



CONSELHO REGIONAL DE CONTABILIDADE DO ESPÍRITO SANTO  
Rua Amélia da Cunha Ornelas, 30, - Bairro Bento Ferreira, Vitória/ES, CEP 29050-620  
Telefone: (27) 3232-1600 - [www.crc-es.org.br](http://www.crc-es.org.br) E-mail: [diretoria@crc-es.org.br](mailto:diretoria@crc-es.org.br)

## **NLL - TERMO DE REFERENCIA DE TIC**

Processo nº 9079618110000798.000048/2025-57

### **1. DEFINIÇÃO DO OBJETO**

- 1.1. 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, tudo em conformidade com as condições e exigências estabelecidas neste instrumento.
- 1.2. O(s) serviço(s) objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.
- 1.3. O prazo de vigência da contratação é de 12 (doze) meses contados dos da assinatura, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021.
- 1.3.1. O presente serviço é enquadrado como continuado tendo em vista as especificações constantes em Estudo Técnico Preliminar;
- 1.4. O detalhamento necessário quanto ao período de vigência constará em instrumento contratual .

### **2. FUNDAMENTAÇÃO DA CONTRATAÇÃO**

- 2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares.

### **3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO, CONSIDERADO O CICLO DE VIDA DO OBJETO**

- 3.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares

### **4. REQUISITOS DA CONTRATAÇÃO**

#### **4.1. Sustentabilidade**

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

#### **4.2. Garantia da contratação**

4.2.1. Não haverá exigência da garantia da contratação dos [artigos 96 e seguintes da Lei nº 14.133, de 2021](#), tendo em vista que o pagamento pelos serviços somente será realizado após a referida prestação e atesto pelo fiscal de contrato. Além disso, em caso de problema que se apresente posteriormente, o CRCES poderá instaurar procedimento administrativo sancionador com base na legislação vigente.

#### **4.3. Vistoria**

4.3.1. Para o correto dimensionamento e elaboração de sua proposta, o licitante poderá realizar vistoria nas instalações do local de execução dos serviços, acompanhado por servidor designado para esse fim, de segunda à sexta-feira, das 09 horas às 16 horas, devendo o agendamento ser efetuado previamente pelo e-mail: [administrativo@crc-es.org.br](mailto:administrativo@crc-es.org.br).

4.3.2. O prazo para vistoria iniciar-se-á no dia útil seguinte ao da publicação do Edital, estendendo-se até o dia útil anterior à data prevista para a abertura da sessão pública.

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

4.3.4. 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.

4.3.5. A não realização da vistoria, quando facultativa, não poderá embasar posteriores alegações de desconhecimento das instalações, dúvidas ou esquecimentos de quaisquer detalhes dos locais da prestação dos serviços, devendo o contratado assumir os ônus dos serviços decorrentes.

#### **4.4. Local e horário da prestação dos serviços**

4.4.1. Os serviços serão prestados na sede do CRCES, localizada na Rua Amélia da Cunha Ornelas, nº 30, Bairro Bento Ferreira, Vitória/ES – CEP: 29.050-620 Rotinas a serem cumpridas.

#### **4.5. Materiais a serem disponibilizados**

4.5.1. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar os materiais, equipamentos, ferramentas e utensílios necessários, nas quantidades estimadas e qualidades a seguir estabelecidas, promovendo sua substituição quando necessário.

#### **4.6. Informações relevantes para o dimensionamento da proposta**

4.6.1. 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.

4.6.2. 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).

4.6.3. 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.

#### **4.7. Especificação da garantia do serviço (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021)**

4.7.1. O prazo de garantia contratual dos serviços é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

#### **4.8. Procedimentos de transição e finalização do contrato**

4.8.1. Apresentar relatório final de atividades, contendo o resumo dos serviços executados, as ocorrências técnicas registradas, pendências identificadas e orientações para continuidade da operação da infraestrutura de TI, incluindo rede, segurança da informação, backup e suporte.

4.8.2. Entregar toda a documentação técnica e operacional produzida durante a execução do contrato, em meio físico e/ou digital, de forma organizada, classificada e atualizada, contemplando registros de configuração de equipamentos, scripts, inventários, diagramas de rede, manuais operacionais e demais documentos que garantam a rastreabilidade e integridade das informações

4.8.3. Transferir conhecimentos e informações relevantes ao(s) servidor(es) designado(s) pela Administração, por meio de reuniões técnicas, relatórios explicativos e capacitação operacional, com foco nos processos relacionados à infraestrutura de redes, segurança da informação, monitoramento e procedimentos de contingência

4.8.4. Assegurar a continuidade dos serviços durante eventual período de transição contratual, caso haja nova contratação em andamento, por prazo acordado com a Administração, a fim de garantir a operação ininterrupta dos serviços essenciais de tecnologia da informação.

4.8.5. Restituir, quando aplicável, equipamentos, materiais, documentos, credenciais, acessos a sistemas e demais bens disponibilizados pela contratante ao longo do contrato.

4.8.6. Emitir declaração formal de encerramento das obrigações contratuais, condicionada à aceitação pela fiscalização e à inexistência de pendências técnicas ou administrativas, comprovando a plena execução dos serviços contratados e a entrega dos produtos finais previstos. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

## **5. MODELO DE EXECUÇÃO DO OBJETO**

5. A execução do objeto seguirá a seguinte dinâmica:

5.1.1. Início da execução do objeto: 5 (cinco) dias da emissão da ordem de serviço;

5.1.2. Descrição detalhada dos métodos, rotinas, etapas, tecnologias procedimentos, frequência e periodicidade de execução do trabalho:

5.1.3. Cronograma de realização dos serviços:

## **6. CARACTERÍSTICAS DA SOLUÇÃO:**

### **6.1. ESTUDO DA SOLUÇÃO DE ACESSO VIA WI-FI.**

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

6.1.2. 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.

6.1.3. 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.

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

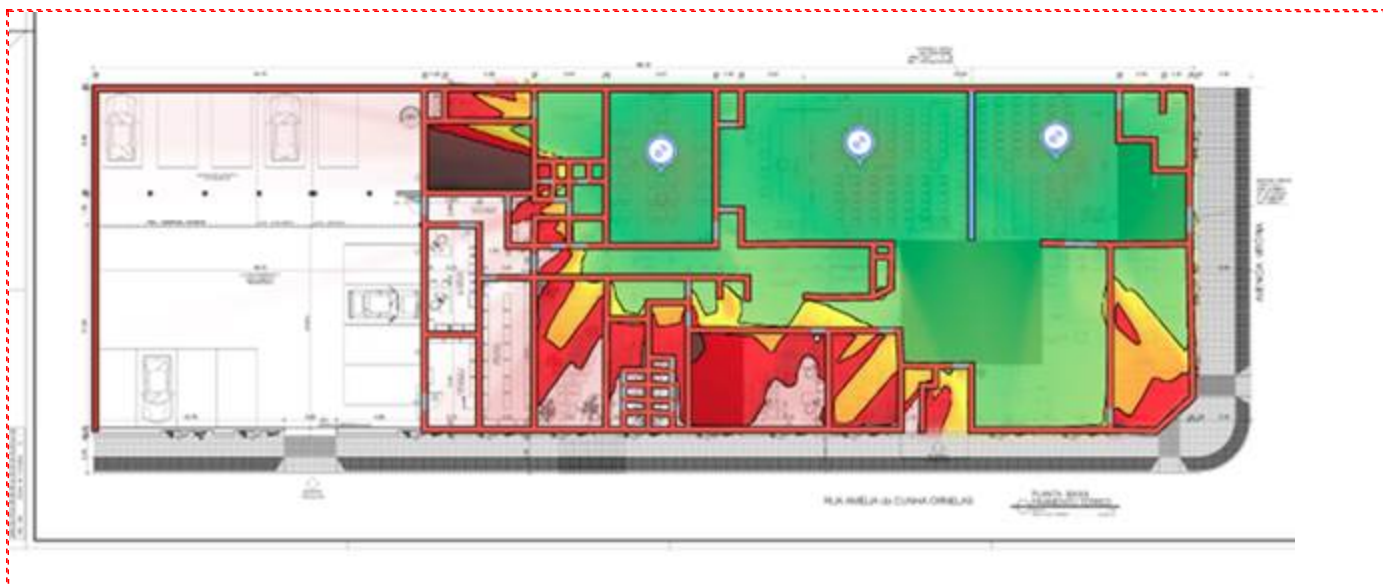
6.1.5. Ainda, será exigida a garantia de toda a solução, compreendendo assistência técnica on-site fornecida pelo fabricante, atualizações de software e firmware dos produtos, manutenção, configuração e monitoramento 24x7, durante toda a vigência da contratação.

6.1.6. 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.

## 6.2. Site Survey Preliminar

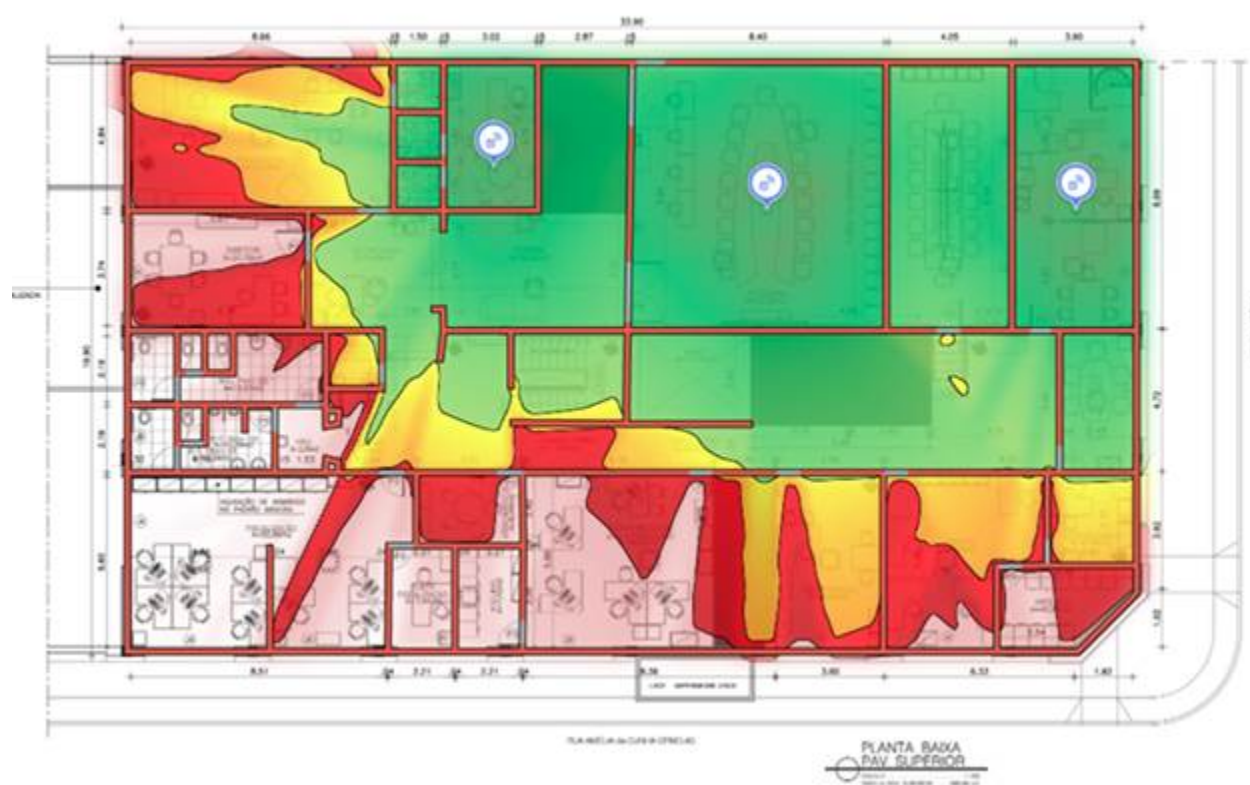
6.2.1. Para a definição da quantidade de equipamentos necessários, o CRCES realizou um levantamento de campo (site survey) preliminar, cujos resultados são apresentados a seguir:

### a) Pavimento térreo - 09 equipamentos

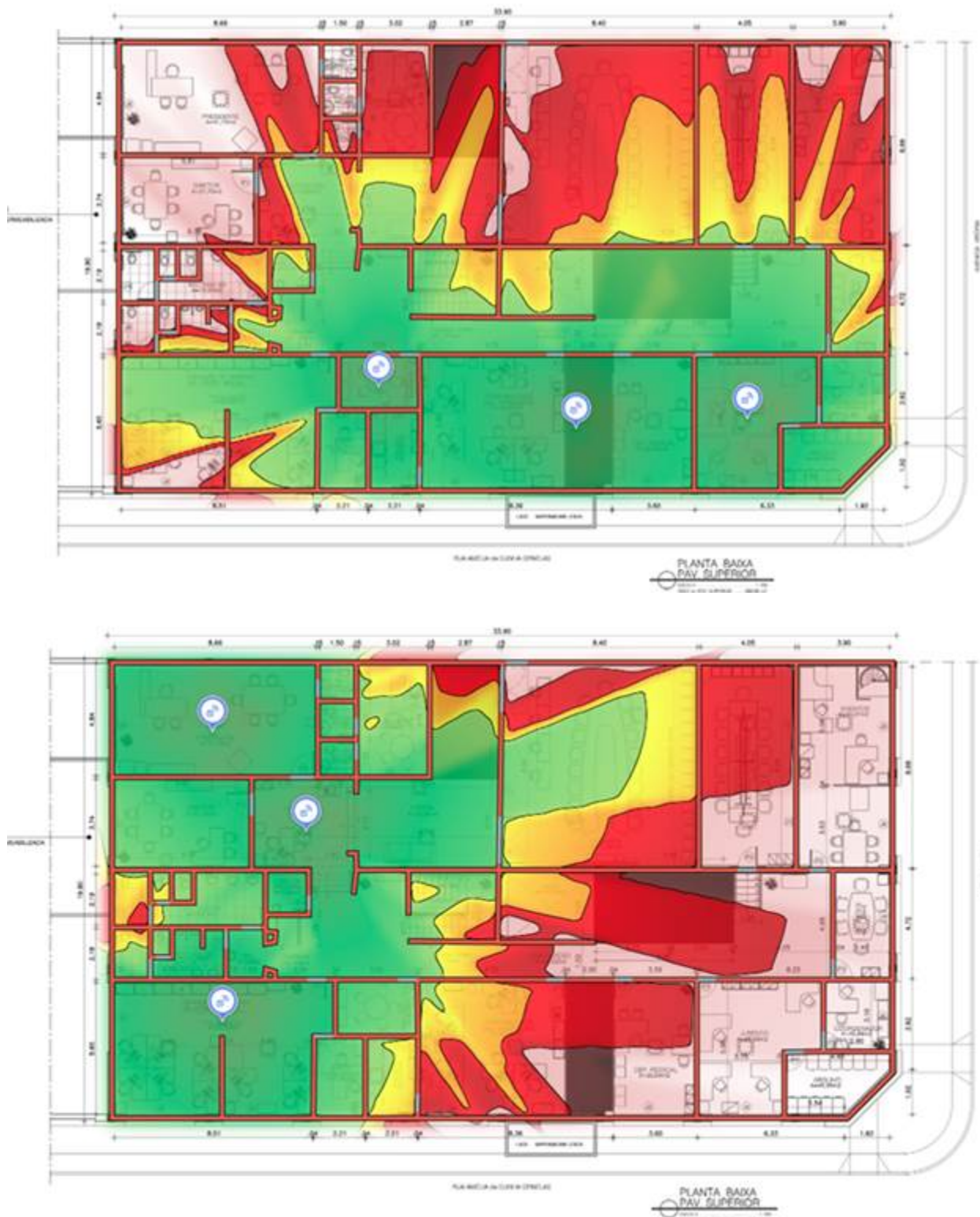




b) Pavimento superior - 09 equipamentos







## 6.2.2. ESTUDO DOS SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3

### 6.2.2.1. Definição do objeto

6.2.2.2. Contratação 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 de acordo com a tabela abaixo:

TIPO	DESCRIÇÃO	QUANTIDADE
Virtualizador	Hyper-V	05
Servidor c/ Windows Server 2022	Dell PowerEdge R640	02
Servidor c/ Windows Server 2022	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
Solução de acesso à internet via Wi-Fi	Conforme item 1 do Termo de referência	
Solução de segurança FWaaS	Conforme item 2 do Termo de referência	
Solução de backup Cooperativo	Conforme item 3 do Termo de referência	

## 7. Definição dos itens.

ITEM	SUBITEM	CATSER	DESCRIÇÃO	DESCRIÇÃO COMPLEMENTAR	UNIDADE DE MEDIDA	QUANTIDADE
01	01	30710	SOLUÇÃO DE ACESSO A INTERNET VIA WI-FI.	Fornecimento e instalação de uma rede corporativa Wi-Fi completa.	Mês	12
	02	30736	SOLUÇÃO DE SEGURANÇA FWaaS	Instalação e gestão de Firewall de Próxima Geração, conforme termo de referência.	Mês	12
	03	30744	SOLUÇÃO DE BACKUP CORPORATIVO	Implementação e de solução de backup local e em nuvem.	Mês	12
	04	30728	SERVIÇOS CONTINUADOS DE SUPORTE N1,N2 E N3	Suporte técnico avançado (remoto e presencial) conforme termo de referência	Mês	12

## 8. Descrição técnica dos itens:

### 8.1. SOLUÇÃO DE ACESSO A INTERNET VIA WI-FI.

#### 8.1.1. Características da solução

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

8.1.1.2. 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.

8.1.1.3. 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.

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

8.1.1.5. 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

8.1.1.6. 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.

8.1.1.7. 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.

## **8.1.2. Características dos pontos de acesso à internet via Wifi.**

8.1.2.1. 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;

8.1.2.2. Deve ser compatível e gerenciado pelo equipamento que está incluso no ITEM “Solução de segurança FWaaS (Firewall como serviço). deste termo ou por solução do mesmo fabricante que possua gerência centralizada;

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

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

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

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

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

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

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

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

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

8.1.2.12. 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;

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

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

8.1.2.15. 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;

8.1.2.16. 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;



- 8.1.2.17. 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;
- 8.1.2.18. 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;
- 8.1.2.19. 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;
- 8.1.2.20. Deve permitir operação em modo Mesh;
- 8.1.2.21. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências;
- 8.1.2.22. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio;
- 8.1.2.23. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL);
- 8.1.2.24. Deve suportar OFDMA;
- 8.1.2.25. 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;
- 8.1.2.26. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID;
- 8.1.2.27. Deve suportar BSS Coloring;
- 8.1.2.28. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz;
- 8.1.2.29. Deve suportar operação em 6GHz com canais de 20, 40, 80 e 160MHz;
- 8.1.2.30. Deve possuir sensibilidade mínima de -93dBm quando operando em 5GHz com MCS0 (HT20);
- 8.1.2.31. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz;
- 8.1.2.32. Deve possuir antenas internas ao equipamento com ganho mínimo de 5dBi em 5GHz e 6GHz;
- 8.1.2.33. 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;
- 8.1.2.34. 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;
- 8.1.2.35. 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;
- 8.1.2.36. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps;
- 8.1.2.37. Em conjunto com o controlador wireless, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS);
- 8.1.2.38. 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;
- 8.1.2.39. Em conjunto com o controlador wireless, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- 8.1.2.40. Em conjunto com o controlador wireless, deve ser compatível e implementar o método de autenticação WPA3;
- 8.1.2.41. 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;
- 8.1.2.42. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

- 8.1.2.43. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
- 8.1.2.44. 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;
- 8.1.2.45. 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;
- 8.1.2.46. Deve implementar o padrão IEEE 802.11e;
- 8.1.2.47. Deve implementar o padrão IEEE 802.11h;
- 8.1.2.48. Deve implementar o padrão IEEE 802.3az;
- 8.1.2.49. Deve suportar ser gerenciado via SNMP;
- 8.1.2.50. Deve suportar consultas via REST API;
- 8.1.2.51. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;
- 8.1.2.52. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45º C;
- 8.1.2.53. Deve possuir sistema antifurto do tipo Kensington Security Lock ou similar;
- 8.1.2.54. Deve possuir indicadores luminosos (LED) para indicação de status;
- 8.1.2.55. O ponto de acesso deverá ser compatível e ser gerenciado pelos controladores wireless deste processo;
- 8.1.2.56. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;
- 8.1.2.57. Deve possuir certificado emitido pela Wi-Fi Alliance;
- 8.1.2.58. Deve estar homologado pela ANATEL na data de execução do pregão;
- 8.1.2.59. Deve ser licenciado para uso pelo período de duração da contratação.
- 8.1.2.60. Deve possuir garantia para uso pelo período de duração da contratação.
- 8.1.2.61. 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

### **8.1.3. Características do equipamento controlador de pontos de acesso Wifi;**

- 8.1.3.1. Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI;
- 8.1.3.2. 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);
- 8.1.3.3. 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;
- 8.1.3.4. Deverá implementar os padrões IEEE 802.3af (Power over Ethernet – PoE) e IEEE 802.3at (Power over Ethernet Plus – PoE+) com PoE budget de 370W em 24 portas;
- 8.1.3.5. 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;
- 8.1.3.6. Deve possuir 1 (uma) interface USB;
- 8.1.3.7. Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 190 Mpps (milhões de pacotes por segundo);
- 8.1.3.8. Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q;
- 8.1.3.9. Deve possuir tabela MAC com suporte a 32.000 endereços;
- 8.1.3.10. Deve operar com latência igual ou inferior à 1us (microsegundo);
- 8.1.3.11. Deve implementar Flow Control baseado no padrão IEEE 802.3X;
- 8.1.3.12. Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo

com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP);

8.1.3.13. Deve suportar a comutação de Jumbo Frames;

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

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

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

8.1.3.17. Deve implementar serviço de DHCP Relay;

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

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

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

8.1.3.21. 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;

8.1.3.22. 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;

8.1.3.23. 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;

8.1.3.24. 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;

8.1.3.25. 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;

8.1.3.26. 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;

8.1.3.27. 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;

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

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

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

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

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

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

8.1.3.34. 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;

8.1.3.35. 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;

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

8.1.3.37. Deve suportar MAC Authentication Bypass (MAB);

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

8.1.3.39. 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;

- 8.1.3.40. Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado;
- 8.1.3.41. 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;
- 8.1.3.42. Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP;
- 8.1.3.43. Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6;
- 8.1.3.44. 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;
- 8.1.3.45. 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);
- 8.1.3.46. 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;
- 8.1.3.47. Deve suportar o protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol) para a sincronização do relógio;
- 8.1.3.48. Deve suportar o envio de mensagens de log para servidores externos através de syslog;
- 8.1.3.49. Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3;
- 8.1.3.50. Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface);
- 8.1.3.51. Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web;
- 8.1.3.52. Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS);
- 8.1.3.53. Deve permitir ser gerenciado através de IPv6;
- 8.1.3.54. Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch;
- 8.1.3.55. Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento;
- 8.1.3.56. 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;
- 8.1.3.57. Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab;
- 8.1.3.58. 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;
- 8.1.3.59. Deverá suportar ser configurado e monitorado através de REST API;
- 8.1.3.60. Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE);
- 8.1.3.61. Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch;
- 8.1.3.62. Deve suportar temperatura de operação de até 45º Celsius;
- 8.1.3.63. Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos;
- 8.1.3.64. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V e 220V;
- 8.1.3.65. 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;
- 8.1.3.66. Deve ser licenciado para uso pelo período de duração da contratação.
- 8.1.3.67. Deve possuir garantia para uso pelo período de duração da contratação.
- 8.1.3.68. 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

#### **8.1.4. Requisitos da instalação da solução de acesso à internet via Wi-Fi.**

##### **8.1.4.1. Implementação física.**

##### **8.1.4.1.1. Pontos de acesso:**

##### **8.1.4.1.1.1. Serviço de Implementação para rede WLAN8**

8.1.4.1.1.2. 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 3 total, sendo observada a quantidade mínima estabelecida pela DTIC,

8.1.4.1.1.3. Os serviços serão realizados em horário de expediente (07:30 as 16:30) presencialmente nas dependências da CONTRATANTE;

8.1.4.1.1.4. 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;

##### **8.1.4.1.1.5. Requisitos gerais de Implantação**

8.1.4.1.1.6. 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.

8.1.4.1.1.7. Será realizada instalação física conforme a necessidade da contratante.

8.1.4.1.1.8. O ponto de acesso wifi deverá ser fixado no teto ou parede.

8.1.4.1.1.9. 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.

##### **8.1.4.1.2. Controlador de pontos de acesso:**

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

8.1.4.1.2.2. 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;

##### **8.1.4.1.3. Requisitos para instalação do cabeamento:**

8.1.4.1.3.1. Fornecedor e instalação de cabeamento de rede categoria 6 ou superior, certificado para aplicações PoE;

8.1.4.1.3.2. Lançamento dos cabos partindo do switch PoE instalado em rack padrão até os pontos de instalação dos APs conforme planta fornecida;

8.1.4.1.3.3. Conectorização e crimpagem dos cabos em ambos os extremos;

8.1.4.1.3.4. Instalação de caixas de superfície ou embutidas nos pontos de acesso;

8.1.4.1.3.5. Fixação dos APs no teto ou parede, de acordo com o projeto de cobertura de sinal;

8.1.4.1.3.6. Teste de continuidade e certificação com laudo de todos os pontos instalados;

8.1.4.1.3.7. Organização e identificação dos cabos e pontos conforme padrão TIA/EIA-606;

8.1.4.1.3.8. Garantia de funcionamento da alimentação elétrica via PoE e comunicação de rede para cada ponto.

##### **8.1.4.2. Implementação lógica.**

##### **8.1.4.2.1. Pontos de acesso:**

8.1.4.2.1.1. 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

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

8.1.4.2.1.3. Cadastro das subscrições dos APs na plataforma de gerência;

8.1.4.2.1.4. Endereçamento e segmentação das Redes WIRELESS;

8.1.4.2.1.5. 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);

- 8.1.4.2.1.6. Definição de políticas de bloqueio e permissão de acesso;
- 8.1.4.2.1.7. Instalação da versão mais atual de software (firmware) recomendada pelo fabricante;
- 8.1.4.2.1.8. Configuração de Endereços/Interfaces de Gerência;
- 8.1.4.2.1.9. Endereçamento IP, Telnet Seguro (SSH), Web (HTTP/HTTPS),
- 8.1.4.2.1.10. Parâmetros SNMP para monitoração/gerência remota;
- 8.1.4.2.1.11. Configuração de Syslog, quando aplicável;
- 8.1.4.2.1.12. Configuração de redes locais (VLANs);
- 8.1.4.2.1.13. Configuração de redes locais (SSIDs);
- 8.1.4.2.1.14. Configuração de sincronismo de hora NTP ou SNTP;
- 8.1.4.2.1.15. Controle de acesso de usuários a rede através do padrão 802.1x integrado ao Microsoft Active Directory e a plataforma de controle de acesso.
- 8.1.4.2.1.16. Configuração de alarmes e notificações automatizadas via SNMP e/ou SMTP, quando aplicável;
- 8.1.4.2.1.17. Configurar os SSIDs (Locais e Convidados) para as redes conforme planejamento de rede previamente estabelecido;
- 8.1.4.2.1.18. Configurações de grupos de ponto de acesso;
- 8.1.4.2.1.19. Configuração de algoritmo de criptografia a ser utilizado;
- 8.1.4.2.1.20. Configurações de autenticação 802.1x (Active Directory) conforme planejamento de rede previamente estabelecido;
- 8.1.4.2.1.21. Identificar os pontos de acesso por localização conforme survey realizado;
- 8.1.4.2.1.22. Configuração de segurança de rede;
- 8.1.4.2.1.23. Realizar testes de desempenho de RF dos pontos de acesso wireless;
- 8.1.4.2.1.24. Adequar o posicionamento de pontos de acesso da solução instalada;
- 8.1.4.2.1.25. Configuração de alertas ou alarmes críticos, de acordo com definições feitas na fase de planejamento;
- 8.1.4.2.1.26. Emissão de relatórios de implantação contendo:
- 8.1.4.2.1.27. Mapas de rede,
- 8.1.4.2.1.28. Relação de equipamentos implantados,
- 8.1.4.2.1.29. Configurações feitas nos softwares;
- 8.1.4.2.1.30. Resultado dos testes realizados;

#### **8.1.4.2.2. Controlador de pontos de acesso:**

- 8.1.4.2.2.1. Instalação da versão mais atual de software (firmware) recomendada pelo fabricante;
- 8.1.4.2.2.2. Configuração de Endereços/Interfaces de Gerência;
- 8.1.4.2.2.3. Endereçamento IP;
- 8.1.4.2.2.4. Telnet, se necessário;
- 8.1.4.2.2.5. Secure Shell (SSH), se necessário;
- 8.1.4.2.2.6. Web (HTTP), se necessário;
- 8.1.4.2.2.7. Restrições (Filtros/ACLs) de Acesso;
- 8.1.4.2.2.8. Autenticação;
- 8.1.4.2.2.9. Parâmetros SNMP para monitoração/gerência remota;
- 8.1.4.2.2.10. Configuração de redes locais (VLANs);
- 8.1.4.2.2.11. Configuração de sincronismo de hora NTP ou SNTP;
- 8.1.4.2.2.12. Configuração do protocolo Rapid Spanning Tree (RSTP);
- 8.1.4.2.2.13. Configuração de BPDU GUARD;
- 8.1.4.2.2.14. Configuração de Root Spanning Tree;
- 8.1.4.2.2.15. Interfaces de roteamento IP;
- 8.1.4.2.2.16. Protocolos de roteamento dinâmico OSPF, conforme Projeto de Rede elaborado;
- 8.1.4.2.2.17. Implementação de interfaces IP com Virtual Redundancy Router Protocol (VRRP), se aplicável;
- 8.1.4.2.2.18. Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado;
- 8.1.4.2.2.19. Otimização da Solução
- 8.1.4.2.2.20. Aplicar as melhores práticas e configurar para que o equipamento seja gerenciado pela

plataforma de gerenciamento unificado.

- 8.1.4.2.2.21. Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido;
- 8.1.4.2.2.22. Criação de Vlan, tantas necessárias ao ambiente de acordo com as definições do projeto;
- 8.1.4.2.2.23. Criação dos Roteamentos de Vlan, tantos necessários de acordo com as definições do projeto
- 8.1.4.2.2.24. Ativação de recursos para o controle de broadcast storms;
- 8.1.4.2.2.25. Implementação dos recursos de qualidade de serviço (QoS), conforme Projeto de Rede elaborado;
- 8.1.4.2.2.26. Implementação de filtros ou Access Control Lists para bloqueio de tráfego desnecessário ou indevido;
- 8.1.4.2.2.27. Controle de acesso a rede através do padrão IEEE 802.1x;
- 8.1.4.2.2.28. Instalação dos módulos de gerência ofertados, e todos outros componentes necessários para o seu funcionamento;
- 8.1.4.2.2.29. Configuração de DHCP Snooping;
- 8.1.4.2.2.30. Configuração de DHCP Relay;
- 8.1.4.2.2.31. Configuração de interface confiável ( trust Interface);
- 8.1.4.2.2.32. Configuração de alertas ou alarmes críticos, para cada ativo mapeado, de acordo com definições feitas na fase de planejamento.
- 8.1.4.2.2.33. Configurações dos perfis de acesso à rede baseadas na Política de Segurança;
- 8.1.4.2.2.34. Criação e ativação de regras de acesso e perfis de acesso à rede;
- 8.1.4.2.2.35. Configuração de parâmetros de qualidade de serviço (QoS);
- 8.1.4.2.2.36. Configuração das políticas acesso para a rede dos usuários, integrados com a base LDAP/RADIUS e TACACS existente;
- 8.1.4.2.2.37. Distribuição, ativação e testes das políticas de acesso nos switches fornecidos;
- 8.1.4.2.2.38. Criação de filtros e/ou ACLs (Access Control Lists) de acordo com a política;
- 8.1.4.2.2.39. Ativação e teste das ACLs nos equipamentos fornecidos;
- 8.1.4.2.2.40. Homologação
- 8.1.4.2.2.41. Certificação final da solução, mediante testes de comunicação e apresentação de relatórios com os dados gerados.
- 8.1.4.2.2.42. Documentação em formato PDF contendo os itens a seguir:
- 8.1.4.2.2.43. As-Built completo do projeto, assinada pelo responsável técnico pela execução e Gerente de Projeto.
- 8.1.4.2.2.44. Arquivos de configuração dos ativos de rede;
- 8.1.4.2.2.45. Backup das configurações dos softwares utilizados;
- 8.1.4.2.2.46. Imagens das versões de software implantadas nos ativos de rede quando de sua entrega.

## **8.2. Solução de segurança FWaaS (Firewall como serviço).**

### **8.2.1. Características da solução.**

- 8.2.1.1. A solução proposta abrange a contratação de serviços especializados para a implementação e gestão de um firewall de próxima geração (NGFW).
- 8.2.1.2. O objetivo é assegurar a proteção, o monitoramento e o controle da infraestrutura de TI do CRCES.
- 8.2.1.3. 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.
- 8.2.1.4. 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.
- 8.2.1.5. Deverá ser fornecido os equipamentos, cabeamento e pontos de rede necessários para o

pleno funcionamento da solução

8.2.1.6. 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

8.2.1.7. 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.

8.2.1.8. 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

## **8.2.2. Requisitos técnicos dos equipamentos que compõe a solução:**

### **8.2.2.1. Características simplificadas:**

8.2.2.1.1. Deve suportar, no mínimo, 1 Gbps de throughput com a funcionalidade de firewall habilitada para tráfego IPv4, independentemente do tamanho do pacote;

8.2.2.1.2. Deve suportar, no mínimo, 1.500.000 (Um milhão e quinhentos mil) de conexões simultâneas;

8.2.2.1.3. Deve suportar, no mínimo, 45.000 (quarenta e cinco mil) novas conexões por segundo;

8.2.2.1.4. Deve Suportar, no mínimo, 6,5 (Seis virgula cinco) Gbps de throughput VPN IPSec;

8.2.2.1.5. Deve estar licenciado para, ou suportar sem o uso de licença, no mínimo, 200 (duzentos) túneis de VPN IPSEC Gateway-to-Gateway simultâneos;

8.2.2.1.6. 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;

8.2.2.1.7. Deve suportar, no mínimo, 1,4 Gbps de throughput de IPS;

8.2.2.1.8. Deve suportar, no mínimo, 1 Gbps de throughput de Inspeção SSL;

8.2.2.1.9. Deve suportar, no mínimo, 900 Mbps de throughput enquanto executa serviços de segurança como IPS, antivírus ou inspeção SSL.

8.2.2.1.10. Deve possuir, pelo menos, 6 (portas) interfaces RJ45 de 1GB;

8.2.2.1.11. Deve possuir, pelo menos, 2 portas de mídia com interfaces SFP de 1GB/ RJ45 1GB;

8.2.2.1.12. Deve possuir, pelo menos, 2 (portas) para gerenciamento de dispositivos do mesmo fabricante do equipamento;

8.2.2.1.13. Deve possuir porta console RJ-45;

8.2.2.1.14. 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;

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

8.2.2.1.16. Deve possuir Fontes redundantes.

8.2.2.1.17. Deve ser possível configurar alta disponibilidade das seguintes formas: Ativo-Ativo, Ativo-Passivo e em Cluster.

8.2.2.1.18. Deve ser licenciado para uso pelo período de duração do contrato.

8.2.2.1.19. Deve possuir garantia para uso pelo período de duração do contrato.

8.2.2.1.20. Firewalls de próxima geração (NGFW):

8.2.2.1.21. 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.

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

8.2.2.1.23. 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;

8.2.2.1.24. 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;

8.2.2.1.25. 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;

8.2.2.1.26. 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.

#### **8.2.2.2. Funcionalidades de rede e firewall:**

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

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

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

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

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

8.2.2.2.6. Deve possuir a funcionalidade de tradução de endereços estáticos - NAT (Network Address Translation), um para um (1-to-1), N-para-um (N-to-1), vários para um, NAT64, NAT66, NAT46 e PAT;

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

8.2.2.2.8. Deverá suportar sFlow ou Netflow;

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

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

8.2.2.2.11. Deve suportar o protocolo padrão da indústria VXLAN;

8.2.2.2.12. Deve implementar o protocolo ECMP;

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

8.2.2.2.14. Enviar log para sistemas de monitoração externos;

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

8.2.2.2.16. Deve possuir mecanismos de proteção anti-spoofing;

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

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

8.2.2.2.19. Suportar OSPF graceful restart;

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

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

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

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

8.2.2.2.24. A configuração em alta disponibilidade deve sincronizar: Sessões, Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede, Associações de Segurança das VPNs e Tabelas FIB;

8.2.2.2.25. Deverá possuir alta disponibilidade (HA), trabalhando no esquema de redundância do tipo Ativo-Passivo e também Ativo-Ativo, com divisão de carga, com todas as licenças de software habilitadas para tal sem perda de conexões;

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

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

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

8.2.2.2.29. Deve possuir recursos de automação, com a finalidade de facilitar a operação diária dos firewalls. Suportar, pelo menos, a tomada de ações como execução de scripts, envio de e-mails,

notificações via Teams e APIs mediante hosts comprometidos, agendamentos, mudanças de configuração e ocorrência de eventos de rede e segurança pré-definidos;

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

8.2.2.2.31. Deverá suportar controle por zonas de segurança;

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

8.2.2.2.33. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;

8.2.2.2.34. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;

8.2.2.2.35. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

8.2.2.2.36. Controle, inspeção e descriptografia de SSL por política para tráfego de saída (Outbound);

8.2.2.2.37. Deve descriptografar tráfego outbound em conexões negociadas com TLS 1.2 e TLS 1.3;

8.2.2.2.38. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;

8.2.2.2.39. Suporte a objetos e regras IPV6;

8.2.2.2.40. Suporte a objetos e regras multicast;

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

#### **8.2.2.2.42. Funcionalidade de controle de aplicações:**

8.2.2.2.43. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;

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

8.2.2.2.45. 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;

8.2.2.2.46. Deverá possuir, pelo menos, 15 (quinze) categorias para classificação de aplicações;

8.2.2.2.47. 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;

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

8.2.2.2.49. 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;

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

8.2.2.2.51. 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;

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

8.2.2.2.53. Atualizar a base de assinaturas de aplicações automaticamente;

8.2.2.2.54. 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;

8.2.2.2.55. 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;

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

8.2.2.2.57. 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;

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

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

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

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

8.2.2.2.62. 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;

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

8.2.2.2.64. 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);

8.2.2.2.65. 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;

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

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

8.2.2.2.68. Funcionalidade de prevenção de intrusão de ameaças:

8.2.2.2.69. 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;

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

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

8.2.2.2.72. 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;

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

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

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

8.2.2.2.76. 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;

8.2.2.2.77. Deve permitir o bloqueio de vulnerabilidades;

8.2.2.2.78. Deve permitir o bloqueio de exploits conhecidos;

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

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

8.2.2.2.81. Detectar e bloquear a origem de portscans;

8.2.2.2.82. Bloquear ataques efetuados por worms conhecidos;

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

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

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

8.2.2.2.86. 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;

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

8.2.2.2.88. Identificar e bloquear comunicação com botnets;

8.2.2.2.89. 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;

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

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

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

8.2.2.2.93. 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.

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

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

8.2.2.2.96. 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;

8.2.2.2.97. Funcionalidade de filtro de conteúdo web e dns:

8.2.2.2.98. 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);

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

8.2.2.2.100. 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;

8.2.2.2.101. 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;

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

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

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

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

8.2.2.2.106. Permitir a customização de página de bloqueio;

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

8.2.2.2.108. 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;

8.2.2.2.109. 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;

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

8.2.2.2.111. Funcionalidade de identificação de usuários:

8.2.2.2.112. 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;

8.2.2.2.113. 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;

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

8.2.2.2.115. 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;
- 8.2.2.2.116. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
- 8.2.2.2.117. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
- 8.2.2.2.118. 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);
- 8.2.2.2.119. 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;
- 8.2.2.2.120. Deve suportar o envio e recebimento de credenciais via RADIUS;
- 8.2.2.2.121. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;
- 8.2.2.2.122. Funcionalidade de filtro de dados:
- 8.2.2.2.123. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP);
- 8.2.2.2.124. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 8.2.2.2.125. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 8.2.2.2.126. 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.
- 8.2.2.2.127. Funcionalidade de geolocalização:
- 8.2.2.2.128. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- 8.2.2.2.129. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;
- 8.2.2.2.130. Funcionalidade de vpn.
- 8.2.2.2.131. Suportar VPN Site-to-Site e Cliente-To-Site;
- 8.2.2.2.132. Suportar IPSec VPN;
- 8.2.2.2.133. A VPN IPSEC deve suportar 3DES;
- 8.2.2.2.134. A VPN IPSEC deve suportar Autenticação MD5 e SHA-1;
- 8.2.2.2.135. A VPN IPSEC deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- 8.2.2.2.136. A VPN IPSEC deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- 8.2.2.2.137. A VPN IPSEC deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- 8.2.2.2.138. A VPN IPSEC deve suportar Autenticação via certificado IKE PKI
- 8.2.2.2.139. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- 8.2.2.2.140. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;
- 8.2.2.2.141. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de troubleshooting;
- 8.2.2.2.142. 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;
- 8.2.2.2.143. Atribuição de DNS nos clientes remotos de VPN;
- 8.2.2.2.144. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, AntiSpyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 8.2.2.2.145. Suportar autenticação via AD/LDAP, certificado e base de usuários local;
- 8.2.2.2.146. Suportar leitura e verificação de CRL (Certificate Revocation List);
- 8.2.2.2.147. Deverá manter uma conexão segura com o portal durante a sessão;
- 8.2.2.2.148. 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);
- 8.2.2.2.149. Funcionalidade de qos, traffic shaping e priorização de tráfego;
- 8.2.2.2.150. 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;

8.2.2.2.151. Suportar a criação de políticas de QoS e Traffic Shaping para os seguintes itens:

8.2.2.2.152. Endereço de origem e Endereço de destino;

8.2.2.2.153. Usuário e grupo;

8.2.2.2.154. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;

8.2.2.2.155. Por porta;

8.2.2.2.156. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

8.2.2.2.157. 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;

8.2.2.2.158. O QoS deve possibilitar a definição de fila de prioridade;

8.2.2.2.159. Suportar priorização em tempo real de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype;

8.2.2.2.160. Suportar marcação de pacotes Diffserv, inclusive por aplicação;

8.2.2.2.161. Suportar modificação de valores DSCP para o Diffserv;

8.2.2.2.162. Suportar priorização de tráfego usando informação de ToS (Type of Service);

8.2.2.2.163. Disponibilizar estatísticas em tempo real para classes de QoS ou Traffic Shaping;

8.2.2.2.164. Deve suportar QOS (Traffic-Shapping), em interface agregadas ou redundantes;

8.2.2.2.165. Deve possibilitar a definição de bandas distintas para download e upload;

8.2.2.2.166. Funcionalidade de balanceamento inteligente de links;

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

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

8.2.2.2.169. 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);

8.2.2.2.170. 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;

8.2.2.2.171. 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;

8.2.2.2.172. 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);

8.2.2.2.173. 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).

8.2.2.2.174. 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:

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

8.2.2.2.176. 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;

8.2.2.2.177. 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;

8.2.2.2.178. 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;

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

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

8.2.2.2.181. 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);

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

8.2.2.2.183. 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;

8.2.2.2.184. 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;

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

8.2.2.2.186. 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;

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

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

8.2.2.2.189. 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);

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

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

8.2.2.2.192. 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;

8.2.2.2.193. 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;

8.2.2.2.194. 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.

8.2.2.2.195. Funcionalidade de controlador de rede sem fio:

8.2.2.2.196. 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:

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

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

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

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

8.2.2.2.201. 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;

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

8.2.2.2.203. 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;

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

8.2.2.2.205. 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;

8.2.2.2.206. 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;

8.2.2.2.207. 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;

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

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

8.2.2.2.210. 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;

8.2.2.2.211. 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;

8.2.2.2.212. 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;

8.2.2.2.213. 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;

8.2.2.2.214. 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;

8.2.2.2.215. 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;

- 8.2.2.2.216. 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;
- 8.2.2.2.217. 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;
- 8.2.2.2.218. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP;
- 8.2.2.2.219. 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;
- 8.2.2.2.220. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários;
- 8.2.2.2.221. Deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio;
- 8.2.2.2.222. A solução deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming;
- 8.2.2.2.223. 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;
- 8.2.2.2.224. 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;
- 8.2.2.2.225. A solução deve implementar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless;
- 8.2.2.2.226. A solução deve suportar priorização via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada;
- 8.2.2.2.227. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas;
- 8.2.2.2.228. 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;
- 8.2.2.2.229. 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;
- 8.2.2.2.230. A solução deve permitir a configuração de quais data rates estarão ativos na ferramenta e quais serão desabilitados;
- 8.2.2.2.231. 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;
- 8.2.2.2.232. A solução deve suportar a configuração do BLE (Bluetooth Low Energy) nos pontos de acesso que tenham este recurso;
- 8.2.2.2.233. 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;
- 8.2.2.2.234. 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;
- 8.2.2.2.235. A solução deve permitir a configuração de Short Guard Interval para o rádio 5GHz;

- 8.2.2.2.236. A solução deve implementar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs;
- 8.2.2.2.237. 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;
- 8.2.2.2.238. 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;
- 8.2.2.2.239. 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;
- 8.2.2.2.240. Deve implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;
- 8.2.2.2.241. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES);
- 8.2.2.2.242. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3;
- 8.2.2.2.243. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID;
- 8.2.2.2.244. 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;
- 8.2.2.2.245. 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;
- 8.2.2.2.246. 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;
- 8.2.2.2.247. 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;
- 8.2.2.2.248. 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;
- 8.2.2.2.249. A solução deve permitir a hospedagem do captive portal na memória interna do controlador wireless;
- 8.2.2.2.250. 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;
- 8.2.2.2.251. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede;
- 8.2.2.2.252. A solução deve permitir que a página de autenticação seja hospedada em servidor externo;
- 8.2.2.2.253. A solução deve permitir a configuração do captive portal com endereço IPv6;
- 8.2.2.2.254. 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;
- 8.2.2.2.255. 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;
- 8.2.2.2.256. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado;
- 8.2.2.2.257. A solução deve implementar recurso de DHCP Server (em IPv4 e IPv6) para facilitar a configuração de redes visitantes;
- 8.2.2.2.258. A solução deve suportar o protocolo OSPF em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura de rede LAN e WLAN;
- 8.2.2.2.259. A solução deve identificar automaticamente o tipo de equipamento e sistema operacional utilizado pelo dispositivo conectado à rede wireless;
- 8.2.2.2.260. 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;

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

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

8.2.2.2.263. 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;

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

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

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

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

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

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

8.2.2.2.270. 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;

8.2.2.2.271. 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;

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

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

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

8.2.2.2.275. 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;

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

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

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

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

8.2.2.2.280. Funcionalidade de controlador de rede cabeada:

8.2.2.2.281. 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:

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

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

8.2.2.2.284. 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;

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

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

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

- 8.2.2.2.288. Através da interface gráfica deve ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches;
- 8.2.2.2.289. Através da interface gráfica deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches;
- 8.2.2.2.290. Através da interface gráfica deve ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches;
- 8.2.2.2.291. Através da interface gráfica deve ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches;
- 8.2.2.2.292. Através da interface gráfica deve ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches;
- 8.2.2.2.293. 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,;
- 8.2.2.2.294. Através da interface gráfica deve ser capaz de aplicar políticas de segurança e controle de tráfego para filtrar o tráfego da rede;
- 8.2.2.2.295. A solução deve ser capaz de identificar as aplicações acessadas na rede através de análise DPI (Deep Packet Inspection);
- 8.2.2.2.296. Deve ser capaz de configurar parâmetros SNMP dos switches;
- 8.2.2.2.297. 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;
- 8.2.2.2.298. A solução deve permitir o envio automático de e-mails de notificação para os administradores da rede em caso de eventos de falhas;
- 8.2.2.2.299. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica;
- 8.2.2.2.300. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches;
- 8.2.2.2.301. A solução deve apresentar graficamente informações sobre disponibilidade dos switches;
- 8.2.2.2.302. Deve prover indicadores de saúde dos elementos críticos do ambiente;
- 8.2.2.2.303. Deve registrar eventos para auditoria de todos os acessos e mudanças de configuração realizadas por usuários;
- 8.2.2.2.304. Deve realizar as funções de gerenciamento de falhas e eventos dos switches da rede;

### **8.2.3. Requisitos da instalação da Solução de segurança FWaaS (Firewall como serviço)**

#### **8.2.3.1. Implementação Física:**

- 8.2.3.1.1. Levantamento de toda estrutura física do ambiente;
- 8.2.3.1.2. Levantamento da estrutura Elétrica;
- 8.2.3.1.3. Verificação do espaço a ser instalado os equipamentos;
- 8.2.3.1.4. Abertura e conferência das caixas dos equipamentos;
- 8.2.3.1.5. Fixação do equipamento no RACK;
- 8.2.3.1.6. Conexão da fonte de alimentação elétrica em réguas de tomada;
- 8.2.3.1.7. Conexão de cabo UTP utilizando o protocolo TCP/IP para utilização do console de gerenciamento;
- 8.2.3.1.8. Conexão das interfaces de rede com os switches;

#### **8.2.3.2. Implementação lógica:**

- 8.2.3.2.1. Parametrização do Licenciamento;
- 8.2.3.2.2. Parametrização das interfaces de rede;
- 8.2.3.2.3. Atualização da última versão de Firmware;
- 8.2.3.2.4. Parametrização das regras de NAT;
- 8.2.3.2.5. Parametrização do Filtro de Conteúdo (WebFilter);
- 8.2.3.2.6. Parametrização de Controle de Aplicação;
- 8.2.3.2.7. Parametrização de VPN (Virtual Private Network);
- 8.2.3.2.8. Parametrização IDS/IPS;
- 8.2.3.2.9. Parametrização DNS;
- 8.2.3.2.10. Parametrização de Gateway Antivírus;



- 8.2.3.2.11. Parametrização de Objetos de Endereço;
- 8.2.3.2.12. Parametrização de Grupo de Objetos;
- 8.2.3.2.13. Parametrização de Load Balancing;
- 8.2.3.2.14. Parametrização de SSO (Single Sign-on);
- 8.2.3.2.15. Parametrização de SNMP;
- 8.2.3.2.16. Parametrização de NTP;
- 8.2.3.2.17. Parametrização de PortGroups;
- 8.2.3.2.18. Parametrização de Zones;
- 8.2.3.2.19. Parametrização de Serviços;
- 8.2.3.2.20. Parametrização de Rotas;
- 8.2.3.2.21. Parametrização de DHCP

### **8.3. SOLUÇÃO DE BACKUP CORPORATIVO**

#### **8.3.1. Características do Software de Backup**

- 8.3.1.1. Deverá ser disponibilizado 14 licenças para backup de máquinas virtuais,
- 8.3.1.2. 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.
- 8.3.1.3. Gerenciamento Centralizado: Interface centralizada para gerenciar backups tanto locais quanto na nuvem, possibilitando uma visualização única de todos os dados armazenados.
- 8.3.1.4. 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.
- 8.3.1.5. 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.
- 8.3.1.6. Compressão de Dados: A compressão deve ser personalizável para otimizar o desempenho conforme as necessidades da infraestrutura, especialmente em volumes de escrita diários significativos.
- 8.3.1.7. 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.
- 8.3.1.8. 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.
- 8.3.1.9. 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.
- 8.3.1.10. 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.
- 8.3.1.11. 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.
- 8.3.1.12. 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.
- 8.3.1.13. 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.
- 8.3.1.14. 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.
- 8.3.1.15. 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.
- 8.3.1.16. 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.

8.3.1.17. Arquivamento Inteligente: Capacidade de arquivar backups antigos na nuvem para economizar espaço local, enquanto mantém acessível para restauração conforme necessário.

8.3.1.18. 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.

8.3.1.19. 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.

8.3.1.20. 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.

8.3.1.21. Restauração Granular: Capacidade de restaurar desde arquivos individuais até máquinas inteiras (físicas ou virtuais), com velocidade e flexibilidade.

8.3.1.22. Recuperação Bare-Metal: Capacidade de restaurar máquinas físicas diretamente para novas instâncias ou hardware, sem a necessidade de configuração manual de cada sistema.

8.3.1.23. Testes de Restauração Automática: Testes automáticos de restauração para garantir que os backups estão íntegros e prontos para serem restaurados se necessário.

8.3.1.24. 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.

8.3.1.25. 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.

8.3.1.26. 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.

8.3.1.27. Controle de Acessos Granular: Capacidade de definir permissões específicas para diferentes tipos de dados e volumes de backup, garantindo que acessos indevidos sejam evitados.

8.3.1.28. 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.

8.3.1.29. 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.

8.3.1.30. Automatização de trabalhos de Backup: Capacidade de automatizar os processos de backup, permitindo agendamentos e execuções automáticas conforme as necessidades do ambiente.

8.3.1.31. Integração com Ferramentas de Orquestração: Suporte para integração com ferramentas

8.3.1.32. de orquestração e automação (ex: scripts PowerShell, APIs).

8.3.1.33. 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.

8.3.1.34. 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.

8.3.1.35. 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.

### **8.3.2. Características do backup local:**

8.3.2.1. 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.

8.3.2.2. 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.

### **8.3.3. Características do backup em nuvem:**

- 8.3.3.1. 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.
- 8.3.3.2. O armazenamento em nuvem deve ser compatível com o software de backup fornecido.
- 8.3.3.3. 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.
- 8.3.3.4. 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.
- 8.3.3.5. 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.
- 8.3.3.6. 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.
- 8.3.3.7. 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.
- 8.3.3.8. Permite que múltiplas versões de um arquivo sejam mantidas no caso de necessidade de recuperação de dados antigos.
- 8.3.3.9. 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.
- 8.3.3.10. O armazenamento em nuvem deve fornecer criptografia de dados em trânsito (durante a transferência) e em repouso (armazenados).
- 8.3.3.11. TLS/SSL deve ser usado para proteger os dados durante a transferência.
- 8.3.3.12. Criptografia em repouso é necessária para proteger os dados armazenados, utilizando algoritmos como AES-256.
- 8.3.3.13. Chaves de criptografia devem ser gerenciadas de forma segura, seja pelo cliente ou pelo provedor de nuvem.
- 8.3.3.14. O serviço deverá oferecer alta disponibilidade de pelo menos 99,99% e garantir SLA mínimo de 99,9% para o acesso ao armazenamento.
- 8.3.3.15. O armazenamento deve possuir capacidade de escala praticamente ilimitada, sem necessidade de intervenção manual, manutenção ou monitoramento contínuo por parte da CONTRATANTE.
- 8.3.3.16. 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.
- 8.3.3.17. A CONTRATADA deverá assegurar que os dados permaneçam exclusivamente em território brasileiro durante todo o período de vigência contratual, inclusive cópias e réplicas.
- 8.3.3.18. 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.
- 8.3.3.19. 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.
- 8.3.3.20. 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.).
- 8.3.3.21. 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.
- 8.3.3.22. 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.

8.3.3.23. Ferramentas de monitoramento nativas devem estar integradas.

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

#### **8.3.4. Requisitos da instalação da Solução de Backup corporativo:**

8.3.4.1. Implementação Física:

8.3.4.1.1. Verificar a estrutura elétrica do equipamento fornecido pelo CRC;

8.3.4.1.2. Verificar a conexão da fonte de alimentação elétrica em régua de tomada;

8.3.4.1.3. Verificar a conexão das interfaces de rede com os switches;

8.3.4.2. Implementação lógica.

8.3.4.2.1. Configurar o sistema de armazenamento local do equipamento, devendo:

8.3.4.2.1.1. Criar e configurar o arranjo de discos em RAID 5;

8.3.4.2.1.2. Instalar e configurar sistema operacional baseado em Linux (com preferência por versões LTS, como Ubuntu Server ou Debian Stable);

8.3.4.2.1.3. Provisionar o volume lógico para armazenamento dos dados de backup, com diretórios e permissões apropriadas; 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.

8.3.4.2.1. Será responsável por configurar o software de backup na infraestrutura local, integrando-o com o ambiente em nuvem, devendo:

8.3.4.2.2.1. Garantir que os dados de backup armazenados localmente estejam sincronizados com os dados de backup na nuvem;

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

#### **8.4. SERVIÇOS CONTINUADOS DE SUPORTE N1, N2 E N3**

8.4.1. Definição do objeto

8.4.1.1. 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, ativos de rede, firewall, 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.

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

8.4.1.3. 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.

8.4.1.4. Atuar proativamente na resolução de problemas relativos à parte lógica e física das soluções;

##### **8.4.1.5. A contratada deverá:**

8.4.1.5.1. Monitorar o ambiente a fim de garantir que os recursos estão funcionando adequadamente na solução;

8.4.1.5.2. Gerar e fornecer, mediante solicitação, relatórios técnicos de desempenho e disponibilidade, incluindo estatísticas de uptime, latência de links, falhas críticas e acessos aos dispositivos

8.4.1.5.3. Possuir sistema de abertura de chamados pela internet.

8.4.1.5.4. Monitorar latência e uptime dos links configurados.

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

8.4.1.7. 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.

#### **8.4.2. Características do serviço prestado.**

##### **8.4.2.1. Monitoramento e suporte técnico:**

- 8.4.2.1.1. Realizar o monitoramento proativo das estações de trabalho, identificando preventivamente falhas e promovendo ações corretivas;
- 8.4.2.1.2. Prestar suporte técnico remoto ilimitado aos usuários, conforme os seguintes níveis:
- 8.4.2.1.3. Nível 1 (N1): Atendimento de primeiro nível (dúvidas operacionais e incidentes comuns);
- 8.4.2.1.4. Nível 2 (N2): Suporte intermediário, com resolução de problemas técnicos e administrativos;
- 8.4.2.1.5. Nível 3 (N3): Suporte avançado, envolvendo infraestrutura, servidores e sistemas críticos;
- 8.4.2.1.6. Executar o monitoramento completo do ambiente de TI, por meio de ferramentas especializadas de mercado.

##### **8.4.2.2. Serviços ambiente Legado:**

###### **8.4.2.2.1. Manutenção, gestão de ativos e rede:**

- 8.4.2.2.1.1. Executar manutenção corretiva e preventiva em todos os ativos tecnológicos listados na “Tabela do parque de informática do CRCES”;
- 8.4.2.2.1.2. Realizar gestão e manutenção da estrutura hiperconvergente, garantindo operação contínua e eficiente dos recursos virtualizados;
- 8.4.2.2.1.3. 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.
- 8.4.2.2.1.4. Executar a gestão técnica da infraestrutura de rede, abrangendo:
- 8.4.2.2.1.5. Administração de lans, vlans e sub-redes, com segmentação lógica adequada ao ambiente corporativo;
- 8.4.2.2.1.6. Configuração de protocolos de segurança de rede, como acls, 802.1X, VLAN tagging e controle de broadcast;
- 8.4.2.2.1.7. Implementação de boas práticas para prevenção de incidentes, como isolamento de tráfego e controle de acesso;
- 8.4.2.2.1.8. Apoio à CONTRATANTE na atualização de topologias, mapeamento de rede e análise de performance.
- 8.4.2.2.1.9. Executar serviços de instalação e gerenciamento de cabeamento de rede, incluindo as interligações entre os diversos setores da sede e o servidor central.

###### **8.4.2.2.2. Serviços gerenciados:**

- 8.4.2.2.2.1. Prestar serviços gerenciados de segurança da rede e ativos de TI, incluindo políticas de proteção e respostas a incidentes;
- 8.4.2.2.2.2. Realizar a aplicação gerenciada de atualizações de segurança (patches) em estações de trabalho e servidores;
- 8.4.2.2.2.3. Gerenciar e administrar o ambiente de Office 365, incluindo usuários, licenças e segurança da informação;
- 8.4.2.2.2.4. Realizar a gestão e manutenção do banco de dados SQL Server, incluindo monitoramento de performance, backups e segurança.

###### **8.4.2.2.3. Controle, inventário e chamados:**

- 8.4.2.2.3.1. Manter atualizado o inventário de hardware e software, contendo marca, modelo, especificações, localização e situação operacional dos ativos;
- 8.4.2.2.3.2. Efetuar a gestão de chamados por meio de sistema de tickets, com categorização por tipo de incidente, severidade, prazo e status de resolução.

###### **8.4.2.2.4. Logística e apoio à contratação:**

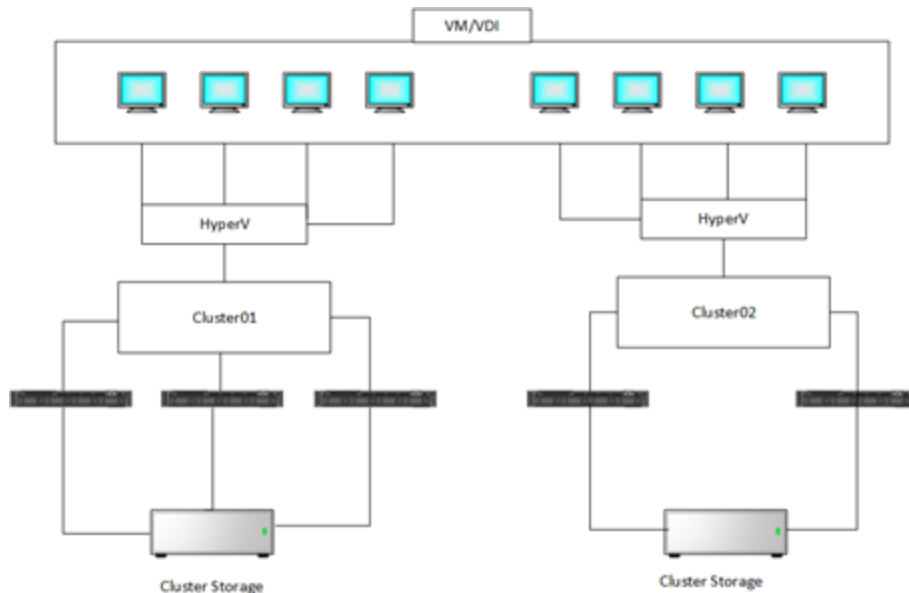
- 8.4.2.2.4.1. Executar a logística de coleta e entrega de equipamentos entre a sede da CONTRATANTE e os locais de atendimento;
- 8.4.2.2.4.2. Prestar assessoria técnica nas aquisições de bens e serviços relacionados à TI, incluindo:
- 8.4.2.2.4.3. Elaboração de especificações técnicas;
- 8.4.2.2.4.4. Análise de propostas técnicas;
- 8.4.2.2.4.5. Apoio em processos licitatórios;
- 8.4.2.2.4.6. O prazo para entrega de pareceres técnicos será de até 5 (cinco) dias úteis, a partir de solicitação formal da CONTRATANTE.

#### 8.4.2.2.5. Atendimento presencial:

8.4.2.2.5.1. Disponibilizar 02 (duas) visitas técnicas presenciais por semana, com duração mínima de 6 (seis) horas por visita, para execução de tarefas presenciais corretivas, preventivas e de alinhamento com a equipe técnica da CONTRATANTE.

#### 8.4.3. Tabela do parque de informática do CRCES:

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



#### 8.4.4. Manutenção preventiva e corretiva.

##### 8.4.4.1. Manutenção Preventiva:

8.4.4.1.1. 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.

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

8.4.4.1.2.1. Verificação de funcionamento dos componentes físicos e lógicos;

8.4.4.1.2.2. Limpeza técnica interna e externa;

8.4.4.1.2.3. Aferição e calibração de dispositivos, quando aplicável;

8.4.4.1.2.4. Atualização de firmwares, BIOS e softwares;

8.4.4.1.2.5. Verificação e otimização de configurações;

8.4.4.1.2.6. Avaliação do desempenho geral e análise de logs;

8.4.4.1.2.7. Testes de funcionalidade e conectividade.

8.4.4.1.2.8. Realizar monitoramento contínuo do sistema de backup local, incluindo:

8.4.4.1.2.8.1. Acompanhamento da integridade dos discos e volumes lógicos;

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

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

8.4.4.1.3. 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.

8.4.4.1.4. 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.

8.4.4.1.5. 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.

8.4.4.1.6. 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.

#### **8.4.4.2. Manutenção Corretiva:**

8.4.4.2.1. Em caso de surgimento de problema técnico em qualquer um dos equipamentos ou serviços listados no item de manutenção preventiva 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.

8.4.4.2.2. 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.

8.4.4.2.3. 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.

8.4.4.2.4. 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.

8.4.4.2.5. 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.

8.4.4.2.6. 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 dias úteis após o recebimento dos novos equipamentos/peças.

8.4.4.2.7. Os prazos acima poderão ser revistos, mediante a apresentação de justificativa válida e aceita pela contratante.

8.4.4.2.8. Durante a execução do serviço externo, a empresa contratada deverá:

8.4.4.2.9. Se responsabilizar pelo transporte dos equipamentos que serão retirados;

8.4.4.2.10. Providenciar termo de responsabilidade de retirada;

8.4.4.2.11. Cumprir todas as obrigações constantes e assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.

8.4.4.2.12. 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;

8.4.4.2.13. O descarregamento do produto ficará a cargo da Contratada, devendo ser providenciada a devida mão de obra;

8.4.4.2.14. A Contratada deverá comunicar a data de entrega com 2 (dois) dias úteis de antecedência ao CRCES;

8.4.4.2.15. Os produtos serão recebidos por empregado do CRCES e, no caso de recebimento provisório, não implicará em aceitação dos mesmos;

8.4.4.2.16. O recebimento definitivo não isenta a empresa de responsabilidades futuras quanto à qualidade do produto entregue;

8.4.4.2.17. Todas as peças que apresentaram problemas e foram substituídas deverão ser identificadas e entregues ao departamento de T.I do CRCES.

#### **8.4.5.2. Suporte para o item 2 “SOLUÇÃO DE SEGURANÇA FWaaS”:**

##### **8.4.5.2.1. Serviço Continuado**

8.4.5.2.1.1. Após a instalação a CONTRATADA deverá manter, monitorar e gerenciar todo o ambiente após a sua instalação na modalidade 8x5;

8.4.5.2.1.2. Efetuar toda rotina de backup das configurações semanalmente;

8.4.5.2.1.3. 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;

8.4.5.2.1.4. Realizar as seguintes configurações sempre que solicitadas pela CONTRATANTE:



- 8.4.5.2.1.5. Atividades relativas à Solução de Segurança:
- 8.4.5.2.1.6. Criação das rotas para links.
- 8.4.5.2.1.7. Criação de NAT.
- 8.4.5.2.1.8. Liberação de portas.
- 8.4.5.2.1.9. Configuração do Filtro de Conteúdo.
- 8.4.5.2.1.10. Configuração do Controle de Aplicativos.
- 8.4.5.2.1.11. Configuração do Agente para autenticação LDAP.
- 8.4.5.2.1.12. Configuração para o Single Sign-On (SSO).
- 8.4.5.2.1.13. Configurações dos serviços avançados de segurança (IPS, Antivírus).
- 8.4.5.2.1.14. Configuração de VPN client to site.
- 8.4.5.2.1.15. Configuração de VPN site to site.
- 8.4.5.2.1.16. Criação de regras de Firewall.
- 8.4.5.2.1.17. Criação de regras de QoS.
- 8.4.5.2.1.18. Emitir relatório de segurança mensal por localidade.
- 8.4.5.2.1.19. Criar relatórios e dashboards de acordo com as orientações a serem formuladas.
- 8.4.5.2.1.20. 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.
- 8.4.5.2.1.21. 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.

#### **8.4.5.3. Suporte para o item 3 “SOLUÇÃO DE BACKUP CORPORATIVO”**

##### **8.4.5.3.1. Serviço Continuado**

- 8.4.5.3.1.1. Deverá realizar monitoramento contínuo do servidor de backup local, incluindo:
- 8.4.5.3.1.2. Acompanhamento da integridade dos discos e volumes lógicos;
- 8.4.5.3.1.3. Monitoramento do uso de espaço em disco e alertas proativos;
- 8.4.5.3.1.4. Verificação da consistência dos arquivos de backup e testes periódicos de restauração.
- 8.4.5.3.1.5. Será responsável pelo suporte técnico completo ao servidor de backup local, devendo atuar:
- 8.4.5.3.1.6. De forma remota, em primeira instância, e presencialmente, caso não seja possível resolver o incidente de forma remota;
- 8.4.5.3.1.7. Dentro dos prazos estabelecidos no Acordo de Nível de Serviço (ANS/SLA).
- 8.4.5.3.1.8. 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:
- 8.4.5.3.1.9. Notificar formalmente a CONTRATANTE sobre a necessidade de expansão;
- 8.4.5.3.1.10. Realizar a instalação de novos discos no equipamento, previamente adquiridos pela CONTRATANTE ou fornecidos pela CONTRATADA, conforme contratação;
- 8.4.5.3.1.11. Reconfigurar o RAID e volumes lógicos, preservando os dados existentes e a integridade do ambiente;
- 8.4.5.3.1.12. Ajustar as políticas de backup e monitoramento para o novo ambiente.
- 8.4.5.3.1.13. Toda e qualquer alteração na infraestrutura de backup local deverá ser previamente comunicada e autorizada pelo CRC-ES.

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

- 8.4.5.4.1. A CONTRATADA deve garantir os seguintes níveis de serviço e atendimento:
- 8.4.5.4.2. 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.
- 8.4.5.4.3. 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.

8.4.5.4.4. 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

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.

#### 8.4.5.4.5. Descrição de atendimento para cada nível de severidade:

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

8.4.5.4.5.2. 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.

8.4.5.4.5.2.1. 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.

8.4.5.4.5.2.2. 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.

8.4.5.4.5.3. 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.

8.4.5.4.5.3.1. 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.

8.4.5.4.5.3.2. 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.

8.4.5.4.5.4. 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.

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

8.4.5.4.5.4.2. 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.

8.4.5.5. 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.

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

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

## **9. MODELO DE GESTÃO DO CONTRATO**

9.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

9.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

9.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

9.4. O CRCES poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

9.5. Após a assinatura do contrato, o CRCES poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

### **9.6. Preposto**

9.6.1. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado.

9.6.2. Fiscalização

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

9.6.4. O fiscal do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

9.6.5. O fiscal do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º e Decreto nº 11.246, de 2022, art. 22, II);

9.6.6. Identificada qualquer inexatidão ou irregularidade, o fiscal do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

9.6.7. O fiscal do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV);

9.6.8. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V);

9.6.9. O fiscal do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

9.6.10. O fiscal do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

9.6.11. Caso ocorra descumprimento das obrigações contratuais, o fiscal do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as

providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

#### **9.6.12. Gestor do Contrato**

9.6.13. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

9.6.14. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

9.6.15. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

9.6.16. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

9.6.17. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

9.6.18. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

9.6.19. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

### **10. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO**

10.1. A avaliação da execução do objeto utilizará o relatório/checklist para atesto de notas fiscais para aferição da qualidade da prestação do serviço.

10.1.1. Será indicada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, caso se constate que a Contratada:

10.1.1.1. não produzir os resultados acordados,

10.1.1.2. deixar de executar, ou não executar com a qualidade mínima exigida as atividades contratadas; ou

10.1.1.3. deixar de utilizar materiais e recursos humanos exigidos para a execução do serviço, ou utilizá-los com qualidade ou quantidade inferior à demandada.

10.1.1.4. A utilização do IMR não impede a aplicação concomitante de outros mecanismos para a avaliação da prestação dos serviços.

10.1.1.5. A aferição da execução contratual para fins de pagamento considerará os seguintes critérios:

10.1.1.6. A avaliação da execução do objeto será conduzida utilizando o instrumento de verificação de conformidade, em conformidade com as especificações técnicas estabelecidas no item 5.

10.2. Do recebimento

10.2.1. Os serviços serão recebidos provisoriamente, no prazo de 15 (quinze) dias, pelos fiscais, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo. (Art. 140, I, a, da Lei nº 14.133, de 2021 e Arts. 22, X e 23, X do Decreto nº 11.246, de 2022).

10.2.2. O prazo da disposição acima será contado do recebimento de comunicação de cobrança

oriunda do contratado com a comprovação da prestação dos serviços a que se referem a parcela a ser paga.

10.2.3. O fiscal do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências. (Art. 22 e 23, X, Decreto nº 11.246, de 2022 ).

10.2.4. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

10.2.5. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último;

10.2.6. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

10.2.7. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021 )

10.2.8. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

10.2.9. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as

10.2.10. especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

10.2.11. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

10.2.12. Os serviços serão recebidos definitivamente no prazo de 15 (quinze) dias, contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

10.2.13. Emitir documento comprobatório da avaliação realizada pelos fiscais, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022).

10.2.14. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

10.2.15. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

10.2.16. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021 , comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

10.2.17. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

10.2.18. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

10.2.19. Liquidação

10.2.20. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de cinco dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

10.2.21. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, nos casos de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021

10.2.22. Para fins de liquidação, o setor competente deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

10.2.22.1. o prazo de validade;

10.2.22.2. a data da emissão;

10.2.22.3. os dados do contrato e do órgão contratante;

10.2.22.4. o período respectivo de execução do contrato;

10.2.22.5. o valor a pagar; e

10.2.22.6. eventual destaque do valor de retenções tributárias cabíveis.

10.2.23. Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à contratante;

10.2.24. A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da

10.2.25. regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021.

10.2.26. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

10.2.27. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

10.2.28. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

10.2.29. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

10.2.30. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

### 10.3. Prazo de pagamento

10.3.1. O pagamento será efetuado no prazo máximo de até dez dias úteis, contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

### 10.4. Forma de pagamento

10.4.1. O pagamento será realizado preferencialmente por meio de chave pix indicada pelo fornecedor, desde que a conta para pagamento esteja em nome da empresa contratada, ou através de boleto/fatura emitido por este.

10.4.1.1. Na impossibilidade de pagamento via chave pix ou boleto/fatura, o valor poderá ser transferido para conta bancária, desde que a mesma esteja em nome da empresa contratada.

10.4.1.2. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

10.4.2. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

10.4.3. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

## **11. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO**

11.1. Forma de seleção e critério de julgamento da proposta.

11.1.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO GLOBAL.

### **11.2. Regime de execução**

11.2.1. O regime de execução do objeto será empreitada por preço global.

11.3. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

#### **11.3.1. Habilitação jurídica**

11.3.1.1. Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

11.3.1.2. Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio <https://www.gov.br/empresas-e-negocios/pt-br/empreendedor>;

11.3.1.3. Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

11.3.1.4. Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020.

11.3.1.5. Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

11.3.1.6. Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

11.3.1.7. Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

11.3.1.8. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

11.3.1.9. Exigências Adicionais para Cooperativas

11.3.1.10. Caso a empresa participante seja uma cooperativa, deverá apresentar, além dos itens anteriores, a seguinte documentação complementar:

11.3.1.11. Relação de cooperados que atenderão o contrato, com atas de inscrição e comprovação de domicílio na localidade da sede da cooperativa.

11.3.1.12. Declaração de Regularidade de Situação do Contribuinte Individual (DRSCI) para cada um dos cooperados.

11.3.1.13. Comprovação do capital social proporcional ao número de cooperados necessários à execução do contrato.

11.3.1.14. Registro previsto na Lei nº 5.764, de 1971.

11.3.1.15. Comprovação de integração das quotas-partes dos cooperados que executarão o contrato.

11.3.1.16. Documentos de regularidade jurídica da cooperativa: ata de fundação, estatuto social, regimento dos fundos, editais e registros das últimas assembleias, além da ata que autorizou a participação na licitação.

11.3.1.17. Última auditoria contábil-financeira ou declaração de que a auditoria não foi exigida pelo órgão fiscalizador.

11.3.1.18. Modelo de gestão operacional, conforme a IN SEGES/ME nº 05/2017.

#### **11.3.2. Habilitação fiscal, social e trabalhista**

11.3.2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;



11.3.2.2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

11.3.2.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

11.3.2.4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

11.3.2.5. Prova de regularidade com a Fazenda Estadual do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

11.3.2.6. Prova de regularidade com a Fazenda Municipal/Distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

11.3.2.7. Caso o fornecedor seja considerado isento dos tributos Estadual/Distrital ou Municipal relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

11.3.2.8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

### **11.3.3. Qualificação Econômico-Financeira**

11.3.3.1. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

### **11.3.4. Qualificação Técnica**

Para a qualificação técnica, a empresa deverá cumprir os seguintes requisitos:

#### **11.3.4.1. Requisitos de Capacidade Técnica da Empresa**

11.3.4.1.1. Comprovação de aptidão para execução de serviço similar, de complexidade tecnológica e operacional equivalente ou superior à do objeto desta contratação, ou do item pertinente, por meio da apresentação de certidões ou atestados emitidos por pessoas jurídicas de direito público ou privado, ou pelo conselho profissional competente, quando for o caso.

**11.3.4.1.1.1.** Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contrato(s) executado(s) com as seguintes características mínimas:

- a) Serviços de backup em nuvem com, no mínimo, 25 terabytes de capacidade de armazenamento utilizável.
- b) Gestão de ambientes com infraestrutura virtualizada e VDI (Virtual Desktop Infrastructure) com pelo menos 30 estações virtuais.
- c) Suporte a infraestruturas com mais de 5 servidores físicos e 10 servidores virtuais simultâneos.
- d) Monitoramento e gestão de ambientes com hiperconvergência e armazenamento definido por software (SDS).
- e) Hiperconvergência: Implementação, operação e manutenção de infraestruturas hiperconvergentes, com conhecimento em tecnologias como VMware vSAN, Nutanix AHV e HPE Simplivity.
- f) Gerenciamento de Clusters de Servidores: Expertise em balanceamento de carga, otimização de recursos, failover e alta disponibilidade.
- g) Virtualização com Hyper-V: Conhecimento avançado em provisionamento, gerenciamento de imagens e otimização de desempenho de desktops virtuais.
- h) Administração de Banco de Dados SQL: Otimização de desempenho, segurança, backup e recuperação de desastres.
- i) Gerenciamento de Serviços Online: Expertise em administração de sistemas, redes e segurança da informação para garantir alta disponibilidade.

11.3.4.1.2. Serão admitidos, para fins de comprovação de quantitativo mínimo de serviço, a apresentação e o somatório de diferentes atestados de serviços executados de forma concomitante, pois essa situação equivale, para fins de comprovação de capacidade técnico-operacional, a uma única

contratação.

11.3.4.1.3. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

11.3.4.1.4. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual do Contratante e local em que foram prestados os serviços, entre outros documentos.

#### **11.3.4.2. Qualificação Técnico-Profissional**

11.3.4.2.1. Apresentação do(s) profissional(is), abaixo indicado(s), detentor(es) dos certificados abaixo indicado(s):

a) Certificação em tecnologias de firewall e segurança de rede, como Fortinet, Palo Alto ou Cisco.

b) ITIL v3 ou superior.

c) MCSA Windows Server 2012 ou superior.

d) Certificação para Instalação e Configuração de Switches DELL ou similar.

**11.3.4.3.** O(s) profissional(is) acima indicado(s) deverá(ão) participar do serviço objeto do contrato, e será admitida a sua substituição por profissionais de experiência equivalente ou superior, desde que aprovada pela Administração (§ 6º do art. 67 da Lei nº 14.133, de 2021).

**11.3.4.4.** O profissional técnico indicado poderá ocupar a posição de diretor, sócio ou integrar o quadro permanente da licitante na condição de empregado ou de prestador de serviços, devendo ser comprovada sua vinculação com a licitante, até a data da apresentação dos documentos de habilitação, por meio de carteira de trabalho e previdência social (CTPS), contrato de prestação de serviços, ficha de registro de empregado ou contrato social, conforme o caso.

**11.3.4.4.1** Será admitido a apresentação de Termo de Compromisso de contratação futura assinado pela licitante e pelo profissional indicado.

## **12. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO**

12.1. O custo estimado total da contratação é de R\$ 40.000,00 (quarenta mil reais) mensais, perfazendo o valor global de R\$ 480.000,00 (quatrocentos e oitenta mil reais) para o período contratual, conforme demonstrado na tabela abaixo. Ressalta-se que o valor foi apurado a partir da Pesquisa de Preços e consolidado no respectivo Mapa Comparativo de Preços, em conformidade com o disposto no inciso XXIII, alínea "i", do art. 6º da Lei nº 14.133/2021.

ITEM 1					
SUBITEM	ESPECIFICAÇÕES	CATSER	QUANTIDADE	VALOR MENSAL	VALOR ANUAL
1	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	30710	12	R\$ 17.000,00	R\$ 204.000,00

2	Instalação e gestão de Firewall de Próxima Geração, fortalecendo a segurança da rede e protegendo os dados do CRCES contra ameaças cibernéticas.	30736	12	R\$ 3.000,00	R\$ 36.000,00
3	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.	30744	12	R\$ 8.000,00	R\$ 96.000,00
4	Suporte técnico avançado (remoto e presencial) para manutenção da infraestrutura tecnológica, gestão de incidentes e mudanças, monitoramento contínuo	30728	12	R\$ 12.000,00	R\$ 144.000,00

**12.2** Para comprovar a conformidade técnica da proposta, a empresa deverá enviar no momento do envio da proposta:

- a) Documentação dos produtos ofertados: Catálogos, manuais, prospectos e outros documentos oficiais que permitam a clara identificação dos produtos. Esses documentos podem ser em português ou inglês, originais ou cópias. Não serão aceitos documentos criados especificamente para a licitação. A documentação pode ser entregue em formato eletrônico.
- b) Links de referência: Páginas da internet do fabricante do software, com indicação do endereço URL.

### **13. ADEQUAÇÃO ORÇAMENTÁRIA**

13.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento do CRCES.

13.2. A contratação será atendida pela seguinte dotação:

13.3. 6.3.1.3.02.01.005 - SERVIÇO DE TECNOLOGIA DA INFORMAÇÃO

13.4. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação dos orçamentos pelo Conselho Federal de Contabilidade – CFC.

---

**Wekson José Barbieri Mariano**

Operador de Sistemas

**Aprovo o Termo de Referência.**

Encaminhe-se para as providências necessárias para a seleção do fornecedor, cumprindo as demais etapas legais para a contratação pública.

Contador **Walterleno Maifrede Noronha**  
Presidente



Documento assinado eletronicamente por **Wekson José Barbieri Mariano, Analista - Sistemas / Desenvolvimento**, em 07/10/2025, às 12:41, 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 **Walterleno Maifrede Noronha, Presidente**, em 08/10/2025, às 11:07, 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 **1055314** e o código CRC **CE436A02**.