



## **Apêndice do Anexo I**

### **ESTUDO TÉCNICO PRELIMINAR – IN SGD-ME nº 94/2022**

#### **1 – Definição**

**Inciso I, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022**

O Estudo Técnico Preliminar tem por objetivo planejar a contratação de serviço de segurança da informação baseada em firewall do tipo appliance com suporte técnico continuado.

#### **1.1 - Diretrizes Gerais para Elaboração dos Estudos Preliminares**

1.1.1 O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Formalização de Demanda - DFD, bem como demonstrar a viabilidade técnica e econômica da solução identificada, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação, em consonância com o art. 11 da Instrução Normativa SGD-ME nº 94/2022.

#### **1.2 - Normativos que disciplinam os serviços a serem contratados**

1.2.1 Lei nº 14.133/2021 - Lei de Licitações e Contratos Administrativos.

1.2.2 Instrução Normativa SGD-ME nº 94, de 23 de dezembro de 2022 - Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo.

#### **2 - Das Necessidade de negócio e tecnologia**

**Inciso I, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022**

2.1. Considerando a crescente dependência da organização em relação a serviços digitais e a ampliação da superfície de exposição a ameaças cibernéticas, torna-se imprescindível a adoção de medidas robustas de segurança da informação para garantir a continuidade e a confiabilidade das operações institucionais. Entre os principais riscos identificados, destacam-se o acesso indevido a dados sigilosos, a possibilidade de indisponibilidade de serviços críticos e a ocorrência de ataques externos direcionados à infraestrutura tecnológica.



2.2. Nesse contexto, identifica-se a necessidade de implementação de uma solução de segurança de perímetro por meio de firewall do tipo appliance, que permita a inspeção, filtragem e controle do tráfego de rede de forma centralizada e eficiente. Tal solução deve atender aos requisitos de negócio de proteção das informações institucionais, de resiliência tecnológica e de conformidade normativa, contribuindo para a redução de vulnerabilidades e para a mitigação de riscos relacionados à integridade, confidencialidade e disponibilidade das informações.

2.3. Sob a ótica tecnológica, o firewall em formato appliance oferece desempenho otimizado, atualização contínua de assinaturas de ameaças, escalabilidade e integração com demais ferramentas de segurança da informação. Sua adoção possibilitará a aplicação de políticas de acesso diferenciadas, detecção e prevenção contra intrusões, bem como a geração de relatórios e registros de auditoria necessários ao monitoramento e à governança de TI.

2.4 Assim, a contratação deste serviço configura-se como essencial para assegurar que os objetivos de negócio da instituição sejam atingidos com segurança, eficiência operacional e aderência às boas práticas de gestão de riscos e de governança digital, em conformidade com o disposto no Inciso I do artigo 11 da Instrução Normativa SGD-ME nº 94/2022.

### **3.1 – Requisitos da contratação – Identificação das necessidades de negócio**

3.1.1 Somente poderão participar deste processo licitatório pessoas jurídicas cujo ramo de atividade seja compatível com o objeto da licitação e que apresentem todos os documentos de habilitação exigidos;

3.1.2 A contratada deverá atender as exigências de habilitação jurídica e de regularidade fiscal, social e trabalhista, conforme disciplinado pela Lei 14.133/2021, além de outras exigências de habilitação, qualificação técnica e qualificação econômico-financeira;

3.1.3 O CRQ-IV dispõe em seu datacenter de uma solução de segurança de rede, que compreende as funcionalidades de firewall, filtro de conteúdo, IPS, antivírus de borda e AntiSpam, do fabricante SONICWALL, além de outras ferramentas como firewall para aplicação WEB, balanceamento de carga e rede Wi-Fi. De forma a manter a padronização do ambiente tecnológico que já utiliza as soluções



SONICWALL, se faz necessária a substituição do firewall de rede, de forma que seja assegurada a otimização e padronização do ambiente tecnológico, sendo mais vantajoso em termos de custo, uma vez que existe um conhecimento técnico das principais funcionalidades da solução.

3.1.4 A infraestrutura de segurança da informação do CRQ-IV utiliza atualmente o firewall marca e modelo Sonicwall NSA 2700, responsável pela proteção de perímetro, filtragem de tráfego, controle de acessos e mitigação de ameaças cibernéticas. Contudo, verificou-se a necessidade de substituição deste equipamento pelo modelo Sonicwall NSA 2800, em razão dos seguintes fatores:

- Evolução tecnológica e ciclo de vida
  - a) O NSA 2800 é sucessor direto do NSA 2700, incorporando aprimoramentos de hardware e software que garantem maior longevidade de uso e suporte do fabricante.
  - b) O modelo 2700 encontra-se em estágio avançado de seu ciclo de vida, com risco de entrar em política de descontinuidade (End of Sale / End of Support), o que comprometeria a atualização de firmwares e assinaturas de ameaças.
- Desempenho e capacidade ampliada
  - a) O NSA 2800 oferece maior throughput de firewall e inspeção SSL/TLS, permitindo lidar melhor com o crescimento da demanda de tráfego da rede institucional.
  - b) Há necessidade de escalabilidade para suportar novos serviços digitais.
- Recursos de segurança aprimorados
  - a) O NSA 2800 possui melhorias em inspeção profunda de pacotes (DPI), prevenção contra intrusões (IPS), controle de aplicações e filtragem de conteúdo, alinhando-se às melhores práticas de segurança.
  - b) O equipamento garante maior eficiência contra ataques avançados e tráfego criptografado, o que se tornou essencial diante do aumento de ameaças modernas.
- Conformidade normativa e de governança
  - a) A substituição assegura a aderência às diretrizes de governança digital e segurança da informação, conforme previsto na IN SGD-ME nº 94/2022 e na LGPD, reduzindo riscos de indisponibilidade, vazamento de dados e incidentes de segurança.
  - b) A atualização tecnológica previne fragilidades associadas ao uso de equipamentos em fase de obsolescência.



- Continuidade e mitigação de riscos
  - a) A adoção do NSA 2800 contribui para garantir a continuidade dos serviços institucionais, reduzindo riscos de interrupção em serviços críticos por falhas de desempenho ou suporte.
  - b) A modernização do firewall fortalece o ambiente contra ataques cibernéticos cada vez mais sofisticados, preservando a confidencialidade, integridade e disponibilidade das informações da organização.

3.1.5 Nesse sentido, faz-se necessário a atualização da referida solução Sonicwall para um modelo que atenda a demanda atual do CRQ-IV e possibilitem a continuidade de proteção digital da rede já existente, totalmente planejada, homologada e padronizada na instituição, eliminando o retrabalho com uma possível mudança total de solução e o impacto financeiro com a reorganização total da infraestrutura de rede e treinamento de equipe.

3.1.6 O modelo sugerido, Sonicwall NSA 2800, substituirá o modelo Sonicwall NSA 2700 atualmente em funcionamento no CRQ-IV.

3.1.7 A solução deverá ser composta por equipamentos, software profissional com licença de instalação, implantação, configuração, treinamento, migração da configuração existente, garantia de funcionamento e suporte técnico para toda a solução. O serviço deverá ser oferecido por empresa instalada em território nacional e esteja em conformidade com a Lei 13.709/18 que trata sobre a proteção de dados – LGPD.

3.1.8 Os requisitos de contratação para um serviço de segurança da informação baseado em firewall do tipo appliance normalmente envolvem aspectos técnicos, de negócio, de governança e de conformidade descritos a abaixo:

#### Requisitos de Negócio

- Garantir a proteção das informações institucionais, preservando confidencialidade, integridade e disponibilidade.
- Reduzir riscos de acesso indevido, vazamento de dados e interrupção de serviços críticos.



- Atender às normas e boas práticas de segurança da informação, incluindo a IN SGD-ME nº 94/2022 e a LGPD (Lei Geral de Proteção de Dados).
- Assegurar continuidade operacional dos sistemas e serviços digitais, mesmo em cenários de ataque cibernético.

#### Requisitos Técnicos

- Tipo de solução: firewall de perímetro do tipo appliance dedicado (hardware específico para segurança, não apenas software).
- Funcionalidades mínimas:
  - a) Filtragem de pacotes em camadas de rede e aplicação (NGFW – Next Generation Firewall).
  - b) Controle de acesso baseado em políticas e usuários.
  - c) Inspeção profunda de pacotes (DPI – Deep Packet Inspection).
  - d) Prevenção contra intrusões (IPS/IDS integrados).
  - e) Proteção contra malwares e ataques de negação de serviço (DoS/DDoS).
  - f) Suporte a VPNs seguras (IPSec/SSL).
  - g) Relatórios e registros de auditoria exportáveis para SIEM.
- Desempenho e disponibilidade:
  - a) Capacidade compatível com o tráfego médio e de pico da rede institucional.
  - b) Suporte a alta disponibilidade (HA) com failover automático.
  - c) Escalabilidade para expansão de banda ou crescimento de usuários.
- Gerenciamento:
  - a) Painel centralizado com controle de políticas e monitoramento em tempo real.
  - b) Integração com sistemas de autenticação corporativa (ex.: LDAP, AD).
  - c) Atualizações automáticas de assinaturas de ameaças e patches de segurança.

#### Requisitos de Governança e Conformidade

- Atender às diretrizes de segurança da informação da Administração Pública Federal.
- Suporte à LGPD e normas correlatas de proteção de dados pessoais.
- Geração de logs auditáveis para fins de controle interno e auditoria externa.
- Suporte a relatórios periódicos de conformidade (ex.: incidentes, tentativas de intrusão, acessos negados).



#### Requisitos de Suporte e Sustentação

- Garantia de atualização de software, firmwares e assinaturas de ameaças pelo período contratual.
- Suporte técnico 24x7 com SLA definido (ex.: resposta em até 1h para incidentes críticos).
- Possibilidade de treinamento para equipe interna de TI/Segurança.
- Fornecimento de documentação técnica completa (configuração, operação e melhores práticas).

#### Requisitos de Contratação

- Modelo de fornecimento: contratação como serviço gerenciado (MSS – Managed Security Service).
- Garantia mínima do fabricante de 36 meses ou conforme ciclo de vida recomendado.
- Licenciamento contemplando todos os módulos essenciais (IPS, antivírus, antimalware, controle de aplicações, filtragem web etc.).
- Previsão contratual para atualização tecnológica ou substituição de hardware em caso de obsolescência.
- O equipamento do tipo firewall deverá estar homologado pela ANATEL (Agência Nacional de Telecomunicações). A homologação pela ANATEL assegura que o equipamento atende aos padrões técnicos e de segurança exigidos no Brasil.

### 3.2 – Comprovação da capacidade técnica e comercial

3.2.1 A CONTRATADA deverá comprovar que possui em seu quadro de funcionários, pelo menos (3) três Profissionais Técnicos Certificados pelo fabricante da solução de Next Generation Firewall “SonicWall Network Security Administrator”, e no mínimo (1) um Profissional Técnico Certificado pelo fabricante da solução de Next Generation Firewall “SonicWall Network Security Professional”, emitido por centro autorizado do fabricante, na execução dos serviços de instalação, manutenção e treinamento. A comprovação deverá ser por meio de apresentação do vínculo empregatício CLT ou contrato de prestação de serviço.



3.2.2 O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de reconhecimento assinada pelo representante legal do fabricante no Brasil.

3.2.3 A licitante, caso não seja o fabricante/desenvolvedor da solução, deverá apresentar declaração do fabricante, de que ela possui autorização e capacitação técnica para fornecimento, instalação e configuração dos produtos.

3.2.4 A licitante deve comprovar que é revendedora autorizada do fabricante Sonicwall, por meio de documentação oficial, a qual pode ser verificada diretamente no site do fabricante, no seguinte link: <https://www.sonicwall.com/pt-br/partners/authorized-distributors>.

Justificativa: A comprovação de que a licitante é um distribuidor autorizado, tem o objetivo de minimizar riscos para a instituição, como por exemplo, risco de adquirir produtos em desacordo com as regras do fabricante, ou provenientes de descaminhos fiscais ou contrabandos, ou ainda, de licenças não destinadas para uso no território brasileiro.

#### **4 – Definição e justificativa da natureza continuada dos serviços:**

4.1 A contratação do serviço de segurança da informação baseada em firewall do tipo appliance caracteriza-se como serviço continuado, uma vez que atende a uma necessidade permanente, essencial e ininterrupta da organização.

4.2 O firewall é o principal ponto de defesa no perímetro da rede institucional, responsável por proteger os sistemas contra acessos indevidos, tentativas de intrusão, vazamentos de dados e ataques cibernéticos. A proteção das informações e a disponibilidade dos serviços digitais da organização exigem monitoramento constante, aplicação contínua de políticas de segurança, atualização de assinaturas de ameaças e suporte técnico especializado, atividades que não podem ser interrompidas sem comprometer diretamente a operação da instituição.

4.3 Além disso, o ambiente de ameaças cibernéticas é dinâmico, com surgimento diário de novas vulnerabilidades e técnicas de ataque. Assim, a manutenção e atualização contínua do serviço são indispensáveis para assegurar a confidencialidade, integridade e disponibilidade da informação, bem



como para garantir a conformidade com normativos vigentes, tais como a Instrução Normativa SGD-ME nº 94/2022 e a Lei Geral de Proteção de Dados (LGPD).

4.4 Portanto, a contratação deve ser enquadrada como serviço de natureza continuada, visto que a interrupção ou descontinuidade do serviço implicaria riscos elevados de indisponibilidade dos sistemas institucionais, prejuízos à segurança da informação, descumprimento de obrigações legais e normativas, e impacto direto na prestação dos serviços públicos digitais à sociedade.

## 5 – Estimativas das quantidades:

Fornecimento de 2 (dois) firewalls appliance em modo de alta disponibilidade (HA – High Availability) pode ser justificada sob vários aspectos de negócio, técnicos e de conformidade.

### 5.1 Garantia de Continuidade dos Serviços

- a) O firewall é componente crítico de segurança e conectividade da instituição. A interrupção do seu funcionamento, mesmo que temporária, poderia causar indisponibilidade de sistemas essenciais, impactando diretamente a operação e os serviços prestados à sociedade.
- b) A configuração em HA permite que, em caso de falha de um equipamento, o outro assuma automaticamente, assegurando disponibilidade ininterrupta.

### 5.2 Mitigação de Riscos Operacionais

- a) Reduz o risco de ponto único de falha (SPOF – Single Point of Failure), uma das principais vulnerabilidades em ambientes de rede e segurança da informação.
- b) A alta disponibilidade garante resiliência contra falhas de hardware, erros de software, panes elétricas ou manutenção programada, preservando a integridade e continuidade da operação

### 5.3 Atendimento a Normas e Boas Práticas de Segurança da Informação

- a) Alinhamento às diretrizes da IN SGD-ME nº 94/2022, que preveem medidas de proteção tecnológica para a continuidade dos serviços digitais e a redução de riscos de indisponibilidade.
- b) Atende também às melhores práticas de segurança da informação definidas em frameworks internacionais (ISO/IEC 27001, NIST, COBIT), que recomendam redundância em controles críticos de segurança.





#### 5.4 Suporte a Escalabilidade e Crescimento da Demanda

- a) A operação em HA possibilita distribuição de carga (dependendo da arquitetura adotada), garantindo melhor desempenho e suporte ao aumento no volume de acessos, serviços digitais e usuários conectados.
- b) Garante que a infraestrutura possa evoluir sem comprometer desempenho ou segurança.

#### 5.5 Eficiência em Manutenção e Gestão

- a) Permite que atualizações, manutenções preventivas e corretivas sejam realizadas em um dos appliances enquanto o outro mantém a operação, eliminando a necessidade de janelas de indisponibilidade.
- b) Simplifica a gestão de mudanças, reduzindo riscos durante atualizações críticas de firmware ou políticas de segurança.

#### 5.6 Proteção da Imagem Institucional e Conformidade Legal

- a) A indisponibilidade de serviços públicos digitais ou falhas de segurança poderiam gerar impacto negativo à imagem institucional, além de possíveis sanções legais, especialmente no contexto da LGPD.
- b) O investimento em HA demonstra compromisso com a gestão de riscos, a governança de TI e a segurança da informação.

Item	Descrição	Quantitativo
1	Firewall do tipo Appliance NGFW em modo de alta disponibilidade	02
2	Serviço de instalação, configuração, migração de dados e ativação.	Setup completo de instalação até o início da operação
3	Suporte técnico continuado	Suporte na modalidade 24 x 7 x 365 durante a vigência do contrato
4	Licença APSS 3 anos para NSA 2800	01
5	Licença Analytics SAAS 90 DAYS para NSA 2800	01
6	Licenças de CSE Private Access Basic	30



**6 – Descrição da Solução:**  
Inciso I, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

**6.1 DO OBJETO**

Prestação de segurança da informação baseada em firewall do tipo appliance com suporte técnico continuado

Item	Quant.	Unid.	CATSER	Descrição
1	36	Mês	27014	Prestação de serviços de segurança da informação baseada em firewall do tipo appliance com suporte técnico continuado, compreendendo:  01 Appliance Sonicwall NSA 2800 01 Appliance Sonicwall NSA 2800 HA 01 Licença APSS 3 anos para NSA 2800 01 Licença Analytics SAAS 90 DAYS para NSA 2800 30 licenças de CSE Private Access Basic
2	01	Unid.	27014	Serviços de Implantação, configuração, migração dos dados e ativação do serviço.

**6.2 CARACTERÍSTICAS GERAIS DOS FIREWALLS FÍSICOS**

Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões.

Para proteção do ambiente contra os ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW.

A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7.

Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço. Um appliance é projetado para executar uma tarefa específica de forma eficiente e simplificada, com recursos e software otimizados para essa finalidade.

Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes.



Os firewalls devem ser entregues com licenciamento válido para, no mínimo, 36 meses, incluindo garantia e suporte.

Deve ser capaz de atualizar de forma automática o Firmware, patches e atualizações de segurança.

A solução deve permitir o uso de armazenamento externo para System Logs, Threat Logs, AppFlow reporting data e Packet Captures, garantindo persistência de dados após reinicializações do firewall

O painel deve exibir detalhes sobre o último contato do Firewall com o gerenciador de licenciamento, mostrando o status de atualização de licenças e atualizações de assinaturas

Deve fornecer APIs para que os fornecedores externos de NAC possam transmitir o contexto de segurança aos firewalls e que esta funcionalidade seja compatível com a utilização simultânea de fornecedores externos distintos.

A solução de segurança não pode aplicar nenhum tipo de exceção de inspeção de tráfego (by-pass) oriunda de condições de limitação de capacidade de processamento de forma automática. Toda e qualquer exceção (by-pass) de inspeção e tráfego deve ser possível apenas através de ação explícita e específica criada pelo administrador da plataforma através de configurações realizadas pela console gráfica do appliance, ou pela plataforma centralizada de gerenciamento da solução.

### 6.3 CARACTERÍSTICAS DIVERSAS

Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino.

Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do tunel IPSec.

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

Deve possuir proteção anti-spoofing.

Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;

Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF.

Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a: endereço de origem, endereço de destino, serviço e aplicação.

A solução deverá possuir a tecnologia SD-WAN (Software Defined WAN), e que a mesma seja nativa da solução, sem a necessidade de qualquer tipo de licenciamento complementar, para evitar



indisponibilidade no ambiente mesmo em caso de expiração do licenciamento vigente.

Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:

- Latência;
- Jitter;
- Perda de pacotes.

O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal lógico.

A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas.

A solução de SD-WAN deve permitir encaminhamento de tráfego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook.

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

Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas.

Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes.

Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN.

Deve suportar DHCP relay.

Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários.

Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, interface (física e virtual) ou zona de segurança.

Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (instant messengers) incluindo, no mínimo, ICQ, WhatsApp, Google



Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo.

Deve ter suporte à proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso.

Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados.

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

Detectar e bloquear a origem de portscans.

Deve permitir o bloqueio de ataques.

Deve permitir o bloqueio de exploits conhecidos.

O gateway Antivírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP e SMTP.

Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser descriptografado de forma transparente à aplicação.

Implementar DSCP (Differentiated Services Code Points).

Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede.

Implementar controle e gerenciamento de banda para a tecnologia VoIP (Voice OverIP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço.

Implementar mecanismo de sincronismo de horário através do protocolo NTP.

Possuir suporte ao protocolo SNMP versões 2 e 3.

Possuir suporte a log via syslog.

Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica.

Reconhecer aplicações como, no mínimo, peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail.

Para tráfego criptografado SSL/TLS, deve de-criptografar pacotes possibilitando a leitura de payload



dos pacotes para checagem de assinaturas de aplicações conhecidas pelo fabricante.

Controle, inspeção e de-criptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.2 e TLS 1.3

Deve permitir a funcionalidade de ARP bridging

Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm"

A solução deve permitir a visualização gráfica das regras de segurança e acesso.

#### 6.4 ALTA DISPONIBILIDADE

Devem ser fornecidos 02 (dois) appliances de NGFW com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada.

A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Passivo, com as implementações de Failover.

Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador.

A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster.

A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover.

A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover.

A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança.

A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante.

A solução de HA deve permitir que o dispositivo primário trate todo o tráfego, mantendo o dispositivo secundário atualizado em tempo real sobre as informações de conexão de rede, garantindo uma transição transparente para o dispositivo secundário em caso de failover, sem que haja perda das conexões de VPN, FTP, Oracle SQL\*NET, Real Audio, VPN Client, Dynamic ARP Objects, Informações de DHCP Server, Multicast, IGMP, usuários ativos, RIP e OSPF.



## 6.5 REQUISITOS MÍNIMOS DOS FIREWALLS

Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 6 Gbps ou superior.

Desempenho em modo de Inspeção (descriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 1.8 Gbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item.

Desempenho mínimo de 7 Gbps de IPS.

Suporte mínimo de 2.000.000 conexões simultâneas/concorrentes no modo SPI.

Suporte mínimo de 50.000 novas conexões por segundo.

Deve possuir armazenamento interno de no mínimo 128 GB e suportar expansão de armazenamento interno para até 512Gb.

Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC.

Deve possuir 16 interfaces 1 GbE padrão RJ-45.

Deve possuir 3 interfaces 10GbE SFP+;

Deve possuir 1 interface do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento.

Deve possuir 2 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G.

A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 50 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 1000 usuários simultâneos.

A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 500 usuários simultâneos.

Deve suportar 2000 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos.

Deve suportar, no mínimo, 5.5Gbps de desempenho de VPN IPSEC.

Os desempenhos apontados devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitados. Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame.

O fornecimento dos produtos e seus licenciamentos devem ser entregues através de empresa credenciada e autorizada pelo fabricante. Isto deve ser comprovado através de carta de



reconhecimento assinada pelo representante legal do fabricante no Brasil.

O Equipamento deverá ser homologado pela ANATEL.

Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados.

O licenciamento para todos os serviços de Next Generation Firewall deverá ser de no mínimo 36 meses.

A garantia do hardware deverá ser de 36 meses.

É imprescindível que a solução não possua um limite de tamanho de inspeção de arquivos no uso da tecnologia 'gateway antimalware', já que tal restrição poderia permitir a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

#### 6.6 CARACTERÍSTICAS DE VPN

Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

Suportar algoritmos de criptografia 3DES, AES 128, AES 256 e AESGCM16-256

Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384.

Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits).

Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2.

Autenticação via de tuneis IPsec via certificado digital para VPNs Site-to-Site e Client-to-Site.

A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android.

Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico.

Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC.

Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos.

Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário.





Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego.

Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.

Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication.

Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

#### **6.7 ACESSO REMOTO PARA OS ENDPOINTS (ZTNA/VPNaaS)**

Contratação de serviço para Acesso Remoto Seguro à rede corporativa, na modalidade ZTNA (Zero-Trust Network Access), para 30 usuários, pelo período de 36 meses.

A solução proposta deverá contemplar, no mínimo, todas as funcionalidades e características da edição SonicWall Cloud Secure Edge (CSE) - Secure Private Access (SPA) Basic ou uma solução tecnicamente equivalente ou superior que atenda a todos os requisitos descritos neste documento.

A solução deve ser entregue como um serviço de nuvem (SaaS/SSE), com gerenciamento centralizado em portal web, sem a necessidade de instalação e manutenção de hardware (appliance) adicional no ambiente da Contratante.

A solução deve operar sob o framework de Acesso à Rede Zero Trust (ZTNA).

A plataforma deve possuir múltiplos pontos de presença (PoPs) distribuídos globalmente para garantir baixa latência e alta disponibilidade de acesso para os usuários.

Deve fornecer um cliente (agente) leve, isto é, com baixo consumo de recursos, para ser instalado nos dispositivos dos usuários, compatível com os principais sistemas operacionais do mercado (no mínimo: Microsoft Windows 10/11, MacOS, iOS e Android).

A solução deverá possuir as seguintes funcionalidades de acesso e conectividade:

- **Acesso ZTNA Baseado em Túnel (VPNaaS):** A solução deve estabelecer um túnel seguro e criptografado (baseado em DTLS) do dispositivo do usuário até o ponto de presença mais próximo na nuvem do provedor.



- **Acesso à Rede Privada:** Deve permitir o acesso seguro a segmentos de rede privados e recursos internos baseados em faixas de endereço IP (notação CIDR) e servidores DNS internos.
- **Suporte a Protocolos:** Deve suportar todo o tráfego baseado nos protocolos TCP e UDP dentro do túnel estabelecido.
- **Conector de Rede:** Deve utilizar um conector de software leve, instalado no ambiente da Contratante (on-premises ou nuvem privada), para estabelecer a conexão entre a nuvem do serviço e a rede interna, sem a necessidade de abrir portas de entrada (inbound) no firewall.

A solução deverá possuir as seguintes funcionalidades de Segurança e Políticas de Acesso:

- **Gerenciamento Centralizado de Políticas:** Todas as políticas de acesso devem ser criadas e gerenciadas através de um console único na nuvem.
- **Políticas Baseadas em Identidade:** As regras de acesso devem ser baseadas na identidade do usuário e em sua associação a grupos, com integração obrigatória a provedores de identidade (IdP) modernos via protocolo SAML 2.0 (ex: Microsoft Entra ID, Okta, Google Workspace).
- **Controle de Acesso (Camada 4):** Deve permitir a criação de políticas que definam quais usuários/grupos podem acessar quais recursos, especificados por endereços IP/CIDR e nomes de domínio totalmente qualificados (FQDN).

A solução deverá possuir as seguintes funcionalidades de Gerenciamento, Monitoramento e Visibilidade:

- **Console de Gerenciamento Unificado:** Deve oferecer um portal web intuitivo para configuração de políticas, gerenciamento de usuários e monitoramento do ambiente.
- **Logs e Relatórios:** A plataforma deve fornecer logs detalhados e em tempo real de todas as tentativas de acesso (bem-sucedidas e falhas), permitindo a auditoria e a investigação de eventos de segurança.

## 6.8 CONTROLE DE AMEAÇAS

Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Antivírus e Anti-Bot integrado ao próprio appliance de segurança.

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



Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego.

Implementar funcionalidade de detecção e bloqueio de “call-backs”.

A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede.

A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP.

Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS.

Implementar interface CLI segura através do protocolo SSH.

Possuir Antivírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream.

A solução deve permitir criar regras de exceção de acordo com a proteção.

Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;

Permitir o bloqueio de malwares (vírus, worms, spyware etc.).

A solução deve ser capaz de proteger contra os ataques a DNS.

A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares.

A solução deve ser capaz de prevenir acesso a websites maliciosos.

A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH.

A solução deverá receber atualizações de um serviço baseado em cloud.

A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos.

A solução antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS.

A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade

A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficientes frente ameaças exploradas por vulnerabilidades do tipo meltdown.

A solução de Gateway Antivírus deverá ter a tecnologia complementar de Anti Virus-Cloud, para que os mecanismos existentes de verificação sejam ampliados.

A solução deve ser capaz de bloquear proativamente o acesso a domínios maliciosos conhecidos por meio de filtragem DNS, reduzindo assim o risco de infecções por malware e outros ataques



cibernéticos.

A solução deve prover o bloqueio de URL baseado em reputação, identificando e bloqueando proativamente entidades suspeitas.

#### 6.9 PROTEÇÃO CONTRA OS ATAQUES AVANÇADOS

A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”.

Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS.

A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH.

Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle.

Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real.

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

Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android.

Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware.

A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas.

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

Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados.

Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego;

Conter ameaças avançadas de dia zero.



Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador.

Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;

Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos.

Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado.

Implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado.

Possuir Antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS.

Mitigar ameaças de dia zero de forma transparente para o usuário final.

Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro.

Implementar mecanismo de pesquisa por diferentes intervalos de tempo.

Mitigar ameaças de dia zero via tráfego de internet.

Permitir a contenção de ameaças de dia zero sem a alteração da infraestrutura de segurança.

Mitigar ameaças de dia zero que possam burlar o sistema operacional emulado.

A solução deve permitir a criação de listas brancas (whitelist) baseadas no MD5 do arquivo.

Mitigar ameaças de dia zero antes da execução e evasão de qualquer código malicioso.

Conter e mitigar exploits avançados.

A análise em nuvem ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Antivírus e Anti-Spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede).

Suporte a submissão manual de arquivos para análise através do serviço de Sandbox.

As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se alojam em memória, atuando permanentemente e em tempo real.

A Solução de segurança de Firewalls deverá ter um sistema de inspeção baseado em fluxo que execute análises simultâneas de tráfego de entrada e saída em alta velocidade, sem proxying or



buffering.

A Solução deve unificar diversas funções de segurança em um único conjunto integrado, inspecionando os arquivos de usuários locais, remotos e móveis.

A Solução deve descriptografar e inspecionar o tráfego criptografado, como HTTPS, SMTPS, NNTPS etc., sem afetar o desempenho.

A solução de segurança de Firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças, com sandboxing usando multi-mecanismos baseado em nuvem, permitindo:

Inspeção profunda de memória em tempo real

Inspeção profunda de pacotes livre de remontagem,

Descriptografia e inspeção TLS/SSL,

Inteligência e controle de aplicativos

Recursos SD-WAN seguros

É imprescindível que a solução não possua um limite de tamanho de inspeção de arquivos no uso da tecnologia 'gateway antimalware', já que tal restrição poderia permitir a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

#### 6.10 CARACTERÍSTICAS DE FILTRO DE CONTEÚDO WEB

Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 89 (oitenta e nove) categorias distintas, com mecanismo de atualização e consulta automáticas.

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

Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico.

Permitir a customização de página de bloqueio.

Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante.

Deve permitir submissão de novos sites para categorização.



Permitir a classificação dinâmica de sites web, URLs e domínios.

Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet.

Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web.

Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana.

#### 6.11 CARACTERÍSTICAS DE AUTENTICAÇÃO

Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea.

Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API.

Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento.

Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW.

Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o login na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser.

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 NGFW.

Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando.

Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida.

Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet.



A solução deve possibilitar SSO via API.

## 6.12 CARACTERÍSTICAS DE RELATÓRIOS

A solução deverá prover relatórios com histórico mínimo de 90 dias.

A solução deverá prover relatórios referente as atividades dos usuários.

A solução deverá prover relatórios referente ao uso de aplicações web, com no mínimo as seguintes informações:

- nome da aplicação
- quantidade de conexões
- percentual que a aplicação representa do tráfego da rede e quantidade de Megabytes trafegados

A solução deverá prover relatórios referente ao consumo de rede dos usuários, com no mínimo as seguintes informações:

- nome do usuário
- quantidade de conexões
- percentual que tráfego do usuário representa na rede
- quantidade de Megabytes trafegados

A solução deverá prover relatórios referente ao consumo de rede por endereço IP, com no mínimo as seguintes informações:

- endereço IP
- quantidade de conexões
- percentual que tráfego que o IP representa na rede
- quantidade de Megabytes trafegados

A solução deverá prover relatórios referente aos acessos web com no mínimo informações referentes às categorias acessadas, quantidade de conexões e percentual que cada categoria web representou no tráfego de rede.

A solução deverá arquivar relatórios gerados automaticamente, permitindo o administrador fazer o download em formato PDF.

A solução deverá permitir geração e envio agendado de relatórios.





### 6.13 INSTALAÇÃO E CONFIGURAÇÃO

A contratada deverá instalar os equipamentos com a participação da equipe técnica da Gerência de Tecnologia e Informação do CRQ-IV;

Ficará sob responsabilidade da contratada realizar toda a transferência das configurações existentes no equipamento Sonicwall NSA 2700, utilizado pelo CRQ-IV, para os equipamentos objeto desta licitação.

A instalação dos equipamentos deve considerar a utilização em modo de alta disponibilidade, ou seja, deverão ser instalados de modo caso haja falha no equipamento primário o secundário assume a operação automaticamente garantindo o funcionamento e desempenho do serviço.

A empresa contratada deverá apresentar um plano de instalação incluindo metodologia e cronograma de implantação da solução, definindo atividades, prazos, responsabilidades e recursos utilizados para a instalação.

Os dias apresentados para execução das atividades devem ser considerados “dias corridos”, isto é, dias não úteis como final de semana e feriados devem ser considerados para a execução do projeto e atendimento dos prazos.

Evento	Descrição	Prazo máximo para conclusão
1	Assinatura do contrato	
2	Reunião inicial do projeto, levantamento de informações.	5 dias após a assinatura
3	Entrega do Documento “Plano de Implantação”.	5 dias após o evento 2
4	Avaliação pelo CRQ-IV do Plano de Implantação.	2 dias após o evento 3
5	Emissão do termo de homologação do Plano de Implantação	2 dias após o evento 4
6	Entrega de todos os componentes da solução	30 dias após o evento 1
7	Conferência de todos os componentes entregues da solução	1 dia após o evento 6
8	Emissão do termo de homologação de recebimento dos equipamentos e softwares da solução	1 dia após o evento 7
9	Instalação física da solução	5 dias após o evento 8
10	Emissão do termo de homologação da instalação física da solução	1 dia após o evento 9



11	Instalação lógica da solução Período de funcionamento experimental Implantação e testes na solução de backup Eliminação de pendências Período sem falhas	5 dias após o evento 10
12	Emissão do termo de homologação da instalação lógica da solução.	1 dia após o evento 11
13	Acompanhamento operacional do ambiente de redes por parte da CONTRATADA.	1 dia após o evento 12
14	Emissão do termo de homologação da solução implantada	1 dia após o evento 13
15	Tempo estimado Total do projeto	60 dias corridos

As atividades de instalação física da solução deverão observar os seguintes aspectos:

- A montagem completa (Fixação das Componentes no rack, Interligação com Switches etc.) da totalidade dos equipamentos entregues, de forma que, ao final, tudo fique organizado e pronto para ser logicamente configurado e utilizado.

Ficará a cargo e às expensas da Contratada:

- Atividades relacionadas ao cabeamento interno no Rack de Redes que abrigará a solução, passagem, organização, marcação e rotulação dos componentes envolvidos.
- Fornecimento de todo o material necessário para essas atividades incluindo cabos, conectores, suportes, line cords, path cords, fixadores, etiquetas etc.
- Instalação, configuração, ativação e licenciamento de todos os softwares que envolve a solução de modo que possibilite a homologação de todas as funcionalidades requeridas no Edital.
- O CRQ-IV fornecerá o Rack que abrigará os equipamentos da solução.
- O CRQ-IV indicará dentro do seu Datacenter localizado no 2º andar da sede o local exato para a instalação dos equipamentos.

As seguintes condições deverão ser observadas acerca da execução dos serviços de implantação das funcionalidades técnicas da solução no ambiente:

- A instalação da solução deverá, preferencialmente, ser efetuada de forma a não afetar o funcionamento dos recursos ou equipamentos atualmente em operação, nem impedir ou



interromper a rotina de trabalho de funcionários e colaboradores do CRQ-IV, devendo ser executada em finais de semana ou horários alternativos ao expediente de atendimento do CRQ-IV.

- No caso de necessidade de interrupção dos recursos, equipamentos ou da rotina de trabalho de qualquer setor funcional, em decorrência da instalação da solução, esta deverá estar devidamente planejada e ser acordada com antecedência junto ao CRQ-IV;
- As atividades de instalação lógica da solução deverão observar a implantação dos componentes de software da solução deverá estar em consonância com a metodologia, parâmetros e funcionalidades indicadas no documento “Plano de Implantação”.

#### **6.14 MONTAGEM DOS EQUIPAMENTOS E INSTALAÇÃO DA SOLUÇÃO**

As atividades de instalação física da solução deverão observar os seguintes aspectos:

- A montagem completa (Fixação das Componentes no rack, Interligação com Switches etc.) da totalidade dos equipamentos entregues, de forma que, ao final, tudo fique organizado e pronto para ser logicamente configurado e utilizado;
- II) Ficará a cargo e às expensas da Contratada:
  - a) Atividades relacionadas ao cabeamento interno no Rack de Redes que abrigará a solução, passagem, organização, marcação e rotulação dos componentes envolvidos.
  - b) Fornecimento de todo o material necessário para essas atividades incluindo cabos, conectores, suportes, line cords, path cords, fixadores, etiquetas etc.
  - c) Instalação, configuração, ativação e licenciamento de todos os softwares que envolve a solução de modo que possibilite a homologação de todas as funcionalidades requeridas neste instrumento.
  - d) O CRQ-IV fornecerá o Rack que abrigará os equipamentos da solução.
  - e) O CRQ-IV indicará dentro do seu Datacenter localizado no 1º andar da sede o local exato para a instalação dos equipamentos.

#### **6.15 CRITÉRIOS PARA INSTALAÇÃO LÓGICA DA SOLUÇÃO**

- As seguintes condições deverão ser observadas acerca da execução dos serviços de implantação das funcionalidades técnicas da solução no ambiente:
  - a) A instalação da solução deverá, preferencialmente, ser efetuada de forma a não afetar o funcionamento dos recursos ou equipamentos atualmente em operação, nem impedir ou



interromper a rotina de trabalho de funcionários e colaboradores do CRQ-IV, devendo ser executada em finais de semana ou horários alternativos ao expediente de atendimento do CRQ-IV.

b) No caso de necessidade de interrupção dos recursos, equipamentos ou da rotina de trabalho de qualquer setor funcional, em decorrência da instalação da solução, esta deverá estar devidamente planejada e ser acordada com antecedência junto ao CRQ-IV.

c) As atividades de instalação lógica da solução deverão observar os seguintes aspectos:

c.1) A implantação dos componentes de software da solução deverá estar em consonância com a metodologia, parâmetros e funcionalidades indicadas no documento “Plano de Implantação”.

d) Deverá ser elaborada juntamente com a equipe técnica do CRQ-IV, qual a melhor estratégia de instalação da solução considerando as melhores práticas de segurança.

#### 6.16 IMPLANTAÇÃO E TESTES

- Os serviços objeto desta contratação são compostos de planejamento, instalação, customização, integração, ativação, documentação, suporte técnico, logístico e gerência da implantação dos componentes da solução, além da transferência de conhecimento técnico e atividades de HandsOn;
- Por instalação, customização, integração e ativação entendem-se todos os procedimentos relacionados à instalação e configuração, física e lógica, parametrização e testes de quaisquer componentes de hardware e software fornecidos neste termo, de modo a garantir o pleno funcionamento da solução, inclusive garantindo a operacionalização e integração com os demais componentes de hardware e software atualmente em uso no CRQ-IV;
- A CONTRATADA deverá criar e manter atualizada documentação das atividades, processos, testes, homologação, entrega e conferência, reuniões de trabalho, compromissos e prazos de modo a compor uma documentação final da implantação a ser entregue ao CRQ-IV no final do processo;
- A CONTRATADA caberá demonstrar todas as funcionalidades requeridas para avaliação por parte do CRQ-IV, as quais deverão ser testadas em todas as variações possíveis, através de testes específicos;



- O CRQ-IV acompanhará todo o procedimento para realização dos testes, não podendo a CONTRATADA realizá-los omitindo quaisquer informações ou métodos utilizados;
- Na demonstração das funcionalidades, a CONTRATADA não poderá alegar, em nenhuma hipótese, a utilização de procedimento, ou qualquer técnica protegida por propriedade industrial ou intelectual que impeçam o CRQ-IV de ter comprovação integral sobre os resultados deles;
- Os testes que deverão ser executados para certificar as funcionalidades implementadas devem abranger, no mínimo:
  - a) Teste de acesso e navegação dos micros da rede interna;
  - b) Teste de filtro de navegação em URL's bloqueadas;
  - c) Teste de acesso aos Servidores da DMZ, interna e externamente;
  - d) Teste de criação e acesso de VPN's;
  - e) Teste de intrusão via ferramenta de benchmark;
  - f) Teste de Failover de hardware para validação de alta disponibilidade;
- O não atendimento a qualquer desses requisitos ou prazos, por completo ou em parte, sujeitará a CONTRATADA à aplicação das sanções contratuais correspondentes.
- Todos os componentes de hardware e software requeridos para atender as funcionalidades exigidas no Edital, mesmo que não estejam especificados e cotados na proposta, serão considerados como parte integrante dos serviços de instalação e deverão ser fornecidos sem ônus adicional para o CRQ-IV.

#### 6.17 SUPORTE TÉCNICO CONTINUADO

- A CONTRATADA deverá prestar, ao longo da vigência do Contrato (36 meses), serviços de suporte técnico da solução fornecida, os quais devem contribuir para assegurar a continuidade do pleno funcionamento da solução.
- A CONTRATADA deverá manter equipe disponível durante 24 horas x 365 dias para atendimento remoto e/ou onsite com mobilização e deslocamento em até 2 horas após acionamento e orientações do CRQ-IV. Essa equipe será acionada em casos críticos de parada na rede ocasionados por quaisquer ameaças, devendo a contratada solucionar definitivamente o problema em até 4 horas
- Características do Suporte Continuado:



- a) Suporte Remoto Especializado com cobertura 24x7x365 dias.
- b) Suporte Presencial Especializado com cobertura 24x7x365 para manutenções críticas de indisponibilidade e falta de acesso a recursos de rede dependentes do equipamento.
- c) Atendimento Remoto e On Site para resolução de chamados de severidade “Emergencial” e ou “Mau Funcionamento”, em português sem limite de chamados, os níveis de severidade estão detalhados em SLA – Acordo de Nível de Serviço.
- d) Realizar o acompanhamento das atualizações Update e Upgrade no durante o período de contrato.
- e) Suporte Remoto (via Webex, VPN, SSH, HTTPS) para realização de manutenção periódica e ajustes do Firewall.
- f) Equipe disponível durante 24 horas x 365 dias para atendimento remoto e/ou onsite com mobilização e deslocamento em até 2 horas após acionamento e orientações do CRQ-IV. Essa equipe será acionada em casos críticos de parada na rede ocasionados por quaisquer ameaças, devendo a contratada solucionar definitivamente o problema em até 4 horas.
- g) Nos casos de deslocamento dos técnicos da Contratada até a sede do CRQ-IV para suporte técnico não poderá haver custo adicionais. O custo de deslocamento ficará por conta da Contratada.
- h) Visita técnica programada para a realização de manutenções preventivas e corretivas do sistema, geração de relatórios técnicos e melhorias no ambiente de forma geral. Essa visita deverá ocorrer, no mínimo, 1 (uma) vez a cada 30 dias.
- i) A contratada deverá disponibilizar equipamento da mesma marca com características iguais ou superiores ao utilizado pelo CRQ-IV para contingência em caso de defeito, indisponibilidade, intermitência ou quaisquer outros defeitos que causem impacto direto na disponibilidade dos recursos de rede do CRQ-IV.
- j) A substituição do equipamento defeituoso deverá ocorrer em até 2 horas.
- l) Disponibilização das atualizações de versão e patches de correção dos drivers de componentes durante o tempo de garantia e do contrato;
- m) Acesso online a documentação e recursos técnicos, base de conhecimento e fóruns de discussão;
- n) Número ilimitado de requisições de suporte;
- o) Acesso aos recursos de suporte através de telefone e página da Internet.



p) Os serviços de suporte técnico deverão prevenir o surgimento de problemas nos produtos e auxiliar na solução deles, através de visita mensal preventiva a ser programada e realizada por técnico da contratada, observando os itens abaixo:

- p.1) Atualização de microcódigos, firmwares, drivers e softwares utilitários;
- p.2) Alteração e adaptação de configurações dentro do escopo contratado;
- p.3) Instalação e desinstalação de módulos e componentes dentro do escopo contratado referente à problemas e/ou falhas ocorridas;
- p.4) Quaisquer outras intervenções na solução de forma a assegurar o bom funcionamento dela, de acordo com as necessidades do CRQ-IV.
- p.5) Deverá ser possível notificar incidentes de falhas à CONTRATADA, via atendimento telefônico, no regime de 24 horas por dia, sete dias por semana, incluindo os feriados, locais, regionais e nacionais. Os chamados telefônicos notificando incidentes deverão ser atendidos em língua portuguesa pela central de atendimento da CONTRATADA;
- p.6) A CONTRATADA deverá disponibilizar relatório com informações sobre o atendimento aos chamados elaborados pelo técnico após as visitas ou atendimentos, detalhando quais procedimentos foram realizados.

#### Nível de Serviços - SLA

- O objetivo deste Acordo de Nível de Serviço (SLA) é definir as responsabilidades e dependências entre a CONTRATADA e o CONTRATANTE para os serviços e produtos contratados.
- Os acordos operacionais previstos neste documento não devem ter precedência nem limitar as respectivas obrigações e responsabilidades já descritas no contrato feito entre o CRQ-IV e a CONTRATADA.
- Este SLA descreve como o CRQ-IV e a CONTRATADA irão tratar seu relacionamento, para assegurar que os serviços serão corretamente entregues ao CRQIV.
- Define os compromissos requeridos entre a CONTRATADA - como provedora de serviços e tecnologias e o CRQ-IV, para a entrega dos serviços contratados.



## SEVERIDADE

Os níveis abaixo devem ser observados para classificação de severidade na abertura de chamados ao Suporte Técnico, devendo ser registrados no momento do atendimento.

Severidade	Descrição	Tempo máximo para início do atendimento	Penalidade por descumprimento
Emergencial	Falha no sistema, fora de operação, interrompido	Até 1 hora	Multa de 10% do valor pago mensalmente por incidente ocorrido
Mau Funcionamento	Falha intermitente em serviços suportados que torne o ambiente lento ou em pequenos grupos a operação está afetada, mas sem interrupção. Ajustes de configuração para liberação de acesso a sites restritos ou downloads de arquivos cuja extensões estejam bloqueadas.	Até 2 horas	Multa de 10% do valor pago mensalmente por incidente ocorrido
Atividade Remota Programada	Realização de manutenção preventiva, atualizações e atividades agendadas.	Até 12 horas	Multa de 5% do valor pago mensalmente por incidente ocorrido

- A Contratada permitirá que um técnico da equipe do CRQ-IV possa realizar ajustes das permissões quanto aos acessos a sites e arquivos bloqueados aos usuários cujo objetivo é tornar a demanda destes serviços com agilidade. O CRQ-IV ficará obrigado a comunicar a CONTRATADA as alterações que realizar na configuração do firewall.
- Os prazos acima relacionados serão computados a partir do momento de abertura do chamado pelo funcionário do CRQ-IV a central de suporte da CONTRATADA.





#### 6.18 CRITÉRIOS PARA ABERTURA DE CHAMADOS TÉCNICOS

- A CONTRATADA deverá prestar o serviço de suporte nas modalidades, presencial, Web ou telefônica, em idioma português do Brasil.
- A CONTRATADA deverá manter o serviço de suporte técnico disponível para abertura e acompanhamento de chamados em tempo integral 24 x 7 (vinte e quatro horas por dia, sete dias por semana, todos os dias do ano, inclusive sábados, domingos e feriados).
- CONTRATADA deverá garantir que o CRQ-IV efetue um número ilimitado de chamados de suporte durante a vigência do Contrato para suprir suas necessidades de utilização, sem ônus adicional para o CRQ-IV.
- A CONTRATADA deverá fornecer ao CRQ-IV um número de telefone que possibilite ligações para sua o suporte técnico, para fins de abertura e acompanhamento de chamados. A CONTRATADA deverá fornecer ao CRQ-IV acesso a pelo menos 3 (três) pessoas autorizadas para abertura e acompanhamento de chamados de suporte.
- Na abertura de cada chamado técnico deverá ser emitido um registro contendo informações detalhadas do chamado.
- Uma vez feito o contato por este número de telefone, a CONTRATADA terá os prazos estabelecidos nos termos deste Acordo de Nível de Serviços para dar uma solução à ocorrência, conforme seu grau de severidade.

#### 6.19 OBRIGAÇÕES DA CONTRATADA

- Manter o CONTRATANTE sempre informado de todas as versões e atualizações de software disponibilizadas pelos fabricantes dos softwares contratado, entregando a documentação relativa à nova versão entregue.
- Sempre que solicitado, fornecer boletins técnicos e manuais de uso atualizados.
- A CONTRATADA deverá fornecer ao CRQ-IV, proativamente as atualizações, modificações e/ou melhorias introduzidas nos softwares tão logo haja disponibilidade do material.
- A CONTRATADA deverá informar proativamente ao CRQ-IV sobre a descoberta de bugs nos softwares contratados, durante toda a vigência do contrato.
- A CONTRATADA deverá divulgar para o CRQ-IV as descrições destes bugs e seus possíveis impactos.



- A CONTRATADA deverá apresentar ao CRQ-IV, as informações sobre patches de correção e o local disponível na Internet onde tais atualizações estarão disponíveis, com as A CONTRATADA deverá indicar a localização na Internet, para download, das correções lançadas (patches).
- O CRQ-IV deverá ter como opção executar ou não as atualizações de softwares disponibilizadas.
- Não divulgar dados ou informações relacionadas aos serviços e produtos objeto do presente, mantendo sigilo absoluto em relação a todos os dados acessados ou que venham a ser gerados, no processo de prestação dos serviços tendo como referência a Lei Geral de Proteção de Dados.
- Serão de inteira responsabilidade e às expensas da CONTRATADA, sem nenhum custo adicional para o CRQ-IV:
  - a) Apoio, suporte técnico e logístico eventualmente necessário ao adequado funcionamento da solução;
  - b) Disponibilização de profissionais qualificados para execução das atividades do projeto e todas as obrigações trabalhistas relacionadas em dia conforme legislação específica;
  - c) Todos os ônus relativos a transporte, alimentação, e hospedagem de profissionais, transporte e instalação dos equipamentos, ligações telefônicas para suporte técnico durante o processo de implantação da solução, montagem física dos equipamentos que compõem a solução, disponibilização de ferramentas e insumos diversos requeridos durante qualquer das fases de implantação da solução;
  - d) Configuração lógica dos componentes da solução proposta de forma a viabilizar integralmente os testes a serem realizados como parte da homologação da solução e o adequado funcionamento em ambiente de produção;
  - e) Atividades de concepção, projeto, planejamento, implementação, suporte técnico, assistência técnica e apoio logístico eventualmente necessário à adequada implantação da solução;
  - f) Demonstração de todas as características técnicas e funcionalidades previstas na contratação, durante a fase de homologação de funcionalidades da solução;



- g) Deverá acionar o suporte técnico diretamente do fabricante dos equipamentos e componentes de sua proposta de preço, caso necessário para a adequada implantação da solução;
- h) Especificações técnicas de toda a solução para efeito de instalação elétrica, climatização e pesos.
- Correrão por conta, responsabilidade e risco da CONTRATADA as consequências de:
    - a) Sua negligência, imperícia, imprudência e/ou omissão;
    - b) Ato ilícito seu, de seus empregados ou de terceiros em tudo que se referir ao objeto desta licitação;
    - c) Cumprir durante a execução do objeto todas as leis e posturas federais estaduais e municipais pertinentes e vigentes, sendo a única responsável por prejuízos decorrentes de infrações a que houver dado causa;
    - d) Manter, durante o período de contratação, o atendimento das condições de habilitação exigidas na licitação.
    - e) Demais disposições contidas no instrumento contratual.

## **7 – Análise comparativa de soluções:**

Inciso II, do artigo II da Instrução Normativa SGD-ME nº 94/2022

7.1 A diferença entre usar um firewall do tipo appliance (físico/dedicado) e um firewall em nuvem (virtual ou cloud-based) envolve aspectos de infraestrutura, gerenciamento, custos e cenários de uso. Considerando as características de cada solução, a melhor que se aplica as necessidades do CRQ-IV é a contratação do firewall do tipo appliance (físico/dedicado).

Critério	Firewall Appliance (físico/dedicado)	Firewall em Nuvem (cloud-based/virtual)
Infraestrutura	Equipamento físico instalado no datacenter/rede local	Serviço virtual hospedado em provedor de nuvem ou como FWaaS
Modelo de custo	CAPEX (aquisição, suporte e manutenção)	OPEX (assinatura/pagamento por uso)
Desempenho	Alto, pois usa hardware dedicado otimizado	Variável, depende da infraestrutura do provedor e do plano contratado
Escalabilidade	Limitada ao hardware adquirido (precisa trocar/expandir)	Elástica, cresce sob demanda
Controle físico	Total, pois o equipamento é da	Indireto, dependente do provedor de



Critério	Firewall Appliance (físico/dedicado)	Firewall em Nuvem (cloud-based/virtual)
	instituição	nuvem
Cenário ideal de uso	Datacenters on-premises, ambientes críticos de rede local	Ambientes híbridos, multi-cloud e acesso remoto distribuído
Disponibilidade (HA)	Necessita dois appliances em redundância	Alta disponibilidade nativa da nuvem (depende do SLA contratado)
Atualizações	Dependem do time interno ou contrato de suporte	Feitas automaticamente pelo provedor ou via painel de gestão
Latência	Baixa, pois o tráfego é processado localmente	Pode ser maior, dependendo da rota até a nuvem
Conectividade	Funciona mesmo sem internet (protege rede interna)	Depende de conexão estável à nuvem
Conformidade/Segurança	Mais indicado quando há exigência de controle físico do ambiente	Atende melhor quando há necessidade de distribuição e integração com SaaS e cloud

- Firewall Appliance: melhor para proteger redes locais e datacenters próprios, com alto desempenho e controle físico, mas menos flexível para expansão.
- Firewall em Nuvem: melhor para proteger aplicações e usuários em ambientes híbridos ou 100% cloud, com escalabilidade e flexibilidade, mas dependente do provedor e da conectividade.

## 7.2 – Necessidades similares em outros órgãos ou entidade da Administração Pública e as soluções adotadas.

Inciso II, letra “a” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Órgãos e entidades da Administração Pública utilizam, de forma ampla, sistemas de segurança baseados em firewall como um dos principais mecanismos para a gestão da segurança da informação.

Por que usam:

- O firewall é a primeira camada de defesa da rede institucional, protegendo contra acessos indevidos, ataques cibernéticos, vazamentos de dados e tentativas de indisponibilidade de serviços.



- Atende às exigências normativas, como a Instrução Normativa SGD-ME nº 94/2022, que determina a adoção de medidas de proteção para garantir a confidencialidade, integridade e disponibilidade da informação.
- É um requisito para conformidade com a Lei Geral de Proteção de Dados (LGPD), pois auxilia na prevenção de incidentes de segurança que possam expor dados pessoais.

Exemplos de uso na Administração Pública:

- Ministérios e autarquias utilizam firewalls appliance em seus datacenters para proteger redes internas e serviços críticos.
- Tribunais e órgãos de justiça aplicam firewalls de última geração (NGFW) para controlar acessos e inspecionar tráfego criptografado.
- Instituições de ensino e pesquisa públicas usam firewalls para segmentar redes, proteger usuários e monitorar conexões.
- Órgãos financeiros e arrecadatários (ex.: Receita Federal, bancos públicos) utilizam firewalls robustos em alta disponibilidade (HA) para assegurar serviços online 24/7.

Ou seja, o uso de firewalls (appliance ou em nuvem) é prática consolidada na Administração Pública como parte da gestão da segurança da informação e da governança digital.

#### 7.3 – As alternativas de mercado:

Inciso II, letra “b” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

As alternativas de mercado consideradas foram: firewall em nuvem e firewall do tipo appliance. Optou-se pela contratação de firewall do tipo appliance, por atender melhor aos requisitos de desempenho, resiliência, segurança da informação e conformidade com normativos aplicáveis à Administração Pública. Além do que o órgão já possui uma estrutura de segurança da informação baseado neste modelo.

#### 7.4 – A existência de softwares disponíveis conforme descrito na Portaria STI/MP Nº 46, de 28/09/2016

Inciso II, letra “c” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.



7.5 – As políticas, os modelos e os padrões de governo, a exemplo dos Padrões de Interoperabilidade de Governo Eletrônico – ePing, Modelo de Acessibilidade em Governo Eletrônico – eMag, Padrões Web em Governo Eletrônico – ePwg, padrões de Design System de governo, Infraestrutura de Chaves Públicas Brasileira – ICP Brasil e Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos – e-ARQ Brasil, quando aplicáveis

Inciso II, letra “d” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

7.6 – As necessidades de adequação do ambiente do órgão para viabilizar a execução contratual  
Inciso II, letra “e” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

A substituição do firewall Sonicwall modelo NSA 2700 pelo modelo NSA 2800 exige a adequação do ambiente computacional em aspectos físicos, lógicos e operacionais. No âmbito da infraestrutura, devem ser avaliados espaço em rack, disponibilidade elétrica e compatibilidade de cabeamento e interfaces de rede. No campo lógico, faz-se necessária a migração e revisão das regras de segurança, objetos, políticas de firewall, VPNs e inspeção de tráfego, assegurando sua plena integração com serviços já existentes, como diretórios de autenticação, proxies e sistemas de monitoramento. Operacionalmente, é imprescindível a capacitação da equipe técnica para utilização dos novos recursos do equipamento, bem como a atualização de procedimentos de administração e resposta a incidentes. Além disso, caso o ambiente utilize configuração em alta disponibilidade (HA), deve-se realizar a devida adequação e testes de failover para garantir continuidade dos serviços. Tais medidas asseguram que a nova solução opere em conformidade com os requisitos de desempenho e segurança, mantendo a integridade e a disponibilidade dos serviços essenciais da organização.

7.7 – Os diferentes modelos de prestação de serviços;  
Inciso II, letra “f” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

7.8 – Os diferentes tipos de soluções em termos de especificação, composição ou características dos bens e serviços integrantes;  
Inciso II, letra “g” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.



7.9 – A possibilidade de aquisição na forma de bens ou contratação como serviço;  
Inciso II, letra “h” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

O objeto desta contratação será como serviço.

7.10 – A ampliação ou substituição da solução implantada;  
Inciso II, letra “i” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Substituição da solução implantada.

7.11 – As diferentes métricas de prestação de serviço e de pagamento;  
Inciso II, letra “j” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Os pagamentos dos serviços contratados serão realizados mensalmente.

8 – Análise comparativa de custos das soluções técnica e funcionalmente viáveis:  
Inciso III, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

8.1 – Comparação de custos totais de propriedade:  
Inciso III, letra “a” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.

8.2 – Memória de cálculo que referencie os preços e os custos utilizados na análise  
Inciso III, letra “b” do artigo 11 da Instrução Normativa SGD-ME nº 94/2022

Não se aplica.



**9 – Estimativa do custo total da contratação:**  
**Inciso IV, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022**

9.1 Para alcançar a melhor contratação, mediante a competitividade em busca da proposta mais vantajosa. O custo estimado desta contratação possui caráter sigiloso e será tornado público apenas e imediatamente após o julgamento das propostas.

**10 Identificação dos benefícios a serem alcançados**  
**Inciso V, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022**

10.1 Os benefícios da contratação de um sistema de segurança da informação baseado em firewall do tipo appliance podem ser descritos diretamente em relação aos princípios de economicidade, efetividade, eficiência e eficácia, que são exigidos na Administração Pública.

Economicidade	Investimento em solução dedicada, com maior vida útil e menor risco de gastos emergenciais com incidentes de segurança. Maior previsibilidade orçamentária, evitando despesas decorrentes de ataques, indisponibilidade ou multas por descumprimento da LGPD.
Efetividade	Atendimento pleno ao objetivo de proteger a rede contra acessos não autorizados, ataques cibernéticos e vazamento de dados. Permite aplicar políticas de segurança adequadas ao ambiente, de forma consistente e centralizada. Suporte a recursos avançados (NGFW, IPS, inspeção SSL, sandboxing), garantindo proteção em múltiplas camadas
Eficiência	Equipamento de uso exclusivo para segurança, com hardware otimizado e throughput elevado, garantindo melhor desempenho na filtragem de tráfego. Monitoramento centralizado e geração de relatórios automatizados, otimizando o trabalho da equipe de TI. Possibilidade de operação em alta disponibilidade (HA), garantindo continuidade de serviços críticos com menor esforço de gestão.
Eficácia	Cumprimento dos objetivos estratégicos de segurança da informação, alinhados às normas da Administração Pública e à LGPD. Redução significativa da probabilidade e do impacto de incidentes de segurança. Melhoria da confiança e disponibilidade dos serviços digitais oferecidos ao cidadão e aos servidores públicos.
Objetivo Estratégico	OE11 – Adotar as melhores práticas de Governança e Gestão e OE12 – Promover a inovação de processos e serviços, por meio de melhoria contínua e das ferramentas de Inteligência Artificial.





10.2 A contratação de firewall do tipo appliance assegura uma solução economicamente viável, efetiva na proteção, eficiente na operação e eficaz no atendimento aos objetivos de segurança da informação, oferecendo proteção robusta, continuidade de serviços e conformidade legal para os órgãos da Administração Pública.

10.3 Elemento Despesa: 33.90.39.007-Locação de Máquinas e Equipamentos

**11 – Declaração de Viabilidade da Contratação:**  
**Inciso V, do artigo 11 da Instrução Normativa SGD-ME nº 94/2022**

A contratação de um sistema de segurança da informação baseado em firewall do tipo appliance é viável e justificada para os órgãos e entidades da Administração Pública, considerando os seguintes aspectos:

- Viabilidade Técnica
  - a) O firewall appliance atende aos requisitos de segurança, desempenho, confiabilidade e alta disponibilidade necessários à proteção da rede institucional.
  - b) É compatível com a infraestrutura de rede existente, suportando integrações com VPN, autenticação corporativa, sistemas de monitoramento e SIEM.
- Viabilidade Econômica
  - a) A aquisição proporciona economicidade, pois reduz riscos de incidentes, evita custos emergenciais com indisponibilidade de serviços ou ataques cibernéticos, e tem vida útil prolongada.
  - b) O investimento é justificado frente aos benefícios de proteção e continuidade operacional.
- Viabilidade Operacional e Administrativa
  - a) A equipe técnica está capacitada para gerenciar e operar o equipamento, garantindo eficiência no monitoramento, aplicação de políticas de segurança e resposta a incidentes.
  - b) Procedimentos de manutenção, atualização e alta disponibilidade podem ser implementados sem impacto relevante nos serviços.



- Viabilidade Legal e Normativa
  - a) A solução está em conformidade com a IN SGD-ME nº 94/2022, a LGPD e demais normativos de segurança da informação aplicáveis à Administração Pública.
  - b) Atende aos requisitos de governança, confidencialidade, integridade e disponibilidade das informações.

## 12 Classificação quanto ao acesso a informação

- 12.1 Nos termos da Lei nº 12.527, de 18 de novembro de 2011, o presente Estudo não se classifica como sigiloso.

São Paulo, 07 outubro de 2025.

Equipe Técnica de Planejamento da Contratação

Alexandre de Paula  
Integrante Requisitante

Claudio A. Gimenez  
Integrante Técnico

Aprovação

Alexandre de Paula  
Gerente / Tecnologia da Informação