os riscos de falhas, perdas ou vazamentos de dados.
- Garantir a continuidade das atividades do CRCES em caso de eventuais problemas técnicos, desastres naturais ou ataques cibernéticos, por meio de um plano de recuperação de desastres baseado em backup em nuvem.
- Otimizar os custos e os recursos do CRCES, evitando gastos desnecessários com infraestrutura, manutenção e atualização de equipamentos e softwares.
- Melhorar o atendimento e a satisfação dos profissionais da contabilidade e da sociedade em geral, oferecendo serviços de qualidade, rapidez e confiabilidade.

## 11. PROVIDÊNCIAS A SEREM ADOTADAS PELA ADMINISTRAÇÃO PREVIAMENTE À CELEBRAÇÃO DO CONTRATO

Para a execução do objeto deste estudo, não há necessidade de nenhuma adequação do ambiente do órgão.

## 12. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES;

Para o objeto deste estudo, não são necessárias contratações correlatas ou interdependentes.

## 13. DESCRIÇÃO DE POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS, QUANDO APLICÁVEL;



Não se aplica a esta contratação.

#### 14. POSICIONAMENTO CONCLUSIVO SOBRE A ADEQUAÇÃO DA CONTRATAÇÃO PARA O ATENDIMENTO DA NECESSIDADE A QUE SE DESTINA.

Diante da complexa e crítica infraestrutura de TI do CRCES, composta por tecnologias de ponta e interligadas, a contratação de uma empresa especializada em gerenciamento de TI se torna imprescindível para garantir a segurança, confiabilidade, disponibilidade e bom funcionamento dos sistemas da instituição.

A simples contratação de "qualquer um" para este serviço, sem o devido detalhamento no Termo de Referência, coloca em risco a efetividade da gestão da TI, a segurança dos dados e a própria continuidade das operações do CRCES.

O detalhamento no Termo de Referência, como demonstrado acima, é crucial para:

- a. Assegurar a contratação da empresa mais qualificada e experiente para o serviço.
- b. Definir claramente as expectativas e responsabilidades de ambas as partes.
- c. Permitir a avaliação objetiva das propostas e a escolha da melhor solução.
- d. Facilitar o acompanhamento e a fiscalização do contrato.
- e. Mitigar riscos e garantir o sucesso da contratação.
- f. Atender aos princípios da Lei 14.133 e da Administração Pública.
- g. Portanto, a contratação de um profissional ou empresa sem a devida qualificação e sem o detalhamento adequado no Termo de Referência pode gerar diversos problemas, como:
  - h. Falhas na prestação do serviço, comprometendo a segurança, confiabilidade e disponibilidade dos sistemas.
  - i. Aumento de custos com retrabalho, correções e possíveis perdas.
  - j. Dificuldades na comunicação e na resolução de conflitos.
  - k. Dificuldades na fiscalização do contrato e na cobrança de resultados.
  - l. Riscos de inadimplência e de litígios.
- m. Em suma, a contratação de uma empresa especializada em gerenciamento de TI para o CRCES exige um Termo de Referência detalhado e abrangente, que defina claramente os requisitos técnicos, as responsabilidades e os níveis de serviço esperados. Essa medida garante a efetividade da contratação, a qualidade dos serviços prestados e a proteção dos interesses da instituição.
- n. Investir em um Termo de Referência bem elaborado é um investimento na segurança, confiabilidade e no sucesso da gestão da TI do CRCES.
- o. Além disso, essa medida promove transparência e integridade, uma vez que impede o envolvimento de terceiras partes que possam diluir a responsabilidade direta da contratada. A restrição à exploração industrial visa, ainda, assegurar que o objeto seja destinado exclusivamente ao cumprimento das finalidades públicas, sem desvios para utilização comercial ou industrial que contrariem o interesse público.
- p. Para comprovação de capacidade, deve exigir-se que os licitantes apresentem atestados técnicos que demonstrem a execução dos serviços com infraestrutura própria e sem uso de exploração industrial, atendendo assim ao critério de "estrutura própria" e garantindo os altos padrões esperados.

Com base nas informações estabelecidas neste documento, nas justificativas apresentadas no Documento de Formalização da Demanda – DFD, a Equipe de Planejamento DECLARA a viabilidade da contratação de empresa especializada, Serviços de TI inclui a gestão de redes, ativos de rede, servidores, estações de trabalho, nobreaks e monitores. A empresa será responsável por suporte técnico remoto e presencial, manutenção preventiva e corretiva, e monitoramento de links de internet e infraestrutura hiperconvergente.

#### 15. Normativos que disciplinam o serviço a ser contratado:

[Lei nº 14.133](#), de 1º de abril de 2021 - Lei de Licitações e Contratos Administrativos.

[Decreto nº 10.947](#), de 25 de janeiro de 2022 - Regulamenta o inciso VII do caput do art. 12 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o plano de contratações anual e instituir o Sistema de Planejamento e Gerenciamento de Contratações no âmbito da administração pública federal direta, autárquica e fundacional.

[Decreto nº 7.174](#), de 12 de maio de 2010 - Regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União.

[Instrução Normativa SGD/MGI nº 6](#) de 29 de março de 2023 - Regulamenta os requisitos e procedimentos para aprovação de contratações ou de formação de atas de registro de preços, a serem efetuados por órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISIP do Poder Executivo federal, relativos a bens e serviços de tecnologia da informação e comunicação - TIC.

[Instrução Normativa SGD/ME nº 94](#) de 23 de dezembro de 2022 - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISIP do Poder Executivo Federal.

[Instrução Normativa SLTI nº 01](#), de 19 de janeiro de 2010 - Dispõe sobre os critérios de sustentabilidade ambiental na aquisição de bens, contratação de serviços ou obras pela Administração Pública Federal direta, autárquica e fundacional e dá outras providências;

#### 16. Do Acesso às Informações contidas nos presentes Estudos Preliminares:

Nos termos da Lei nº 12.527, de 18 de novembro de 2011, esta Equipe de Planejamento entende que:

<input checked="checked" type="checkbox"/>	As informações contidas nos presentes Estudos Preliminares <b>DEVERÃO ESTAR DISPONÍVEIS</b> para qualquer interessado, pois não se caracterizam como sigilosas.
<input type="checkbox"/>	As informações contidas nos presentes Estudos Preliminares <b>ASSUMEM CARÁTER SIGILOSOS</b> , nos termos do Art. 23 da Lei nº 12.527/2011, e, portanto, deverão ter acesso restrito.
<input type="checkbox"/>	

**17. Equipe de Planejamento:**

São responsáveis pela elaboração do presente documento que materializa os Estudos Preliminares da presente contratação os seguintes servidores:

<b>Wekson José Barbieri Mariano</b> Matrícula 87 Membro da Equipe de Planejamento	<b>Elaine Leopoldino Ferreira</b> Matrícula 198 Membro da Equipe de Planejamento	<b>Vanessa Covre Rangel Marques</b> Matrícula 140 Membro da Equipe de Planejamento
---	--	--



Documento assinado eletronicamente por **Elaine Leopoldino Ferreira, Coordenadora**, em 06/10/2025, às 13:39, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Wekson José Barbieri Mariano, Analista - Sistemas / Desenvolvimento**, em 06/10/2025, às 13:47, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Vanessa Covre Rangel Marques, Coordenadora**, em 07/10/2025, às 09:20, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site [https://sei.cfc.org.br/sei/controlador\\_externo.php?acao=documento\\_conferir&id\\_orgao\\_acesso\\_externo=0](https://sei.cfc.org.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **1052670** e o código CRC **0ABEFA74**.