ETP – Estudo Técnico Preliminar
AV – Análise de Viabilidade

1. IDENTIFICAÇÃO DO PROJETO

Projeto: DP- 3683 - [2025] **Id. TraceGP:** 14393	Aquisição de solução de *firewall* de próxima geração (NGFW), com garantia de 36 meses, contemplando *hardware* e *software*, com instalação, configuração, monitoramento, suporte especializado e serviços gerenciados e solução de proteção de *e-mail* corporativo.
Gerente de Projeto:	Lucas Luiz Ribeiro dos Santos

2. PROCESSO SEI

Processo Sei:	0141119-38.2025.8.13.0000

3. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

Equipe de Planejamento da Contratação			
Matrícula	Nome	Área	Integrante demandante / técnico / administrativo /gestor
T0067066	Deilson Antônio Vieira	COINFRA	Integrante técnico
T0063545	Humberto Vieira Maldonado	COINFRA	Integrante técnico
T0063503	Eric Augusto Fernandes	COINFRA	Integrante técnico
T0076802	Eduardo Henrique de Oliveira Horta	COINFRA	Integrante técnico
T0013359	Denilson dos Santos Rodrigues	COINFRA	Integrante técnico
F0353920	Narciso Felicio de Lima Junior	GETEC	Integrante demandante e Gestor técnico

4.FUNDAMENTO

4.1. Necessidade

Visa-se à aquisição perpétua de uma solução de proteção de rede baseada em *firewalls* de próxima geração (*Next Generation Firewall* – NGFW), com garantia mínima de 36 (trinta e seis) meses, abrangendo *hardware*, *software*, licenciamento completo e respectivos serviços de implantação, monitoramento e suporte técnico especializado em regime 24x7x365. O objetivo principal é assegurar a proteção contínua da rede institucional do Tribunal de Justiça de Minas Gerais (TJMG) contra ameaças cibernéticas cada vez mais sofisticadas, ampliando a visibilidade, o controle e a capacidade de prevenção de ataques, em total alinhamento com as melhores práticas de segurança da informação e os marcos regulatórios aplicáveis.

A solução deverá contemplar, obrigatoriamente, o fornecimento de *appliances* físicos dedicados para o ambiente *on-premise*, visando garantir alta performance, disponibilidade e controle da rede local, bem como a disponibilização de instâncias virtuais (VMs) devidamente licenciadas para os ambientes de nuvem pública, a fim de assegurar a proteção integrada e homogênea dos recursos computacionais em arquiteturas híbridas.

Adicionalmente, implantação de uma camada especializada de proteção de *e-mail* corporativo, com foco especial nas contas utilizadas por magistrados, frente ao aumento expressivo de ataques de *phishing*, engenharia social e fraudes direcionadas. Essa solução deverá envolver mecanismos avançados de detecção e resposta baseados em inteligência artificial, análise de reputação, *sandboxing* de anexos, validação de remetentes (SPF, DKIM, DMARC) e mecanismos de quarentena, mitigando riscos de comprometimento e garantindo a integridade da comunicação institucional, elemento crítico à segurança e confiabilidade das informações trocadas no âmbito do Poder Judiciário.

Tal abordagem visa garantir a continuidade dos serviços críticos prestados à sociedade e à Justiça, tornando imprescindível a adoção de medidas que promovam a resiliência cibernética e a mitigação de riscos, considerando a evolução do modelo de arquitetura de rede e a crescente demanda por segurança em múltiplos domínios operacionais.

4.2. Contextualização/Motivação

O Tribunal de Justiça do Estado de Minas Gerais (TJMG), buscando a excelência na prestação jurisdicional e a segurança da informação, deve manter sua infraestrutura de Tecnologia da Informação e Comunicação (TIC) atualizada e coerente com a capacidade necessária de resposta contra ameaças internas e externas.

As atividades do Tribunal, principalmente as atividades-fim (processo judicial e atividades correlatas), estão fortemente amparadas no uso intensivo da tecnologia de informação e de processamento de dados, e um eventual comprometimento de sistemas corporativos teria impacto direto no trabalho, em um ou mais pilares de segurança como confidencialidade, integridade, disponibilidade e autenticidade, bem como na própria credibilidade institucional. Tal impacto pode abranger não só os usuários internos, como também público externo partícipe do processo judicial eletrônico (advogados, partes, Ministério Público, Defensoria, auxiliares da Justiça etc.) e interessados nas informações e nos serviços para a sociedade e órgãos públicos**.**

A crescente demanda por serviços eletrônicos, como o Processo Judicial Eletrônico (PJe) e agora o novo Sistema de Processo Judicial e-Proc (eproc), impulsionou a necessidade de disponibilizar o acesso remoto e seguro aos recursos internos da infraestrutura tecnológica do Tribunal por meio da Internet.

Esse cenário exige soluções que garantam não apenas a disponibilidade, mas também a confidencialidade, integridade e rastreabilidade dos acessos realizados por magistrados, servidores, advogados e partes interessadas, especialmente em ambientes de mobilidade e *home office.*

O uso de sistemas judiciais como o PJe e a ampliação do Eproc reforça a urgência de investir em mecanismos robustos de segurança perimetral, autenticação forte, e monitoramento contínuo,

assegurando a continuidade das atividades jurisdicionais e a proteção de dados sensíveis processados no ambiente digital.

O Tribunal possui em seu portfólio de dispositivos de segurança de rede de TIC (Tecnologia da Informação e Comunicação) uma solução denominada *Next Generation Firewall,* do fabricante *Checkpoint,* modelo 26000.

A atual solução foi adquirida através do contrato 288/2020, cujo objeto englobou o fornecimento e os serviços de suporte, tendo sua vigência a encerrar em 26/11/2025.

Dentre as principais funções desempenhadas pela solução no ambiente de TIC do TRIBUNAL, destacamos:

a) ***Firewall:*** Inspeciona o tráfego de rede que tenta ingressar ou sair da rede interna à internet, aplicando um conjunto de regras predefinidas para permitir ou bloquear conexões com base em diversos critérios, como endereços IP de origem e destino, portas de comunicação e protocolos de rede (TCP, UDP, etc.). Essa capacidade de controle granular impede o acesso não autorizado a serviços e dados sensíveis.

b) **Sistema de Prevenção de Intrusões (IPS):** Detecta e bloqueia tentativas de explorar vulnerabilidades em sistemas e aplicativos, como ataques de *buffer overflow*, varreduras de portas e ataques de negação de serviço (DoS).

c) **Antivírus e *Anti-Malware:*** Inspeciona o tráfego em busca de vírus, *worms*, *trojans* e outros tipos de *malware*, bloqueando ou removendo ameaças.

d) **Controle de Aplicações:** Identifica e controla o tráfego de aplicativos específicos, permitindo ou bloqueando seu uso com base em políticas. Isso é útil para controlar o uso de aplicativos de mensagens instantâneas, redes sociais, etc.

e) **VPN (Rede Privada Virtual):** Permite conexões seguras e criptografadas entre redes ou entre usuários remotos e a rede da organização.

f) **NAT (Tradução de Endereços de Rede):** O NAT permite que múltiplos dispositivos na rede interna compartilhem um único endereço IP público para se comunicarem com a internet. Além de otimizar o uso de endereços IP, o NAT adiciona uma camada de segurança ao ocultar os endereços IP internos, tornando a rede menos visível para atacantes externos.

g) ***Clustering*** **e Alta Disponibilidade:** Permite configurar vários *firewalls* em um cluster para fornecer redundância e garantir a continuidade dos negócios em caso de falha de *hardware*.

h) **Relatórios e *Logs*:** O *firewall* mantém registros das atividades de rede, incluindo tentativas de conexão, tráfego permitido ou bloqueado, e eventos de segurança.

O *firewall* de perímetro exerce um papel estratégico na arquitetura de rede do TJMG, posicionando-se como ponto central de interconexão entre a rede de dados institucional e a Internet. Além de

controlar o tráfego de entrada e saída, ele também opera como camada de roteamento (*Layer* 3) para as redes *wireless* da instituição, sendo responsável pela aplicação de políticas de segurança, segmentação de tráfego e garantia de conectividade para os usuários. Sua posição o torna um elemento crítico tanto para a segurança quanto para a disponibilidade dos serviços digitais do Tribunal.

Nos ambientes em nuvem pública utilizados pelo Tribunal, especificamente nas plataformas AWS (*Amazon Web Service*) e OCI (*Oracle Cloud Infrastructure*), a proteção da rede é realizada exclusivamente por meio de *firewalls* nativos oferecidos pelas respectivas nuvens. Tal solução oferece funcionalidades básicas de controle e filtragem, não atendendo de forma plena aos requisitos avançados de visibilidade, correlação de eventos e prevenção de ameaças.

Nas unidades conectadas por meio do Cinturão Digital e nos prédios estratégicos interligados via infraestrutura MPLS, o roteamento entre as redes locais é executado diretamente por *switches* com capacidade de camada 3 (*Layer 3*). Embora essa configuração atenda aos requisitos básicos de conectividade, ela impõe uma limitação significativa em termos de visibilidade e controle sobre o tráfego leste-oeste — ou seja, o tráfego que circula internamente entre diferentes segmentos de rede dentro da mesma unidade. A ausência de um ponto centralizado de inspeção e controle dificulta a aplicação de políticas de segurança granulares e impede a detecção eficaz de movimentações laterais típicas de ataques sofisticados. Essa lacuna representa um risco para a integridade do ambiente e compromete a capacidade de resposta a incidentes. Diante disso, torna-se fundamental a adoção de mecanismos complementares, como *firewalls* dedicados para segmentação interna, a fim de reforçar a governança, ampliar a visibilidade e alinhar a proteção dessas unidades à arquitetura de segurança institucional do Tribunal.

Outro ponto relevante, é a proteção dos *e-mails* institucionais, que apesar da utilização do Gmail como solução principal de correio eletrônico institucional, da solução de colaboração do *Google Workspace*, cuja camada nativa de segurança oferece funcionalidades básicas de proteção contra *spam*, *malware* e *phishing*, observa-se que esse nível de proteção já não é mais suficiente diante do avanço e da sofisticação dos ataques por *e-mail*. A evolução das técnicas de *phishing, spear phishing*, BEC (*Business Email Compromise*) e campanhas de engenharia social altamente direcionadas demanda a adoção de uma camada adicional de defesa que vá além dos filtros convencionais.

A superfície de ataque do Tribunal expandiu-se de forma significativa nos últimos anos, impulsionada pela adoção em larga escala de modelos de trabalho híbrido, aplicações em nuvem, dispositivos IoT (*Internet of Things,*) e serviços SaaS (*Software as a Service*). Paralelamente, o cenário de ameaças tem se tornado cada vez mais complexo e ágil, com agentes maliciosos se beneficiando do fácil acesso a ferramentas automatizadas e técnicas sofisticadas de exploração.

Nesse novo contexto, as abordagens tradicionais de segurança de rede mostram-se insuficientes para garantir a proteção necessária. Diante disso, a motivação para a adoção de uma nova solução

de *Next Generation Firewall* (NGFW) com capacidade nativa de atuar como *proxy* e roteamento de redes internas está diretamente ligada à necessidade de ampliar a segurança, performance, observabilidade e disponibilidade na saída para a internet e no roteamento do tráfego do cinturão digital do TJMG, permitindo visibilidade e controle sobre o tráfego leste-oeste, que atualmente não é inspecionado nem monitorado de forma estruturada. Essa mudança representa um avanço significativo na postura defensiva da instituição, ao estender a aplicação de políticas de segurança e detecção de ameaças para além da borda da rede, cobrindo também os fluxos internos entre os diversos segmentos da infraestrutura digital. Essa evolução tecnológica permitirá a substituição de uma infraestrutura legada, que presenta limitações técnicas, tornando-se um ponto crítico de instabilidade e risco operacional. A nova solução trará ganho expressivo em visibilidade e controle do tráfego *web*, permitindo a consolidação das camadas de segurança em um único dispositivo de borda, com inspeção de tráfego HTTPS, filtragem de conteúdo, prevenção de ameaças e políticas centralizadas.

Conforme *assessment* técnico realizado em abril do ano corrente pelo fabricante atualmente responsável pela solução de *firewall* em uso no TJMG, foi identificado que o modelo atual de saída para a internet, baseado na utilização de *proxies open source*, não atende adequadamente aos requisitos de performance, disponibilidade e segurança exigidos pelas plataformas modernas de NGFW (*Next Generation Firewall*) e SWG (*Secure Web Gateway*). Importante destacar que os resultados desse *assessment* foram considerados de forma estritamente agnóstica neste estudo técnico preliminar, tendo como base única os requisitos técnicos e operacionais do TJMG. A análise evidenciou a necessidade de reestruturação da arquitetura de rede, priorizando aspectos como ampliação da visibilidade, controle eficaz do tráfego leste-oeste, simplificação da gestão operacional e fortalecimento da resiliência cibernética diante das ameaças cada vez mais sofisticadas.

Embora o *firewall* atualmente implantado conte com licenciamento para funcionalidades como *App Control* e *URL Filtering*, o relatório técnico aponta que a inspeção de tráfego HTTPS, essencial para proteção contra ameaças modernas, exigiria um *upgrade* significativo de *hardware*, dado que a plataforma em uso apresenta limitações de processamento que inviabilizam essa funcionalidade de forma eficaz.

O *assessment* também destacou o aumento expressivo do volume de tráfego de rede, o que levou à adoção de uma estratégia de distribuição de carga, onde aproximadamente 80% dos acessos são direcionados ao *link* principal (*Blink*) e os 20% restantes ao *link* secundário (Algar). Para que o ambiente suporte com estabilidade tanto a carga atual (entre 3,5 Gbps e 4 Gbps), quanto a expansão prevista para até 10 Gbps, o fabricante recomenda a atualização da infraestrutura de *hardware*, sendo o porte do *upgrade* condicionado à necessária segregação de redes, prática comum e recomendada em ambientes de porte semelhante ao do TJMG.

O relatório ainda aponta que apesar de o ambiente contar com a suíte *SandBlast*, que oferece um conjunto abrangente de recursos de prevenção de ameaças, funcionalidades importantes como

Threat Extraction e *Zero Phishing* não estão ativas. A ativação dessas funcionalidades, bem como o pleno aproveitamento das tecnologias de *Threat Prevention*, *Application Control* e URL *Filtering*, demandam a habilitação da Inspeção SSL. Embora tal funcionalidade esteja configurada, ela não está inspecionando o tráfego HTTPS, devido à limitação de recursos computacionais. O relatório técnico concluiu que essa inspeção deve ser ativada apenas após um *upgrade* de *hardware* ou mediante uma segregação adequada do ambiente, de forma a preservar a estabilidade operacional.

Ainda segundo o *assessment*, a funcionalidade de acesso remoto (*VPN Client-to-Site*) atualmente está em uso com integração ao *Active Directory*, mas não há validação de postura nem autenticação multifator (MFA), o que enfraquece a segurança da conexão remota.

Além do *assessment* técnico conduzido pelo fabricante atualmente responsável pela solução de segurança de perímetro do TJMG, o Gartner, reconhecido mundialmente por sua autoridade em pesquisa e consultoria imparcial em tecnologia, também apresenta recomendações estratégicas altamente alinhadas com os desafios enfrentados pelo Tribunal. Segundo o Gartner, as operações de rede tradicionais, muitas vezes baseadas em processos manuais e fragmentados, precisam evoluir para modelos mais integrados, automatizados e orientados por inteligência artificial, sobretudo nos próximos três a cinco anos. Como orientação para modernização da infraestrutura, a entidade recomenda priorizar soluções que ofereçam automação nativa, APIs abertas, integração entre as equipes de rede e segurança, além de suporte às arquiteturas modernas como SD-WAN, ZTNA e SASE.

Essas diretrizes reforçam a necessidade da adoção de tecnologias de última geração, como os *Next Generation Firewalls* (NGFWs) com capacidade nativa de atuação como *proxy*, que são capazes de fornecer visibilidade, controle e proteção de alto nível em ambientes híbridos, distribuídos e de grande escala como o do TJMG.

Nesse contexto, o Gartner define o mercado de *firewalls* de rede como composto por soluções projetadas para realizar inspeção bidirecional de tráfego com estado, ou seja, capazes de analisar tanto o tráfego de entrada quanto o de saída para garantir a integridade e segurança da rede. Esses *firewalls* podem ser implementados com *appliances* físicos, dispositivos virtuais ou controles nativos em ambientes de nuvem, e são compatíveis com diversas arquiteturas: *on-premises*, híbridas ou baseadas inteiramente em nuvem pública ou privada.

Entre os principais recursos dessas soluções, o Gartner destaca:

- Suporte a tabelas de roteamento com tradução de endereços DNAT e SNAT, promovendo maior flexibilidade de arquitetura;
- Inspeção de tráfego baseada em regras com estado, oferecendo controle minucioso das conexões de rede;

- Sistemas de prevenção de intrusão (IPS) e inspeção de *malware* integrados, que ampliam significativamente a capacidade de detecção e resposta a ameaças;
- Filtragem avançada de tráfego de saída, cobrindo protocolos como HTTP, HTTPS e aplicações, o que garante o uso adequado da internet no ambiente institucional;
- Registro detalhado das ações administrativas com geração de relatórios customizáveis e granulares, permitindo visibilidade analítica sobre comportamentos, objetos e tipos de tráfego suspeitos.

Dentre as capacidades opcionais e avançadas, destacam-se:

- *Sandboxing* de rede, que analisa objetos suspeitos em ambientes isolados, atribuindo pontuações de risco com base em seu comportamento;
- Acesso com confiança zero (ZTNA), permitindo políticas dinâmicas baseadas na identidade do usuário e no contexto de acesso;
- Segurança de DNS, com recursos avançados de detecção e bloqueio de ameaças baseadas na camada DNS;
- Seleção dinâmica de caminhos de rede, com base em políticas centralizadas, VPNs de alta disponibilidade e configuração zero-*touch*, ideal para redes distribuídas que exigem alta escalabilidade e disponibilidade contínua.

Além disso, o Gartner reforça em seus relatórios mais recentes a importância de ampliar a proteção do correio eletrônico institucional por meio da adoção de soluções modernas de *Email Security*, recomendando a implementação de camadas adicionais como *Secure Email Gateways* (SEG) e *Integrated Cloud Email Security* (ICES), de forma complementar ou independente, conforme o perfil de risco da organização. Tais soluções são essenciais para enfrentar o crescimento acelerado dos ataques de *phishing, spear phishing* e *quishing* — cada vez mais sofisticados e impulsionados por ferramentas de Inteligência Artificial. O Gartner recomenda ainda que organizações públicas e privadas invistam em plataformas que ofereçam detecção com base em aprendizado de máquina, validação reforçada de remetentes (SPF, DKIM e DMARC), *sandboxing* de anexos, análise de reputação e proteção de dados sensíveis em e-*mails* de saída. No caso do TJMG, esse direcionamento é especialmente relevante para proteger contas críticas, como as de magistrados, que são alvos preferenciais de ataques direcionados e fraudes de engenharia social.

5. Alinhamento estratégico

Aquisição de solução de proteção de rede baseada em *firewall* de próxima geração (*Next Generation Firewall* – NGFW), e solução de prevenção de ameaças e *spam* para *e-mail* em nuvem, está alinhada aos seguintes instrumentos de planejamento do Tribunal de Justiça de Minas Gerais (TJMG):

a) **Plano Estratégico Institucional (PEI) 2021–2026**
https://www.tjmg.jus.br/portal-tjmg/informes/planejamento-estrategico-2021-2026-perspectiva-aprendizagem-e-crescimento.htm

- **Macrodesafio:** Fortalecimento da Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário.
- **Iniciativa Estratégica:** Fortalecer as estratégias digitais do TJMG e a melhoria da governança, da gestão e da infraestrutura tecnológica, garantindo proteção aos dados organizacionais com integridade, confiabilidade, confidencialidade, integração, disponibilidade das informações, disponibilização dos serviços digitais ao cidadão e dos sistemas essenciais da justiça, promovendo a satisfação dos usuários, por meio de inovações tecnológicas, controles efetivos dos processos de segurança e de riscos e da gestão de privacidade e uso dos dados pessoais.

b) **Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2025–2026**
https://www.tjmg.jus.br/portal-tjmg/transparencia/tecnologia-da-informacao-e-comunicacao/

- **Ação Estratégica:** Implementar e manter soluções de infraestrutura tecnológica que garantam a segurança, disponibilidade e continuidade dos serviços de TIC essenciais ao funcionamento do TJMG.

c) **Plano de Contratações Anual (PCA)**
https://www.tjmg.jus.br/portal-tjmg/transparencia/tecnologia-da-informacao-e-comunicacao/

- **Projeto:** A contratação está prevista no Plano de Contratações Anual do TJMG, conforme registro no Sistema de Planejamento e Gerenciamento de Contratações, atendendo às necessidades prioritárias identificadas para o exercício correspondente.

6.Requisitos da solução

6.1. Requisitos de Negócio

6.1.1. A solução a ser contratada deverá atender, no mínimo, aos seguintes requisitos de negócio:

a) Fornecimento de equipamentos do tipo *firewall* de próxima geração (*Next-Generation Firewall* – NGFW), conforme dimensionamento do TRIBUNAL, acompanhados dos sistemas complementares necessários à operação da solução, incluindo plataforma de gerenciamento centralizado, módulos de armazenamento e análise de *logs* e geração de relatórios técnicos e gerenciais.

b) Garantia mínima de 36 (trinta e seis) meses para todos os componentes da solução, abrangendo *hardware*, *software*, licenças, acessórios e demais itens integrados, com suporte técnico, atualizações, correções e substituições incluídas durante o período de vigência.

c) A implantação da solução deverá incluir a entrega física dos equipamentos no (s) local (is) indicado (s) pelo TRIBUNAL, instalação, configuração inicial, testes de funcionamento e

integração com a infraestrutura existente, bem como o acompanhamento técnico necessário para a entrada em operação da solução.

d) Implantação de *firewalls* virtuais (VM-*based*) específicos para ambientes de nuvem pública (como AWS e OCI), com funcionalidades equivalentes aos *appliances* físicos, garantindo inspeção profunda de tráfego, segmentação segura entre *workloads*, controle de políticas baseadas em identidade e aplicação, além de integração com a gestão centralizada da solução *on-premises*, assegurando visibilidade e padronização da política de segurança entre nuvem e datacenter.

e) Implantação de uma solução especializada de proteção de *e-mail* que integre recursos como análise preditiva baseada em inteligência artificial, *sandboxing* em tempo real, validação de remetente com autenticação reforçada (como DMARC, DKIM e SPF), detecção de *links* maliciosos e anexos armadilhados, além de capacidades de resposta automática a incidentes e visualização de ameaças em tempo real.

f) Serviço de Monitoramento e Suporte Técnico Especializado 24x7x365, com equipe capacitada para atendimento remoto e *on-site* (quando necessário), contemplando abertura e acompanhamento de chamados, resposta a incidentes, manutenção preventiva e corretiva, além de relatórios periódicos de desempenho e conformidade.

6.2. Requisitos legais, sociais, ambientais e culturais da Solução de TIC

6.2.1. Conforme estabelecido nos Macrodesafios do Poder Judiciário 2021-2026, o uso racional dos instrumentos de Tecnologia da Informação e Comunicação deverá estar alinhado às políticas de TIC definidas pelo Conselho Nacional de Justiça, que por sua vez visa garantir a confiabilidade, a integridade e a disponibilidade das informações, dos serviços e sistemas essenciais da justiça, por meio do incremento e da modernização dos mecanismos tecnológicos, de controles efetivos dos processos de segurança e de riscos.

6.2.2. Além disso, cabe ressaltar, da Resolução CNJ nº 370, os seguintes macroprocessos pertinentes no Art. 21:

> II – Segurança da Informação e Proteção de Dados:
>
> b) riscos;
>
> c) continuidade de serviços essenciais;
>
> IV – Infraestrutura e Serviços:
>
> a) disponibilidade;
>
> b) capacidade;

c) ativos de infraestrutura, de tecnologia da informação e de telecomunicações corporativas.

6.3. Requisitos temporais

6.3.1. Os serviços deverão ser iniciados até o dia 26/11/2025, quando dar-se-á o término da vigência do CT 288/2020.

6.4. Requisitos de implantação da solução de TIC

6.4.1. A CONTRATADA será integralmente responsável pela correta instalação, configuração e pleno funcionamento dos equipamentos e componentes da solução ofertada, conforme os termos estabelecidos neste documento. Não serão admitidas configurações, ajustes ou modificações que operem os equipamentos ou componentes de *hardware* fora dos parâmetros e condições normais recomendadas pelo fabricante.

6.4.2. A CONTRATADA deverá realizar, em até 15 (quinze) dias úteis após a assinatura do contrato, uma reunião inicial de projeto (*kick-off*) nas dependências do TRIBUNAL. A reunião deverá contar com a participação das áreas de Segurança da Informação e Infraestrutura do TRIBUNAL, bem como do gerente técnico do projeto, responsável comercial, arquiteto de soluções e técnico responsável pela implementação, com o objetivo de alinhar expectativas e definir o Plano de Trabalho para a instalação e configuração da solução.

6.4.3. Após a reunião de *kick-off*, a CONTRATADA deverá elaborar e entregar ao TRIBUNAL DE JUSTIÇA um Projeto Executivo de Implantação, com base nos alinhamentos estabelecidos na referida reunião, contendo, no mínimo:

a) Escopo detalhado dos serviços e produtos fornecidos;

b) Planejamento das atividades, com cronograma físico e de execução em etapas;

c) Desenho lógico da solução e topologia da infraestrutura atual e futura;

d) Descrição dos ambientes e condições técnicas (locais, horários e premissas);

e) Identificação dos pontos de contato entre a CONTRATADA e o TRIBUNAL;

f) Perfil da equipe técnica envolvida, com respectivos quantitativos e certificações, com comprovação formal de qualificação, inclusive com possibilidade de substituição em caso de não conformidade;

g) Plano de gerenciamento de mudanças e de riscos;

h) Itens fora do escopo e cláusulas de responsabilidade;

i) Relação dos artefatos e documentos a serem entregues, incluindo o termo de aceite.

6.4.4. Todos os parâmetros e configurações deverão ser previamente discutidos em reuniões de pré-projeto, com sugestões da CONTRATADA alinhadas às normas técnicas e boas práticas, e sujeitas à aprovação expressa do TRIBUNAL.

6.4.5. A contratada deverá realizar o fornecimento de todos os itens adquiridos – *hardware*, *softwares* e respectivas licenças padrão – no prazo máximo de até 90 (noventa) dias úteis, contados da data de assinatura do contrato, garantindo a instalação, configuração e plena operacionalização da solução de *firewall*.

6.4.6. A etapa de implantação deverá incluir a instalação de equipamentos, sistemas, *softwares* e aplicativos do TRIBUNAL nos PRODUTOS fornecidos, assim como a migração das configurações existentes, desde que tecnicamente viável, para os novos produtos ofertados pela CONTRATADA.

6.4.7. A instalação e configuração da solução deverá ocorrer de forma gradual, transparente e controlada, conforme cronograma e conveniência operacional do TRIBUNAL DE JUSTIÇA, com o objetivo de preservar a continuidade dos serviços.

6.4.8. Durante a fase de testes, implantação e migração, a equipe técnica da CONTRATADA deverá estar integralmente disponível, presencialmente, nos dias e horários definidos pelo TRIBUNAL.

6.4.9. As atividades de instalação e configuração poderão ocorrer, conforme a necessidade da TRIBUNAL, em horário comercial, período noturno, finais de semana ou feriados, devendo a CONTRATADA dispor de equipe compatível com essa exigência.

6.4.10. Durante a implantação, os produtos fornecidos deverão ser colocados em plena operação, sob condições reais de produção, assegurando o correto funcionamento da solução em ambiente definitivo.

6.4.11. A CONTRATADA deverá, sob supervisão e aprovação do TRIBUNAL, planejar e realizar a instalação e configuração dos *softwares* de forma a garantir interoperabilidade total com o ambiente tecnológico existente, sem provocar impacto negativo no ambiente de produção.

6.4.12. A implantação e integração da solução poderá demandar a realização, por parte da CONTRATADA, das seguintes atividades:

a) Instalação e configuração de *softwares*;

b) Acompanhamento da migração de regras e políticas;

c) Elaboração e execução de *scripts*;

d) Análise de desempenho (performance);

e) *Tuning* e ajustes de performance;

f) Diagnóstico e resolução de problemas;

g) Implementação de recursos de segurança.

6.4.13. Será de responsabilidade exclusiva da CONTRATADA a disponibilização de todos os recursos necessários, incluindo *hardware*, *software*, ferramentas e equipe técnica especializada.

6.4.14. Será de responsabilidade exclusiva da CONTRATADA a disponibilização de todos os recursos necessários, incluindo hardware, software, ferramentas e equipe técnica especializada.

6.4.15. A CONTRATADA deverá prover ferramentas e/ou *scripts* de *rollback* imediato, capazes de restaurar a infraestrutura do TRIBUNAL ao seu estado original, caso a instalação da solução apresente falhas críticas.

6.4.16. A CONTRATADA será responsável por fornecer todas as licenças necessárias dos produtos ofertados, bem como de quaisquer componentes adicionais indispensáveis à instalação e pleno funcionamento da solução em ambiente de produção.

6.4.17. Qualquer alteração nos métodos executivos, originalmente definidos, deverá ser previamente submetida à análise e aprovação formal do TRIBUNAL, por meio de documento escrito e justificado.

6.4.18. O encaminhamento formal das demandas referentes aos itens abrangidos por esta contratação será feito exclusivamente por meio de emissão de Ordem de Serviço/Fornecimento, conforme previsto contratualmente.

6.4.19. Ao término dos serviços de implantação, a CONTRATADA deverá entregar em até 15 (quinze) úteis:

a) Relatório técnico *as-built,* contendo todas as configurações executadas, topologias, credenciais administrativas (quando aplicável), endereços de acesso, usuários configurados e demais dados necessários à continuidade operacional.

b) Documentação técnica completa da solução, incluindo: especificações de equipamentos, funcionalidades implementadas, desenhos e diagramas da implantação, bem como comentários e registros de configurações realizadas, inclusive em equipamentos de terceiros, quando aplicável.

6.5. Requisitos de experiência profissional e formação da equipe da CONTRATADA

6.5.1. A CONTRATADA deverá manter equipe técnica certificada e capacitada na solução ofertada, com comprovação por meio de certificados ou declarações emitidas pelo fabricante.

6.6. Requisitos de garantia, manutenção, suporte técnico e operação

6.6.1. **Requisitos de Suporte Técnico**

6.6.1.1. A CONTRATADA deverá disponibilizar serviço de suporte técnico especializado, em regime de 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, durante os 365 dias do ano

(24x7x365), com o objetivo de atender às demandas relacionadas ao funcionamento da solução contratada, pelo período de 36 (trinta e seis) meses

6.6.1.2. O suporte técnico deverá ser acessível por meio de:

a) Aplicação *WEB*, com *login* e senha individualizados fornecidos para os usuários autorizados do TRIBUNAL, para abertura e acompanhamento de chamados;

b) Canais alternativos de atendimento, como telefone e *e-mail*, garantindo redundância de comunicação;

c) Sistema com controle de protocolo, histórico e geração de relatórios gerenciais.

6.6.1.3. Cada usuário autorizado do TRIBUNAL deverá receber identificação e senha de acesso individualizada, assegurando controle de acesso, rastreabilidade e segurança na comunicação com a equipe de suporte técnico.

6.6.1.4. O TRIBUNAL poderá registrar número ilimitado de chamados técnicos durante toda a vigência da garantia da solução, sem qualquer ônus adicional.

6.6.1.5. Entende-se por suporte técnico a facilidade de comunicação colocada à disposição do TRIBUNAL para prestação de informações, esclarecimentos ou orientações sobre:

a) Utilização e funcionalidades da solução (inclusive dicas e atalhos);

b) Configuração de *softwares* e *hardwares*;

c) Instalação e remoção de aplicativos;

d) Atualizações de *software*;

e) Correções e reparos diversos;

f) Intervenções diretas nos equipamentos fornecidos.

6.6.1.6. O suporte técnico será acionado sempre que a solução apresentar falha ou comportamento anômalo que impeça seu funcionamento regular, exigindo intervenção técnica especializada ou substituição de componentes.

6.6.1.7. Durante o atendimento, a CONTRATADA deverá realizar:

a) Análise técnica da solução implantada;

b) Verificação de *logs* e condições operacionais;

c) Emissão de parecer técnico e sugestões de melhorias.

6.6.1.7.1. As recomendações feitas pela CONTRATADA estarão sujeitas à avaliação e deliberação da equipe técnica do TRIBUNAL, que poderá acatar ou rejeitar sua aplicação.

6.6.1.8. Em caso de falha ou defeito de fabricação, o fabricante deverá providenciar a substituição das peças ou do equipamento, conforme necessário. Eventuais substituições de *hardware* deverão ser realizadas em até 1 (um) dia útil a partir da constatação formal da necessidade.

6.6.1.9. Os chamados deverão ser classificados em níveis de severidade, com os seguintes prazos de resposta e resolução:

Severidade	**Descrição**	**Prazo de Resposta (1º contato após abertura do chamado)**	**Prazo de Resolução**
Crítica	Indisponibilidade total da solução ou falha com impacto direto em segurança.	Até 30 minutos	Até 2 horas
Alta	Degradação significativa de desempenho ou falha parcial relevante.	Até 1 hora	Até 4 horas
Média	Problemas pontuais sem impacto crítico, mas que afetam funcionalidades.	Até 2 horas	Até 24 horas
Baixa	Dúvidas, ajustes finos, solicitações de melhoria ou acompanhamento.	Até 8 horas	Até 48 horas

6.6.1.10. A severidade do chamado poderá ser reavaliada pela CONTRATADA ou pelo TRIBUNAL, caso se verifique que foi classificada de forma inadequada. Nesse caso, os prazos de atendimento e solução passarão a ser contados a partir do momento da reavaliação, com base na nova classificação de severidade.

6.6.1.11. A cada abertura de chamado, a CONTRATADA poderá solicitar prorrogação dos prazos de atendimento ou solução, desde que:

a) A solicitação seja feita antes do vencimento do prazo vigente;

b) A justificativa técnica para a prorrogação seja formalmente apresentada;

c) O TRIBUNAL avalie e expresse concordância formal com a prorrogação. A ausência de resposta não implicará aceite tácito.

6.6.1.12. O atendimento aos chamados será iniciado a partir do registro formal no canal de suporte da CONTRATADA e todos os prazos definidos para atendimento e resolução dos chamados começarão a ser contados a partir da abertura do chamado, devendo a CONTRATADA registrar a data e o horário de abertura com precisão.

6.6.1.13. O não cumprimento dos prazos e níveis de serviço aqui definidos sujeita a CONTRATADA às sanções administrativas previstas na legislação vigente e no contrato, incluindo aplicação de penalidades.

6.6.1.14. A CONTRATADA deverá manter equipe técnica capacitada e com conhecimento comprovado na solução ofertada, sendo obrigatória a apresentação de certificações ou declarações emitidas pelo fabricante que atestem a qualificação dos profissionais que prestarem o suporte.

6.6.1.15. A CONTRATADA deverá fornecer ao TRIBUNAL relatórios gerenciais mensais de atendimento, contendo, no mínimo, os dados de:

a) Atendimento:
   - Quantidade de chamados abertos, em andamento e encerrados;
   - Classificação por severidade;
   - Tempo médio de resposta e resolução;
   - Histórico e reincidência de falhas;
   - Ações executadas e status final.

b) Sumário executivo:
   - Objetivo do relatório;
   - Período analisado;
   - Resumo das principais ameaças bloqueadas;
   - Destaques de incidentes ou anomalias detectadas;
   - Conclusões e recomendações.

c) Visão Geral:
   - Equipamentos envolvidos (modelo, fabricante, *firmware*/versão);
   - Serviços ativados: NGFW, IPS, *Application Control*, *Web Filtering*, VPN, etc;
   - Controle de acesso e perfis de acesso;
   - Performance: CPU, Memória e Disco (máximo e média);
   - TOP: Origem, Destino, Política, App, Geo.

d) Indicadores de Segurança:
   - Número de conexões/dia ou picos de tráfego;
   - Volume de tráfego inspecionado (entrada e saída);

- Taxa de bloqueios versus conexões válidas;
- Conexões criptografadas inspecionadas (*SSL Inspection*).

e) Ameaças Bloqueadas e Detectadas:
   - Top ameaças por tipo (*malware, botnet, ransomware,* etc.);
   - Ataques por origem geográfica ou IP;
   - Aplicações mais bloqueadas (ex: *proxy* anônimo, *torrents*, etc.);
   - Tentativas de exploração detectadas (por IPS/IDS);
   - Detecção de tráfego anômalo (*beaconing*, lateral *movement*).

f) Tráfego *Web* e de Aplicações:
   - Principais aplicações acessadas;
   - Aplicações indevidas bloqueadas;
   - Categorias de sites acessados e bloqueados (por política de URL *Filtering*);
   - Aplicações evasivas detectadas (ex: VPNs, proxies, tunelamento DNS).

g) Acesso Remoto e VPN:
   - Usuários que acessaram via VPN (*site-to-site e client-to-site*);
   - Tentativas de login falhas ou suspeitas;
   - Dispositivos conectados via VPN;
   - Horários e localização dos acessos.

h) Políticas de Segurança Aplicadas:
   - Políticas configuradas (ex: por zona, usuário, grupo ou aplicação);
   - Regras mais acionadas e regras obsoletas (*shadowed rules*);
   - Avaliação de boas práticas (ex: políticas muito permissivas).

i) Vulnerabilidades e *Gaps* identificados:
   - Portas e serviços abertos na borda;
   - Falhas de configuração (ex: NAT incorreto, falta de inspeção SSL);
   - *Hardening* ou reconfiguração.

j) *Logs* e Auditoria:
   - Atividades administrativas (quem alterou políticas e quando);
   - Alertas de integridade do sistema (*failover*, HA, atualizações pendentes);
   - Eventos críticos nos *logs* (CPU alta, falhas de disco, quedas de *link*).

k) Recomendações Técnicas:

- Atualizações pendentes;
- Otimizações de políticas;
- Sugestões de segmentação adicional;
- Ativação de funcionalidades inativas (ex: *sandboxing*, *Threat Emulation*).

l) Anexos e Evidências:

- Gráficos e *dashboards*;
- *Logs* relevantes (sanitizados);
- *Screenshots* de alertas e configurações;
- Tabelas com dados detalhados, se necessário.

6.6.1.16. O TRIBUNAL poderá solicitar qualquer relatório da solução com uma frequência mensal o que deverá ser provido pela CONTRATADA num prazo de 5 (cinco) dias úteis.

6.6.1.17. A CONTRATADA também será responsável pela administração e manutenção do serviço em regime de 24x7x365 para atendimentos remotos e o regime 8x5 para atendimentos que possam ser necessários na forma presencial, durante todo o período de prestação de serviço. As tarefas atinentes ao transporte, deslocamento e remessa necessários, seja na implementação, substituição e/ ou remoção de equipamentos defeituosos será de responsabilidade da CONTRATADA.

6.6.1.18. O serviço de monitoramento 24x7 deverá ser obrigatoriamente prestado por meio de Centros de Operações de Rede (NOCs) redundantes, próprios da empresa CONTRATADA, os quais deverão estar plenamente operacionais na data da assinatura do contrato.

6.6.1.19. Esses NOCs atuarão como ponto único de contato (*Single Point of Contact* – SPOC) com a equipe técnica do TRIBUNAL, sendo responsáveis pela recepção, registro e tratamento inicial de chamados, incidentes, problemas, dúvidas e requisições relacionadas aos serviços contratados, funcionando como a primeira instância de atendimento técnico ao TRIBUNAL DE JUSTIÇA.

6.6.1.20. Os serviços prestados pelo NOC da CONTRATADA deverão incluir, no mínimo:

a) Monitoramento proativo da rede *WAN* do TRIBUNAL;

b) Suporte técnico para identificação e resolução de falhas em *hardware* e *software*;

c) Diagnóstico e resolução de problemas de acesso à Internet, sites remotos e serviços de rede corporativa;

d) Atendimento a falhas nos meios de acesso *WAN*, como MPLS e *Ethernet*;

e) Suporte na criação e manutenção de políticas, configurações e parametrizações dos equipamentos fornecidos;

f) Apoio na geração e configuração de relatórios e eventos de segurança detectados ou prevenidos pelos equipamentos;

g) Escalonamento de incidentes ao fabricante, quando necessário;

h) Suporte às configurações de segurança, redundância e gerenciamento dos ativos;

i) Administração e monitoramento de tarefas e políticas de *backup* das configurações;

j) Apoio técnico em auditorias e análise de *logs*.

6.6.1.21. A CONTRATADA deverá atuar de forma:

a) Reativa, para restaurar serviços no menor tempo possível mediante incidentes, por meio de solução definitiva ou paliativa;

b) Proativa, com medidas preventivas que garantam a continuidade operacional dos serviços.

6.6.1.22. Níveis de Atendimento:

a) 1º Nível (24x7): Atendimento telefônico e remoto, responsável pelo registro, triagem e acompanhamento de chamados, bem como pela gestão dos indicadores de monitoramento;

b) 2º e 3º Nível (8x5): Atendimento remoto ou presencial (caso o remoto não resolva), com foco na prevenção e solução de incidentes complexos, identificação da causa raiz e execução de atividades técnicas.

6.6.1.22.1. Em situações de incidentes críticos, mesmo fora do horário comercial, deverá ser assegurado o acionamento emergencial dos níveis 2 e 3, a fim de garantir resposta rápida, continuidade dos serviços essenciais e mitigação imediata dos impactos à operação do Tribunal.

6.6.1.23. Todos os técnicos deverão estar certificados e capacitados para atuar nos equipamentos fornecidos. A comprovação será exigida durante a execução contratual.

6.6.1.24. A CONTRATADA deverá disponibilizar:

a) Canal telefônico (0800 ou equivalente local),

b) Portal *Web* e/ou *e-mail* (em português).

6.6.1.24.1. No ato da abertura, será fornecido número, data e hora do chamado, marcando o início da contagem de SLA (*Service Level Agreement*). O encerramento deve ser formalmente comunicado.

6.6.1.25. A CONTRATADA deverá manter, em seu quadro permanente, profissionais com as seguintes certificações:

a) 02 profissionais com certificação técnica do fabricante dos NGFW ofertados;

b) 02 profissionais com ITIL *Foundation*.

6.6.1.26. A CONTRATADA deverá realizar, sem custo adicional, a atualização de *firmwares* disponibilizados pelo fabricante, mediante autorização prévia do TRIBUNAL e em data/hora acordada.

6.6.1.27. A CONTRATADA deverá fornecer:

a) *Dashboard online* com *status* dos ativos em tempo real;

b) Relatórios mensais digitais (DOCX, XLSX ou PDF) com diagnósticos, indicadores e métricas de desempenho e disponibilidade.

6.6.1.28. A CONTRATADA deverá utilizar ferramenta aderente ao ITIL, contendo no mínimo:

a) Dados do solicitante;

b) Datas e horários de abertura, atendimento e solução;

c) Descrição das ações;

d) Equipamentos ou peças substituídas (com marca, modelo, fabricante e número de série).

6.6.1.29. A CONTRATADA deverá alertar prontamente o TRIBUNAL sobre riscos de falhas operacional, mesmo que não consumado.

6.6.1.30. O TRIBUNAL definirá os administradores dos equipamentos, os quais deverão comunicar a CONTRATADA qualquer alteração realizada, assumindo integral responsabilidade pelas modificações.

6.6.2. **Requisitos de Garantia do Produto**

6.6.2.1. Considera-se “garantia” a obrigação da CONTRATADA em reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, o objeto do contrato ou quaisquer de seus componentes, sempre que forem verificados vícios, defeitos de fabricação, mau funcionamento ou quaisquer incorreções técnicas, durante o período de garantia estabelecido neste documento.

6.6.2.2. O período de garantia dos PRODUTOS será de 36 (trinta e seis) meses, contados a partir da data do recebimento definitivo do objeto contratual, conforme atestado pelo TRIBUNAL.

6.6.2.3. Durante todo o período de vigência da garantia, deverão ser asseguradas ao TRIBUNAL, sem quaisquer ônus adicionais, as seguintes condições mínimas:

a) Acesso irrestrito a atualizações, *patches*, correções de segurança, *drivers* e quaisquer outras melhorias e atualizações de *software*, as quais devem estar disponíveis no *website* oficial do fabricante da solução ou outro meio formalmente comunicado, sem exigência de pagamento de licenças adicionais, taxas ou subscrição;

b) Disponibilização das versões atualizadas de manuais técnicos e da documentação dos equipamentos e *softwares* adquiridos, sempre que forem revisadas ou reeditadas pelo fabricante, devendo a CONTRATADA comunicar formalmente ao TRIBUNAL a disponibilidade dessas atualizações;

c) Garantia de compatibilidade retroativa e cumulativa das atualizações disponibilizadas com os produtos originalmente entregues, de forma a não comprometer sua estabilidade, segurança e desempenho;

d) Prestação de suporte técnico qualificado para a identificação, diagnóstico e resolução de problemas durante o período de garantia.

6.6.3. **Requisitos de Manutenção Preventiva e Corretiva**

6.6.3.1. A CONTRATADA será responsável, durante todo o período de garantia, pela manutenção preventiva e corretiva de todos os componentes da solução fornecida, sejam eles de *hardware*, *software* ou serviços agregados, conforme a seguir especificado.

6.6.3.2. **Manutenção Preventiva**

6.6.3.2.1. A manutenção preventiva visa assegurar o correto funcionamento da solução, por meio de intervenções programadas e deve abranger, no mínimo:

a) Verificação periódica da integridade dos equipamentos e sistemas, incluindo análise de performance, capacidade, alertas e registros de *log*;

b) Aplicação de atualizações de segurança, *firmware* e *patches*, conforme diretrizes do fabricante e melhores práticas do mercado, garantindo compatibilidade com o ambiente do TRIBUNAL;

c) Relatório técnico consolidado das atividades realizadas, a ser apresentado ao TRIBUNAL ao final de cada ciclo de manutenção preventiva (a periodicidade será definida conjuntamente na reunião de *kick-off*);

d) Execução de testes funcionais e diagnósticos de performance para antecipação de falhas.

6.6.3.3. **Manutenção Corretiva**

6.6.3.3.1. A manutenção corretiva consiste nas ações de reparo ou substituição de componentes que apresentem falha, devendo observar as seguintes condições:

a) A CONTRATADA deverá proceder com o atendimento imediato ao chamado técnico, nos prazos definidos, conforme a severidade do problema;

b) A substituição de quaisquer componentes defeituosos deverá ocorrer em até 1 (um) dia útil após a constatação da necessidade da troca, sem prejuízo da continuidade do funcionamento da solução;

c) Os equipamentos substituídos deverão ser equivalentes ou superiores em especificações técnicas e compatíveis com o restante do ambiente;

d) Os serviços corretivos devem ser documentados e relatados ao TRIBUNAL, contendo a descrição da falha, ações executadas, componentes substituídos (se houver) e o tempo total de resolução.

6.6.3.4. A CONTRATADA deverá manter equipe técnica habilitada e capacitada para atender às necessidades de manutenção preventiva e corretiva, com cobertura 24x7x365, conforme estipulado neste documento.

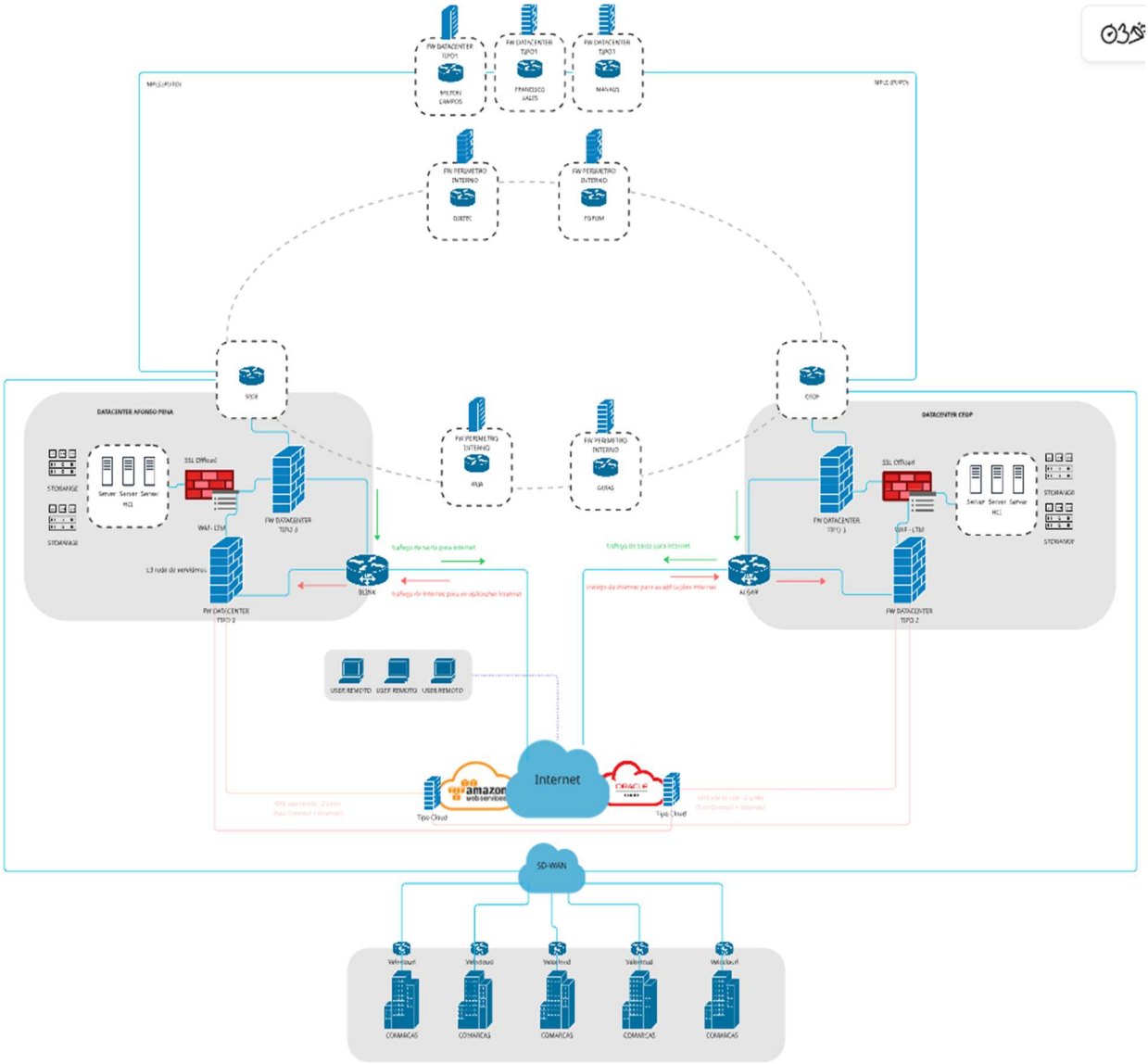
7. Estimativa das quantidades

LOTE ÚNICO			
Item	**Especificação**	**Métrica**	**Quantidade**
1	AQUISIÇÃO DE NGFW “DATACENTER - TIPO 3” COM GARANTIA DE 36 MESES.	UN	2
2	AQUISIÇÃO DE NGFW “DATACENTER - TIPO 2”, COM GARANTIA DE 36 MESES.	UN	2
3	AQUISIÇÃO DE NGFW “DATACENTER - TIPO 1”, COM GARANTIA DE 36 MESES.	UN	3
4	AQUISIÇÃO DE NGFW “TIPO PERÍMETRO INTERNO”, COM GARANTIA DE 36 MESES.	UN	4
5	AQUISIÇÃO DE NGFW “TIPO CLOUD”, COM GARANTIA DE 36 MESES.	NÚCLEO	15
6	SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIO PARA, NO MÍNIMO, 13 EQUIPAMENTOS, COM GARANTIA DE 36 MESES.	UN	2
7	INSTALAÇÃO DE NGFW “TIPO DATACENTER”	UN	7
8	INSTALAÇÃO DE NGFW “TIPO PERÍMETRO E TIPO CLOUD”	UN	6
9	SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE NGFW “TIPO DATACENTER” COM GARANTIA DE 36 MESES.	UN	7
10	SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE NGFW “TIPO PERÍMETRO E TIPO CLOUD” COM GARANTIA DE 36 MESES.	UN	6
11	SOLUÇÃO DE PREVENÇÃO DE AMEAÇAS E SPAM PARA E-MAIL EM NUVEM COM GARANTIA DE 36 MESES.	UN	1.150

A quantidade estimada dos *appliances* do “Tipo Datacenter - Tipo 3 e 2” e “Solução de Gerenciamento Centralizado” leva em conta a topologia de rede dos dois datacenters do TRIBUNAL, além da necessária duplicidade de equipamentos, já que a redundância deles garantirá a resiliência da solução em caso de falhas. Os datacenters do TRIBUNAL estão localizados nos seguintes endereços:

a) Centro Operacional (CEOP) - Av. do Contorno, 629, Belo Horizonte- MG;

b) Data Center Edifício Sede – Avenida Afonso Pena, 4001, Belo Horizonte – MG.



A proposta, representada na figura acima, contempla a aquisição de 02 (dois) *firewalls* de próxima geração (NGFW) do “ Datacenter - Tipo 3”, 02 (dois) NGFW do “Datacenter - Tipo 2”, 03 (três) NGFW do “Datacenter - Tipo 1” e 04 (quatro) NGFW do “Tipo Perímetro Interno”, 15 (quinze) núcleos de CPU para NGFW do “Tipo Cloud” e 1.150 (mil cento e cinquenta) licenças de “Solução de Prevenção de Ameaças e *Spam* para *E-mail*”, com o objetivo de estruturar as frentes críticas da segurança de rede e comunicação do Tribunal de Justiça de Minas Gerais (TJMG), promovendo alta disponibilidade, segmentação avançada e proteção abrangente contra ameaças cibernéticas:

a) **“Datacenter - Tipo 3”:** Dois *appliances* de *firewall* de próxima geração (NGFW) destinados ao controle e proteção do tráfego de saída das redes internas para a Internet institucional, estrategicamente posicionados nos datacenters do TJMG em configuração de alta disponibilidade (HA). Esses equipamentos serão responsáveis por garantir a continuidade operacional mesmo em cenários de falha, oferecendo alta capacidade de inspeção profunda de tráfego, filtragem de conteúdo e aplicação de políticas de segurança avançadas. Além do papel de segurança perimetral de saída, os *appliances* também atuarão na inspeção e visibilidade do tráfego leste-oeste entre as redes internas da SEDE e do CEOP, ampliando o controle sobre a comunicação entre segmentos críticos da infraestrutura e reforçando a proteção contra movimentações laterais de ameaças.

b) **“Datacenter - Tipo 2”:** Dois *appliances* configurados como *firewalls* de data center e concentradores de VPN, projetados para reforçar a segurança das cargas críticas, do tráfego interno e das interconexões com ambientes distribuídos e escritórios remotos. Esses equipamentos também atuarão como *firewalls* de borda para as aplicações expostas ao público, oferecendo proteção avançada contra ameaças oriundas da Internet, por meio de inspeção profunda de pacotes, controle de acesso e políticas de segurança específicas para os serviços publicados externamente. Sua atuação assegura que as aplicações institucionais expostas ao público, como sistemas judiciais, portais e serviços eletrônicos, estejam adequadamente protegidas, conforme as melhores práticas de segurança perimetral e requisitos de disponibilidade. Além disso, esses *appliances* serão os responsáveis pelo gerenciamento das conexões VPN *site-to-site* entre o Tribunal e seus ambientes em nuvem pública (como AWS e OCI), bem como com empresas terceirizadas e instituições parceiras.

c) **“Datacenter - Tipo 1” e “Tipo Perímetro Interno”:** Sete *appliances* dedicados à proteção das áreas estratégicas conectadas ao Cinturão Digital, atuando como uma camada de proteção local para redes que atualmente possuem roteamento direto entre unidades — sem passagem por dispositivos de inspeção. Essas unidades incluem as sedes localizadas na Av. Raja Gabaglia, Rua Goiás, Fórum Lafayette, DIRTEC, bem como as unidades com enlaces MPLS dedicados, como Milton Campos, Francisco Sales e Manaus. A implementação desses NGFWs visa sanar a atual limitação de visibilidade e controle do tráfego leste-oeste, permitindo inspeção granular do tráfego inter-redes local, aplicação de políticas de segurança contextualizadas, e bloqueio de movimentações laterais de ameaças. Além disso, essa abordagem contribui diretamente para o reforço da governança de rede, o alinhamento com a política de segmentação segura do TJMG e o fortalecimento da resiliência cibernética local nas unidades mais críticas da instituição.

d) **“Tipo *Cloud*”:** Quinze núcleos de CPU destinados à alocação entre duas máquinas virtuais (VMs), que atuarão como *firewalls* dedicados à proteção dos ambientes de nuvem pública, proporcionando uma camada avançada de controle, visibilidade e inspeção de tráfego nas plataformas AWS (*Amazon Web Services*) e OCI (*Oracle Cloud Infrastructure*). Esses

dispositivos permitirão a proteção proativa das cargas de trabalho em *cloud*, com segmentação segura entre aplicações, aplicação de políticas baseadas em identidade e contexto, além de detecção e prevenção de ameaças nativas da nuvem. A integração com a gestão centralizada da arquitetura de segurança institucional garantirá uniformidade de políticas e correlação de eventos entre o ambiente *on-premises* e as infraestruturas em nuvem, promovendo uma postura de segurança consistente, auditável e alinhada às melhores práticas do setor.

e) **"Solução de Prevenção de Ameaças e *Spam* para *E-mail*":** Mil licenças da solução de prevenção de *e-mails* que visam atender prioritariamente às contas utilizadas por magistrados, onde o risco de comprometimento representa impactos elevados à continuidade e à confidencialidade das atividades judiciais.

8. LEVANTAMENTO DE MERCADO

8.1. Identificação das Soluções

8.1.1. Solução Única:

Em razão de todos os elementos aqui apresentados e após criteriosa análise de mercado, a DIRTEC entende que a única solução capaz de atender integralmente aos requisitos relacionados, é a aquisição de solução de *firewall* de próxima geração (NGFW), do fabricante *CheckPoint*, para os ambientes *on-premisse* e *cloud*, contemplando *hardware* e *software*, bem como a aquisição de solução de proteção de *e-mail* corporativo, conforme detalhamento abaixo:

8.1.1.1. NGFW (*Next Generation Firewall*) em formato *appliance* para o ambiente *on-premisse*:

Neste modelo, a solução de segurança é adquirida de forma perpétua, contemplando o fornecimento de *appliances* físicos (*hardware*), sistemas operacionais, serviços de instalação e serviço gerenciado. O suporte técnico é contratado com vigência alinhada ao ciclo de vida da solução, abrangendo atualizações, manutenção corretiva e suporte especializado.

Vantagens:

a) **Autonomia tecnológica:** a posse do equipamento físico garante maior controle sobre a arquitetura de segurança, permitindo customizações específicas, integração com soluções legadas e aderência às políticas institucionais de TIC e segurança da informação.

b) **Alta performance e confiabilidade:** *appliances* físicos dedicados oferecem maior capacidade de processamento, desempenho previsível e menor latência na inspeção de tráfego, especialmente em ambientes de missão crítica.

c) **Integração com ecossistemas complexos:** o modelo *on-premises* favorece a integração com sistemas locais, como o caso dos principais sistemas judiciais ainda *on-premise*.

d) Visibilidade total do tráfego: possibilita inspeção profunda (DPI – *Deep Packet Inspection*) e análise do tráfego leste-oeste, algo fundamental para a detecção precoce de movimentações laterais de ameaças e para o cumprimento de requisitos de auditoria e conformidade.

e) Padronização e previsibilidade: Garante continuidade operacional, maior previsibilidade de investimento e menor impacto na curva de aprendizado técnico, uma vez que elimina a necessidade de readaptação frequente a novas tecnologias.

Desvantagens:

a) Em futuras contratações, na ausência de especificação técnica que mantenha o fabricante atual, existe o risco de substituição da tecnologia por solução de outro fornecedor.

b) Essa mudança pode implicar em desafios de compatibilidade, dificultando a migração de políticas, regras e configurações existentes, e exigindo reconfiguração completa do ambiente de *firewall* do TRIBUNAL.

c) A troca de fabricante também pode demandar capacitação adicional da equipe técnica, impactando temporariamente a eficiência operacional.

8.1.1.2. NGFW (*Next Generation Firewall*) em formato VM para ambiente de nuvem pública

Neste modelo, o *Next Generation Firewall* é implementado por meio de máquinas virtuais (VMs) especificamente licenciadas para operação em ambientes de nuvem pública, como *Amazon Web Services* (AWS) e *Oracle Cloud Infrastructure* (OCI). Essas instâncias replicam as funcionalidades avançadas de inspeção, controle e proteção dos *appliances* físicos, permitindo uma segurança homogênea e centralizada entre ambientes híbridos.

Vantagens:

a) Elasticidade e escalabilidade sob demanda: o modelo virtual permite rápida expansão ou redução de capacidade conforme a variação de carga.

b) Segmentação de rede entre *workloads*: viabiliza controle granular do tráfego leste-oeste dentro da própria nuvem, prevenindo movimentações laterais e garantindo microssegmentação eficiente.

c) Padronização de políticas de segurança: integração com o gerenciamento centralizado dos *firewalls on-premises* permite uniformização das políticas e visibilidade única dos eventos de segurança em ambientes híbridos.

Desvantagens:

a) Custos recorrentes baseados em uso: embora evite investimento inicial elevado, os custos operacionais podem aumentar com o tempo, especialmente em ambientes com grande volume de tráfego ou necessidade contínua de alta disponibilidade.

8.1.1.3. **Solução de proteção de e-mail corporativo**

Neste modelo, a solução de proteção de *e-mail* é ofertada como serviço em nuvem (SaaS), com licenciamento por usuário. A ferramenta realiza inspeção avançada de mensagens recebidas e enviadas, integrando recursos como *antispam*, antivírus, *sandbox*, proteção contra *phishing* e ataques baseados em engenharia social (BEC – *Business Email Compromise*), além de funcionalidades de DLP (*Data Loss Prevention*) e criptografia de mensagens.

A solução é integrada ao serviço de e-mail corporativo (Google Workspace) por meio de conectores seguros (API ou SMTP), permitindo inspeção em tempo real e políticas granulares de segurança.

Vantagens:

a) **Atualizações automáticas e inteligência contra ameaças zero-day:** por ser um serviço em nuvem, a solução se beneficia de mecanismos de aprendizado contínuo e atualização em tempo real, oferecendo resposta mais ágil a novas ameaças e campanhas de spam ou *malware*.

b) **Redução da carga de processamento local:** como a análise é feita em nuvem, evita-se sobrecarga dos servidores de e-mail locais e reduz a latência de entrega.

c) **Proteção avançada contra ameaças direcionadas:** integração com mecanismos de *sandboxing* e análise comportamental permite a detecção de *malwares* sofisticados e links maliciosos ocultos em documentos ou e-mails aparentemente legítimos.

d) **Integração com políticas institucionais de segurança:** suporte a regras de DLP, classificação de mensagens, retenção, arquivamento e rastreabilidade completa das ações realizadas sobre cada *e-mail.*

Desvantagens:

a) **Dependência do fornecedor para políticas de customização:** o modelo SaaS pode limitar a flexibilidade em termos de integrações específicas ou customizações de regras muito particulares, dependendo da plataforma contratada.

b) **Exposição ao tráfego externo:** apesar de operarem com elevados padrões de segurança, as soluções SaaS exigem a integração do fluxo de e-mails com servidores fora do domínio da instituição, o que requer avaliação criteriosa de riscos e conformidade com requisitos legais e normativos.

8.2. Soluções consideradas inviáveis

8.2.1. **Utilização de ferramenta de *Firewall* código aberto (*open source*):**

Embora existam no mercado diversas ferramentas de *firewall* baseadas em código aberto, com funcionalidades robustas e comunidades ativas de suporte, a adoção desse modelo não se mostra viável para a realidade institucional do Tribunal de Justiça de Minas Gerais, tendo em vista os

requisitos críticos de disponibilidade, segurança, conformidade regulatória e sustentabilidade operacional de longo prazo.

Vantagens:

a) Algumas distribuições *open source* contam com recursos comparáveis às soluções comerciais, especialmente quando combinadas com módulos adicionais e suporte por subscrição.

b) A comunidade global disponibiliza fóruns, repositórios e tutoriais que podem auxiliar na resolução de problemas pontuais.

Desvantagens:

c) Ausência de suporte técnico completo (*hardware* + *software*): compromete a capacidade de resposta rápida a incidentes, falhas ou atualizações críticas, o que é inaceitável em um ambiente que exige operação contínua 24x7.

d) Risco elevado de indisponibilidade: em situações de falha, a ausência de SLA formal e equipe dedicada de suporte pode resultar em paradas prolongadas, impactando diretamente os serviços judiciais.

e) Falta de validação de mercado e certificações exigidas: muitas soluções não possuem certificações reconhecidas internacionalmente, dificultando sua adequação às exigências de auditoria, conformidade e governança.

f) Escalabilidade limitada e dependência de *hardware* genérico: o uso em *appliances* improvisados impõe limitações severas de desempenho e confiabilidade, sobretudo em redes distribuídas e de grande escala como a do TJMG.

8.2.2. **Contratação de *Firewall* as a *Service*:**

O modelo de *Firewall as a Service* (FaaS), no qual a proteção de perímetro é fornecida como um serviço em nuvem gerenciado por terceiros, apresenta ganhos de agilidade e simplificação operacional para alguns cenários. No entanto, não se revela tecnicamente adequado nem estratégico para o contexto do TJMG, considerando os requisitos institucionais de controle, disponibilidade, integração com infraestrutura local e soberania sobre os dados.

Vantagens:

a) Escalabilidade dinâmica: recursos podem ser ajustados sob demanda, o que é útil para empresas com picos de tráfego sazonais.

b) Gestão simplificada: operações de atualização, manutenção e ajustes são delegadas ao provedor de serviço, liberando a equipe interna para outras atividades.

Desvantagens:

c) **Baixa aderência ao ambiente híbrido do TJMG:** o modelo FaaS é nativamente voltado para ambientes totalmente em nuvem, o que compromete a eficiência na proteção de redes locais complexas, como os datacenters institucionais, o Cinturão Digital e prédios com conectividade dedicada (MPLS).

d) **Custos recorrentes crescentes (OPEX):** embora vantajoso em curto prazo, o modelo de pagamento contínuo pode tornar-se financeiramente menos vantajoso em médio/longo prazo em comparação ao modelo de aquisição perpétua com suporte associado.

e) **Limitações técnicas** para integração com ferramentas específicas de monitoramento, automação e gestão utilizadas pela instituição.

9. Estratégia de contratação

Durante os estudos técnicos, foi identificada a Ata de Registro de Preços nº 2025/03636, firmada entre a Empresa de Tecnologia da Informação do Ceará – ETICE e a empresa NTSEC Soluções em Teleinformática Ltda., parceira da fabricante Check Point, como alternativa plenamente aderente aos requisitos técnicos e operacionais do objeto pretendido. A referida ata demonstrou-se vantajosa não apenas por contemplar os itens necessários à modernização da arquitetura de segurança do TJMG, mas também por apresentar condições comerciais competitivas e já formalizadas. Os itens da ata que atendem a este estudo técnico são:

LOTE ÚNICO			
Item	**Especificação**	**Métrica**	**Qtde.**
1	1915700 - AQUISIÇÃO DE NGFW “DATACENTER - TIPO 3” COM GARANTIA DE 36 MESES.	UN	2
2	1915696 - AQUISIÇÃO DE NGFW “DATACENTER - TIPO 2”, COM GARANTIA DE 36 MESES.	UN	2
3	1915686 - AQUISIÇÃO DE NGFW “DATACENTER - TIPO 1”, COM GARANTIA DE 36 MESES.	UN	3
4	1915676 - AQUISIÇÃO DE NGFW “TIPO PERÍMETRO INTERNO”, COM GARANTIA DE 36 MESES.	UN	4
5	1915710 - AQUISIÇÃO DE NGFW “TIPO CLOUD”, COM GARANTIA DE 36 MESES.	NÚCLEO	15
6	1410964 - SOLUÇÃO DE GERENCIAMENTO CENTRALIZADO E RELATÓRIO PARA ATÉ 50 EQUIPAMENTOS, COM GARANTIA DE 36 MESES.	UN	2
7	1411027 - INSTALAÇÃO DE NGFW “TIPO DATACENTER”	UN	7
8	1411017 - INSTALAÇÃO DE NGFW “TIPO PERÍMETRO INTERNO E TIPO CLOUD”	UN	6
9	1411067 - SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE NGFW “TIPO DATACENTER” COM GARANTIA DE 36 MESES.	UN	7
10	1411057 - SERVIÇO DE MONITORAMENTO E SUPORTE TÉCNICO 24X7 DE NGFW “TIPO PERÍMETRO INTERNO E TIPO CLOUD” COM GARANTIA DE 36 MESES.	UN	6
11	1915720 - SOLUÇÃO DE PREVENÇÃO DE AMEAÇAS E SPAM PARA E-MAIL EM NUVEM COM GARANTIA DE 36 MESES.	UN	1.000*

* Registra-se que a ata vigente contempla um limite de 1.000 licenças para sua adesão, com possibilidade de acréscimo mediante aditivo contratual. Considerando que o valor registrado na ata se mostrou significativamente mais vantajoso em relação às pesquisas de preços realizadas, avaliamos como oportuno aderir à totalidade do quantitativo disponível, já prevendo eventual necessidade de expansão futura por meio de aditivo.

A estruturação destes modelos reforça o compromisso do TJMG com a modernização da sua arquitetura de segurança, alinhando-se às boas práticas de mercado, ao mesmo tempo em que prepara a instituição para os desafios crescentes da transformação digital, mobilidade e proteção de dados.

Além disso, alinha-se às diretrizes de segurança, eficiência e continuidade estabelecidas pelo CNJ (Conselho Nacional de Justiça), fortalecendo a governança de TIC e a maturidade cibernética institucional do Tribunal.

A decisão pela adesão à ata de registro de preços da *CheckPoint* está fundamentada em critérios técnicos, estratégicos e de alinhamento às melhores práticas recomendadas pelo mercado. Segundo análise da Gartner[1], referência mundial em pesquisa e consultoria em tecnologia, a *CheckPoint* figura consistentemente como líder no Quadrante Mágico para *Firewalls* de Rede, sendo destacada por sua ampla visibilidade e aderência a múltiplos casos de uso observados nas organizações.

Fonte: Gartner (dezembro de 2022)

Com base nas mais recentes avaliações do Gartner[2], também se destaca a importância de adoção de soluções especializadas para segurança de *e-mail*. No Quadrante Mágico de 2024 para *Email Security,* o Gartner recomenda fornecedores que combinem tecnologia avançada baseada em inteligência artificial, recursos de detecção e resposta automatizados, e capacidade de mitigação contra ameaças modernas, como *phishing* altamente direcionado, comprometimento de *e-mail* corporativo (BEC) e ataques baseados em engenharia social. A *Check Point* está entre os líderes deste quadrante com soluções que oferecem proteção multicamada, integração com serviços de

[1] https://www.gartner.com/document-reader/document/4022346?ref=solrAll&refval=473883196
[2] https://www.gartner.com/interactive/mq/6019335?ref=solrAll&refval=477656013

threat intelligence globais, visibilidade em tempo real e ferramentas robustas de investigação e resposta a incidentes. Essa recomendação reforça a necessidade do Tribunal de Justiça de Minas Gerais adotar camadas adicionais de proteção de e-mail, especialmente para contas críticas como as utilizadas por magistrados, assegurando a integridade da comunicação institucional frente à crescente sofisticação das ameaças digitais.

Entre os principais fatores que reforçam a decisão do TJMG, destaca-se o constante investimento da *Check Point* em inovação tecnológica, com o lançamento de atualizações significativas de *software* que trouxeram avanços em áreas críticas como proteção da rede contra ataques cibernéticos sofisticados com uma abordagem de prevenção de ameaças 360° baseada em inteligência artificial, alimentada por uma das maiores bases de inteligência de ameaças globais em tempo real, o *Check Point ThreatCloud.* Combinando gerenciamento unificado de políticas, alta escalabilidade e desempenho de classe mundial, a plataforma *Quantum* da *Check Point* oferece proteção abrangente contra *malware*, *phishing*, exploração de vulnerabilidades, ataques de DNS, *ransomware*.

Outro ponto relevante é o portfólio integrado e robusto oferecido pela *Check Point*, que inclui soluções como *Quantum Security Gateway* e *CloudGuard*, que podem ser integradas nativamente ao NGFW em um único ecossistema de segurança. Essa abordagem permitirá ao TJMG consolidar diversas funcionalidades em uma plataforma unificada, reduzindo a complexidade operacional e aumentando a eficiência na administração do ambiente de segurança.

A flexibilidade de implantação é outro diferencial estratégico. A *Check Point* disponibiliza *firewalls* em diferentes modelos, incluindo *appliances* físicos (série *Quantum*), *firewalls virtuais* (VMs) e soluções nativas em nuvem para AWS e OCI (*CloudGuard*). Essa variedade permite ao TJMG atender

ambientes distribuídos e híbridos com um único fabricante, simplificando a arquitetura e promovendo maior governança da segurança.

Em termos de capacidade técnica, os *firewalls* da *Check Point* se destacam pelas funcionalidades avançadas de detecção e prevenção de ameaças (*Threat Prevention*), segurança de DNS, proteção contra ameaças em IoT, e capacidade de inspeção de tráfego SSL com alto desempenho. A visão estratégica do TJMG contempla a adoção progressiva de soluções escaláveis e integradas para garantir a continuidade e a segurança dos serviços digitais, com a *Check Point* oferecendo suporte total às funções de SSE (*Secure Service Edge*), como SWG, CASB e ZTNA, através de sua plataforma *Harmony Connect*. Tais funcionalidades, embora não sejam foco imediato, estão disponíveis para expansão futura de forma nativa e centralizada via *SmartConsole* ou *Infinity* Portal.

A adoção das soluções *Check Point* proporcionará ao TJMG um avanço significativo na proteção de sua infraestrutura digital. A nova plataforma NGFW da *Check Point* é baseada em inteligência artificial, segurança preditiva e automação, oferecendo ganhos mensuráveis em desempenho, segurança, escalabilidade e eficiência operacional.

Com relação ao desempenho do principal *appliance*:

a) Capacidade de inspeção com *Threat Prevention*: até 60 Gbps.

b) *Throughput* com VPN IPSec: até 40 Gbps.

c) Sessões simultâneas: acima de 40 milhões.

d) Conexões por segundo: mais de 1.200.000.

e) Capacidade de VPNs site-to-site e *client-to-site* dimensionadas para até dezenas de milhares de túneis simultâneos, incluindo suporte a IPsec, SSL e autenticação multifator.

Segurança e visibilidade:

a) Suporte completo à inspeção SSL/TLS com milhares de certificados simultâneos.

b) Proteção contra *malware* desconhecido com *ThreatCloud* e *SandBlast Zero-Day Protection*.

c) Integração com AD para controle de identidade, com suporte a MFA e *Single Sign-On.*

A solução também possibilita visibilidade total do tráfego, segmentação por zonas, bloqueio baseado em geolocalização, aplicação de melhores práticas através do *Security Checkup* e análise contínua via *SmartEvent*.

Além da performance, o uso de arquitetura unificada (*Infinity Architecture*) com inspeção em *Single-Pass* e gerenciamento centralizado permite ao TJMG reduzir a complexidade operacional e manter conformidade com normativos do CNJ, como a Resolução 370/2021 (PSI) e 211/2015 (Governança de TIC).

Assim, a adesão à solução da *CheckPoint* representa uma decisão estratégica para a consolidação de uma arquitetura de segurança moderna, preditiva e preparada para os desafios de *cibersegurança* atuais e futuros.

Portanto, ao investir em uma solução de segurança que combina inovação tecnológica, alta performance e conformidade normativa, o TJMG não apenas moderniza sua infraestrutura crítica, mas também reforça seu compromisso com a proteção dos dados institucionais, a continuidade dos serviços jurisdicionais e a conformidade com as melhores práticas de segurança cibernética do setor público.

A adesão à ATA da *CheckPoint* representa um avanço estratégico para o TJMG na consolidação de uma arquitetura de segurança moderna, automatizada e preparada para os desafios atuais e futuros. A solução oferece *firewalls* de próxima geração (NGFW) com recursos líderes de mercado, e contempla subscrições e suporte por um período de 36 meses, com alto valor agregado ao ambiente institucional. Entre os principais benefícios técnicos e operacionais, destacam-se:

Segurança Avançada de Camada de Aplicação e Prevenção de Ameaças – *Check Point:*

Política de Segurança com base em melhores práticas do *Security Gateway* da *Check Point*, permitindo inspeção profunda de tráfego (HTTP/HTTPS), prevenção contra *malwares*, *exploits*, tráfego de comando e controle (C2) e ameaças desconhecidas, tudo reforçado com IA e aprendizado de máquina por meio do *ThreatCloud* AI.

Threat Prevention com eficácia reconhecida globalmente, utilizando motores de inspeção como IPS, *Antivirus, Anti-Bot* e *Threat Emulation*, com atualizações em tempo real via *ThreatCloud.*

Antivírus em tempo real baseado em fluxo (*stream-based*), prevenindo *malwares* embutidos em arquivos, PDFs, *scripts* e conteúdos compactados com mínima latência.

Threat Emulation (*Sandboxing*) com análise comportamental e em memória (*runtime*) em nuvem (*Check Point Cloud*) ou *on-premises* via *SandBlast Appliance*, detectando ataques de dia zero com alta eficácia.

Advanced DNS Security integrada ao módulo *Anti-Bot*, detectando domínios maliciosos (DGA), túneis DNS e atividades de exfiltração de dados com base em reputação e comportamento.

Proteções *Anti-Exploit* e *Anti-Spyware* incluídas no pacote *Threat Prevention*, bloqueando execuções arbitrárias, exploração de falhas de *buffer* e conexões de *hosts* comprometidos.

URL *Filtering* com controle granular por categorias, bloqueio de envio de credenciais e inspeção de tráfego em HTTPS, integrado ao *Identity Awareness* para aplicação por usuário/grupo.

Bloqueio de tipos de arquivos perigosos, como executáveis, DLLs, arquivos. *lnk* e *torrents*, aplicando perfis de *Threat Prevention* e *Application Control* mesmo em ambientes internos.

Infraestrutura de Perímetro Otimizada e Observável – *Check Point*:

Inspeção de tráfego SSL/TLS (HTTPS *Inspection*) com suporte à validação de certificado, controle por versão de protocolo e integração com módulos de *Threat Prevention* para inspeção completa.

Segmentação de rede por zonas de segurança e políticas baseadas em objetos, com controle de tráfego entre segmentos internos, reduzindo superfícies de ataque.

Proteção contra DoS e variações de ataques de negação de serviço com *SmartEvent* e perfis de proteção granular por interface, IP, zona e região geográfica.

Bloqueios Inteligentes e Dinâmicos na Camada de Borda – *Check Point*:

Suporte a *Feeds* externos e IoC (*Indicators of Compromise*) via IOC *Feeds* e *Custom Intelligence Feeds*, permitindo bloqueios automatizados de até milhões de IPs, domínios e URLs maliciosos.

Integração nativa com o *ThreatCloud*, provendo inteligência de ameaças atualizada globalmente, bloqueando C2s, redes de *bulletproof hosting*, e nós de saída Tor antes de atingirem o ambiente interno.

Alta Disponibilidade e Otimização de *Links* com ECMP – *Check Point*:

Balanceamento de múltiplos *links* WAN com ECMP e algoritmos como *Round Robin* e *Weighted Load Balancing*, garantindo redundância e otimização de tráfego entre sites e nuvem.

Suporte nativo a *ClusterXL* e ISP *Redundancy* para alta disponibilidade e *failover* de *links* de Internet ou *WAN*.

Gestão Centralizada e Ciclo Contínuo de Melhoria – *Check Point:*

O gerenciamento centralizado é realizado via *SmartConsole* e *SmartEvent*, com análises contínuas de segurança, monitoramento de conformidade e auditoria de políticas.

Ferramentas como:

a) *Security Best Practices Analyzer*: identifica desvios e recomendações.

b) *Compliance Blade*: auditoria de conformidade com padrões como ISO 27001, PCI-DSS, NIST.

c) *SmartTask* e *SmartWorkflow:* automatização de tarefas administrativas e controle de mudanças.

Benefícios diretos ao TJMG – *Check Point*:

A adesão à Ata de Registro de Preço nº 2025/03636 representa uma medida alinhada ao princípio da economicidade, previsto no artigo 37 da Constituição Federal, que orienta a Administração Pública a buscar a melhor relação entre custo e benefício em suas contratações. Ao optar por um instrumento

já formalizado, o Tribunal evita custos e esforços adicionais com a realização de uma nova licitação, além de se beneficiar de condições comerciais vantajosas previamente negociadas em escala. Essa estratégia permite maior agilidade na implementação da solução, redução de despesas operacionais e otimização dos recursos públicos, assegurando ao mesmo tempo a contratação de uma solução tecnicamente qualificada e alinhada aos requisitos institucionais de segurança e desempenho.

Essa adesão representa uma decisão estratégica que proporciona ao Tribunal de Justiça de Minas Gerais um conjunto robusto de benefícios técnicos e operacionais, alinhados às melhores práticas de segurança cibernética do mercado:

a) Substituição de *proxies* legados *open source*, muitas vezes limitados em funcionalidades e escalabilidade, por mecanismos avançados de inspeção profunda nativamente integrados aos *firewalls* de próxima geração (NGFW) da *Check Point*. Essa substituição garante maior controle, performance e segurança na navegação institucional.

b) Aumento expressivo da visibilidade do tráfego de rede, inclusive no tráfego leste-oeste (entre redes locais), com destaque para os prédios interconectados pelo Cinturão Digital (Av. Raja Gabaglia, Rua Goiás, Fórum Lafayette e DIRTEC) e para as unidades com enlaces MPLS dedicados (Milton Campos, Francisco Sales e Manaus). A adoção de *firewalls* estratégicos nesses pontos permitirá a inspeção granular, segmentação de tráfego e mitigação de movimentos laterais de ameaças, elevando a postura defensiva da instituição.

c) Proteção integrada dos ambientes em nuvem (AWS e OCI) com *firewalls* em formato virtual, garantindo continuidade das políticas de segurança e visibilidade centralizada sobre cargas de trabalho híbridas, distribuídas entre data centers e nuvem pública.

d) Implementação de uma solução especializada de proteção contra ameaças e *spam* em *e-mail*, com foco especial nas contas utilizadas por magistrados. Essa proteção visa mitigar o impacto de campanhas de *phishing*, fraudes direcionadas e comprometimento de e-mail corporativo (BEC), utilizando tecnologias como *sandboxing*, reputação de remetentes, e autenticação reforçada (SPF, DKIM, DMARC).

e) Gestão centralizada e unificada da segurança, com automação de políticas, resposta proativa a incidentes, correlação de eventos em tempo real e geração de relatórios gerenciais e técnicos. Essa abordagem favorece a governança, reduz custos operacionais e amplia a capacidade de detecção e resposta.

f) Adoção de uma solução amplamente reconhecida pelo mercado, com a *Check Point* posicionada como líder no Quadrante Mágico do Gartner para *Firewalls* de Rede e soluções de segurança de *e-mail*, garantindo elevada taxa de bloqueio de ameaças (acima de 99,8%), escalabilidade e integração com o ecossistema de segurança existente.

Assim, a adesão à ATA de Registro de Preços não apenas moderniza a arquitetura de segurança do TJMG, como também fortalece sua resiliência cibernética frente a um cenário cada vez mais complexo de ameaças digitais

10. Estimativa do valor

O quadro abaixo apresenta o valor previsto para esta contratação, cujo detalhamento das estimativas consta no Anexo I deste documento.

Item	Valor da contratação				
	Descrição	Métrica	Qtde	Valor unitário	Total 36 meses
Next Generation Firewall – data Center Tipo 1	*Check Point*-9700 *Appliances-Plus* Licenciamento NGTX período de 36 meses (1915686)	Un	3	1.404.453,30	4.213.359,90
Next Generation Firewall – Sede Tipo 3	*Check Point* – 9300 *Appliance-Plus* licenciamento NGTX período 36 meses (1915676)	Un	4	876.164,40	3.504.657,60
Next Generation Firewall – Data Center Tipo 2	*Check Point* – 19100 *Appliance-Plus* licenciamento NGTX período 36 meses (1915696)	Un	2	2.340.086,90	4.680.173,80
Next Generation Firewall – Data Center Tipo 3	*Check Point* – 29100 *Appliance-Plus* licenciamento NGTX período 36 meses (1915700)	Un	2	3.134.582,20	6.269.164,40
Next Generation Firewall – Nuvem Privada	*Check Point* – *CloudGuard Network* com licenciamento NGTX (por core) por 36 meses (1410964)	Un	15	53.115,50	796.732,50
Solução de Gerenciamento Centralizados e Relatórios para até 13 equipamentos	Check Point – NGSM 50 GWs com licenciamento *SmartEvent na Smart Reporter* por 36 meses (1410964)	Serviço	2	573.473,90	1.146.947,80
Instalação de Firewall – Sede	Instalação *Firewall* Data Center Comprasnet: Und Serviço Técnico = serviço (1411017)	Serviço	6	30.248,60	181.491,60
Instalação Firewall – Data Center	Instalação *Firewall* Data Center Comprasnet: und Serviço Técnico: Serviço (141027)	Serviço	7	56.007,80	392.054,60
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall – Sede	Sérvio de Monitoramento e Suporte Técnico 24x7 de *Firewall* Sede – 36 Meses. Coprasnet: Und Serviço Técnico= Serviço (1411057)	Serviço	6	97.323,20	583.939,20
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall – Data Center	Serviço de monitoramento e suporte técnico 24x7 De *Firewall* Data Center – 36 meses. comprasnet: Und Serviço técnico = Serviço (1411067)	Serviço	7	237.910,20	1.665.371,40
Solução de Prevenção de Ameaças e Spam para E-mail em Nuvem – Office 365 e Google Workspace	*Check Point* – *Harmony E-maiil* com licenciamento complete por 36 meses (1915720)	Serviço	1.000	636,90	636.900,00
				Total da Solução	**24.070.792,80**

11. Descrição e Justificativa da Solução de TIC a Ser CONTRATADA

Recomenda-se a adoção da solução única de *firewall* de próxima geração, com a utilização de *appliances* físicos dedicados para o ambiente *on-premise* e instâncias virtuais (VMs) para os ambientes de nuvem pública.

Essa abordagem permite ao TJMG proteger, de forma robusta e integrada, tanto o perímetro da rede local quanto os ativos hospedados em ambientes de nuvem como AWS e OCI.

A aquisição dos *appliances* físicos atenderá plenamente às necessidades atuais de segurança do datacenter institucional, garantindo suporte completo ao *hardware* e *software* durante todo o ciclo de vida da solução. Já nos ambientes em nuvem, a utilização de *firewalls* em formato virtual (*CloudGuard IaaS*) proporciona flexibilidade, escalabilidade e proteção consistente em *workloads* distribuídos.

Recomenda-se ainda, adoção de uma solução especializada de prevenção de ameaças e *spam* para *e-mails* institucionais, com foco prioritário na proteção das contas de magistrados e unidades críticas. Essa solução deverá complementar as funcionalidades nativas do *Google Workspace*, oferecendo camada adicional de segurança baseada em inteligência artificial, validação de remetentes (SPF, DKIM e DMARC), *sandboxing* em tempo real e detecção de *phishing* sofisticado. Tal medida é fundamental para mitigar riscos de comprometimento por engenharia social, *malware* e fraudes direcionadas, assegurando a integridade da comunicação oficial e fortalecendo a resiliência cibernética do Tribunal.

12. Justificar o Parcelamento ou Não da Solução

É dever do administrador público proteger a Administração e o patrimônio público, assegurando que as contratações sejam realizadas de forma eficiente e vantajosa, conforme previsto no art. 37, inc. XXI da Constituição Federal de 1988. Dessa forma, o instrumento convocatório deve estabelecer exigências que garantam a adequada execução do objeto, sem comprometer o caráter competitivo do certame.

No caso específico desta contratação, os itens previstos compõem uma solução integrada de segurança perimetral, formada por *appliances* de *firewal*l, consoles centralizados de gerenciamento, relatoria e *logs*, além de serviço de instalação, configuração e monitoramento e suporte. A inter-relação entre o fornecimento do *hardware*, *softwares*, serviços e capacitação técnica é essencial para garantir o pleno funcionamento da solução e o sucesso da operação. O fracionamento da contratação em itens ou lotes distintos acarretaria riscos operacionais e administrativos, tais como:

a) **Descontinuidade e incompatibilidade operacional:** A contratação separada poderia gerar conflitos de responsabilidade entre fornecedores distintos, dificultando a gestão e a execução dos serviços de maneira integrada. Além disso, os consoles de gerenciamento centralizado e relatoria precisam ser plenamente compatíveis e integráveis com os *firewalls*, preferencialmente do mesmo fabricante, a fim de garantir suporte unificado, atualização coordenada e máxima eficiência operacional.

b) **Aumento da complexidade na implantação:** A instalação e configuração da solução exigem conhecimento técnico específico da arquitetura e dos componentes fornecidos. A divisão entre fornecedores poderia resultar em atrasos, retrabalho e dificuldades técnicas, comprometendo a eficiência da operação e a segurança da rede.

c) **Riscos à segurança da informação:** A solução trata diretamente da proteção do ambiente de TIC institucional. Fragmentar a responsabilidade entre fornecedores distintos poderia

comprometer a governança da segurança cibernética, além de dificultar a rastreabilidade e o controle sobre eventuais falhas ou vulnerabilidades.

d) **Maior custo operacional e administrativo:** A gestão de múltiplos contratos implicaria aumento da carga administrativa, necessidade de fiscalizações independentes e possível superposição de garantias e suportes, elevando os custos indiretos da contratação.

Diante desses fatores, o parcelamento da contratação comprometeria o alcance dos objetivos esperados, além de representar riscos desnecessários à Administração. A opção pelo lote único justifica-se pela necessidade de garantir a padronização, compatibilidade técnica, segurança, eficiência operacional e economicidade na execução da solução.

13. Demonstrativos dos Resultados Pretendidos

A presente demanda visa a mitigação de diversas ameaças de segurança cibernética que afetam a rede do judiciário, bem como obter os seguintes benefícios:

a) Aumentar o nível de proteção das informações trafegadas na rede judiciário;

b) Proteger contra acesso remoto não autorizado;

c) Permitir uso da internet com maior proteção;

d) Controlar o uso da internet pelos funcionários;

e) Bloquear conteúdo ilegal, imoral e improdutivo;

f) Proteger a rede corporativa contra *malwares* e outros tipos de ameaças cibernéticas

g) Inibir e impedir a invasão de *hackers*;

h) Permitir que funcionários remotos acessem a rede VPN de forma segura;

i) Elevar o nível de confiabilidade dos sistemas;

j) Promover compartilhamento seguro dos dados.

k) Reduzir drasticamente a exposição a ataques de *phishing*, fraudes por *e-mail* e engenharia social, especialmente em contas de magistrados e unidades críticas;

l) Evitar a entrega de mensagens com conteúdo malicioso ou *links* comprometidos por meio de tecnologias de *sandboxing* e validação reforçada de remetentes (SPF, DKIM e DMARC);

m) Garantir a integridade, disponibilidade e confiabilidade da comunicação institucional por e-*mail*, aumentando a resiliência cibernética e a confiança no uso desse canal essencial.

14. Providências

Para o início da execução dos serviços o TRIBUNAL deverá fornecer à CONTRATADA as informações e documentações indispensáveis à execução do objeto contratado, bem como acesso físico às instalações prediais.

15. Contratações correlatas e/ou interdependentes

Não há contratações interdependentes.

16. Impactos Ambientais

Não se vislumbra a ocorrência de possíveis impactos ambientais gerados pela contratação pretendida. Contudo, a CONTRATADA deverá conduzir suas ações em conformidade com os requisitos legais e regulamentos aplicáveis, observando também a legislação ambiental para a prevenção de adversidades ao meio ambiente e a saúde dos trabalhadores e envolvidos na execução do objeto.

17. Posicionamento Conclusivo

Com base nas informações levantadas neste Estudo Técnico Preliminar, a contratação é viável e adequada para atender à necessidade de aquisição perpétua de solução de NGFW.

18. Recursos Necessários à Continuidade do Negócio Durante e Após a Execução do Contrato

18.1. Recursos Materiais

Não há.

18.2. Recursos Humanos

Descrição do Recurso	Qtde.	Competência	Ação para obtenção do Recurso	Responsável
Fiscal Técnico	01	Fiscalizar a entrega do objeto, apoiar o Gestor do Contrato.	Designar servidor responsável pela fiscalização na GETEC	Gerente GETEC
Gestor do Contrato	01	Monitorar a execução do contrato - Autorizar emissão e pagamento NF.	Designar servidor responsável pela gestão nas gerências.	Gerente GETEC

18.3. Estratégia de Continuidade do fornecimento da solução de TIC

O TRIBUNAL pretende garantir a continuidade operacional da solução de segurança perimetral por meio das seguintes estratégias:

a) **Contrato com garantia estendida e suporte técnico:** A contratação contemplará garantia integral de *hardware* e *software* por 36 meses, com suporte técnico do fabricante ou parceiro autorizado, assegurando reposição de peças, atualizações, correções de segurança e atendimento a incidentes.

b) **Soluções redundantes e arquitetura resiliente:** A aquisição de múltiplos *appliances* e consoles possibilitará a distribuição das funções de segurança em mais de um ponto da rede, viabilizando cenários de contingência e continuidade em caso de falhas localizadas.

c) **Documentação técnica e procedimentos operacionais padrão (POP):** A CONTRATADA deverá entregar documentação completa da solução, incluindo manuais de configuração, rotinas de operação e procedimentos de recuperação, permitindo ao TRIBUNAL manter a operação de forma autônoma em caso de necessidade.

d) **Planejamento antecipado da nova contratação:** Considerando a vida útil estimada da solução, o TRIBUNAL iniciará, com antecedência mínima de 12 meses, o planejamento de nova contratação ou eventual prorrogação, garantindo transição suave e sem descontinuidade do serviço.

e) **Acompanhamento contratual contínuo:** A execução contratual será monitorada por equipe técnica, garantindo que as obrigações de suporte, manutenção e atualização sejam cumpridas

dentro dos prazos e padrões exigidos, evitando riscos futuros por negligência ou obsolescência não tratada.

18.4. Estratégia de Transição e Encerramento Contratual

O TRIBUNAL estabelecerá medidas para assegurar a **transição ordenada e segura** ao término do contrato, mitigando riscos de descontinuidade operacional, perda de dados ou vulnerabilidades de segurança. Para isso, serão adotadas as seguintes diretrizes:

a) **Transferência de conhecimento e documentação técnica atualizada:** A CONTRATADA deverá entregar, até os últimos 60 dias do contrato, toda a documentação técnica atualizada da solução, incluindo topologia, regras de segurança, configurações aplicadas, *logs* relevantes e relatórios de performance. Também será exigida uma sessão final de transferência de conhecimento com a equipe técnica do TRIBUNAL.

b) **Desinstalação e descarte controlado (se aplicável):** Em caso de substituição dos equipamentos ao final do contrato, a retirada deverá seguir protocolo seguro, com remoção adequada de dados, reversão de configurações sensíveis e *checklist* de desligamento ordenado, evitando vazamento de informações ou impacto na infraestrutura.

c) **Garantia de suporte até o encerramento efetivo:** O contrato exigirá que o suporte técnico (corretivo, evolutivo e de segurança) seja mantido em pleno funcionamento até a data final da vigência, inclusive nos últimos dias, assegurando que não haja desassistência técnica durante a transição.

d) **Plano de transição gradual (quando aplicável):** Caso a nova contratação envolva mudança de fabricante ou arquitetura, será elaborado plano de coexistência controlada entre a solução atual e a futura, com validação das novas configurações em paralelo e transição progressiva, de modo a garantir continuidade de serviço sem interrupções.

e) **Inventário final da solução:** Será produzido relatório de encerramento contendo o inventário completo dos ativos fornecidos, o status de cada equipamento/*software*, as intervenções realizadas e o histórico de chamados e atualizações ocorridas durante a vigência contratual.

18.5. Estratégia de Independência

Para mitigar o risco de dependência excessiva da CONTRATADA e garantir autonomia técnica e operacional do TRIBUNAL, serão adotadas as seguintes estratégias:

a) **Acesso administrativo pleno à solução:** A configuração dos equipamentos e consoles será realizada com contas administrativas controladas pelo TRIBUNAL, assegurando o acesso irrestrito aos recursos da solução, aos dados de configuração, aos relatórios e aos registros de *log*.

b) **Documentação técnica detalhada e atualizada:** A CONTRATADA será obrigada a entregar manuais, diagramas, topologias e procedimentos técnicos de instalação e operação, garantindo que o TRIBUNAL possa replicar, manter ou migrar a solução com base em conhecimento registrado e não proprietário.

c) **Adoção de tecnologias amplamente reconhecidas:** Será priorizada a contratação de solução baseada em tecnologias consolidadas e com ampla base de mercado, que evitem o uso de componentes excessivamente customizados ou com suporte restrito a um único fornecedor ou integrador.

d) **Planejamento de recontratação e ciclo de vida:** O TRIBUNAL monitorará o ciclo de vida da solução e iniciará com antecedência a estruturação de nova contratação, evitando prorrogações forçadas por dependência tecnológica ou ausência de domínio técnico interno.

19. Aprovação e Assinatura

Integrante Técnico	**Integrante Demandante**
Denilson dos Santos Rodrigues *GETEC/COINFRA* *TJ-13359* *Leonardo José Drummond* *GETEC/CONECT* *F0353086*	*Denilson dos Santos Rodrigues* *GETEC/COINFRA* *TJ-13359* *Leonardo José Drummond* *GETEC/CONECT* *F0353086*
Gestor Técnico	**Gestor Demandante**
Narciso Felício de Lima Junior *GETEC* *F0353920*	*Narciso Felício de Lima Junior* *GETEC* *F0353920*
A CECOR realizou a análise de conformidade do documento de acordo com Resolução nº 468/2022 do Conselho Nacional de Justiça.	
Juliano Rodrigo Luiz Araújo *Ass. Esp. suporte de contratação* *P0131794*	*Mateus Cançado Assis* *Assessor Técnico da CECOR* *TJ-6375-0*

Autoridade Máxima da Área de TIC (ou Autoridade Superior, se aplicável)
Alessandra Campos *Diretoria Executiva de Informática* *TJ-75804*

Anexo I – Estimativa de Valor

a) Contratações de outros órgãos

i) ATA DE REGISTRO DE PREÇOS nº 2025/03636 - Governo do Estado do Ceará – ETICE

Item	*ATA DE REGISTRO DE PREÇOS nº 2025/03636 GOVERNO DO ESTADO DO CEARÁ EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DO CEARÁ - ETICE*					
	Descrição	**Métrica**	**Qtde**	**Valor unitário**	**Total 36 meses**	**Total com serviços de instalação e suporte inclusos no Hardware**
Next Generation Firewall – Data Center Tipo 1	Check Point – 9700 Appliance- Plus licenciamento NGTX período de 36 meses (1915686)	UN	3	R$ 1.404.453,30	**R$ 4.213.359,90**	R$ 5.095.113,90
Next Generation Firewall – Sede Tipo 3	Check Point – 9300 Appliance- Plus licenciamento NGTX período de 36 meses (1915676)	UN	4	R$ 876.164,40	**R$ 3.504.657,60**	R$ 4.014.944,80
Next Generation Firewall – Data Center Tipo 2	Check Point - 19100 Appliance- Plus licenciamento NGTX período de 36 meses (1915696)	UN	2	R$ 2.340.086,90	**R$ 4.680.173,80**	R$ 5.268.009,80
Next Generation Firewall – Data Center Tipo 3	Check Point - 29100 Appliance- Plus licenciamento NGTX período de 36 meses (1915700)	UN	2	R$ 3.134.582,20	**R$ 6.269.164,40**	R$ 6.857.000,40
Next Generation Firewall – Nuvem Privada	Check Point - CloudGuard Network com licenciamento NGTX (por core) por 36 meses (1915710)	UN	15	R$ 53.115,50	**R$ 796.732,50**	R$ 1.051.876,10
Solução de Gerenciamento Centralizado e Relatórios para até 50 equipamentos	Check Point - NGSM 50 GWs com licenciamento SmartEvent and Smart Reporter por 36 meses (1410964)	Serviço	2	R$ 573.473,90	**R$ 1.146.947,80**	R$ 1.146.947,80
Instalação Firewall - Sede *	Instalação Firewall Sede Comprasnet: Und Serviço Técnico = Serviço (1411017)	Serviço	6	R$ 30.248,60	**R$ 181.491,60**	-
Instalação Firewall - Data Center	Instalação Firewall Data Center Comprasnet: Und Serviço Técnico = Serviço (1411027)	Serviço	7	R$ 56.007,80	**R$ 392.054,60**	-
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall - Sede*	Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall Sede – 36 Meses. Comprasnet: Und Serviço Técnico = Serviço (1411057)	Serviço	6	R$ 97.323,20	**R$ 583.939,20**	-
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall - Data Center	Serviço de Monitoramento e Suporte Técnico 24x7 De Firewall Data Center – 36 Meses. Comprasnet: Und Serviço Técnico = Serviço (1411067)	Serviço	7	R$ 237.910,20	**R$ 1.665.371,40**	-
Solução de Prevenção de Ameaças e Spam para E-Mail em Nuvem – Office 365 e Google Workspace**	Check Point – Harmony E-mail com licenciamento complete por 36 meses (1915720)	Serviço	1150	R$ 636,90	**R$ 732.435,00**	R$ 732.435,00
				Total da solução	**R$ 24.166.327,80**	**R$ 24.166.327,80**

* Quantitativo previsto para atender 4 Firewall Sede + 2 Firewall de Nuvem

** Quantitativo previsto para atender aos Desembargadores e Juizes.

ii) ATA DE REGISTRO DE PREÇOS nº 007/2024 - Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro

Item	ATA DE REGISTRO DE PREÇOS nº 007/2024 - Centro de Tecnologia de Informação e Comunicação do Estado do Rio de Janeiro					
	Descrição	Métrica	Qtde	Valor unitário	Total 60 meses	Total 36 meses
Next Generation Firewall – Data Center Tipo 1	Aquisição de appliance firewall Tipo 1 - inclusos: hardware, licenciamento, instalação, configuração e garantia por 60 meses*	UN	3	R$ 6.090.000,00	R$ 18.270.000,00	**R$ 17.539.200,00**
Next Generation Firewall – Sede Tipo 3	Item não solicitado					
Next Generation Firewall – Data Center Tipo 2	Aquisição de appliance firewall Tipo 1 - inclusos: hardware, licenciamento, instalação, configuração e garantia por 60 meses*	UN	2	R$ 6.090.000,00	R$ 12.180.000,00	**R$ 11.692.800,00**
Next Generation Firewall – Data Center Tipo 3	Aquisição de appliance firewall Tipo 1 - inclusos: hardware, licenciamento, instalação, configuração e garantia por 60 meses*	UN	2	R$ 6.090.000,00	R$ 12.180.000,00	**R$ 11.692.800,00**
Next Generation Firewall – Nuvem Privada	Item não solicitado					
Solução de Gerenciamento Centralizado e Relatórios para até 50 equipamentos	Aquisição de console de gerenciamento centralizado para o firewall Tipo 1 com garantia de 60 meses	Serviço	2	R$ 74.000,00	R$ 148.000,00	**R$ 88.800,00**
	Aquisição de console de gerenciamento de logs para o firewall Tipo 1 com garantia de 60 meses	Serviço	2	R$ 74.000,00	R$ 148.000,00	**R$ 88.800,00**
	Aquisição de console de relatoria centralizada para o firewall Tipo 1 com garantia de 60 meses	Serviço	2	R$ 74.000,00	R$ 148.000,00	**R$ 88.800,00**
Instalação Firewall - Sede	Item não solicitado					
Instalação Firewall - Data Center	Incluso no custo do Hardware					
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall - Sede	Incluso no custo do Hardware					
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall - Data Center	Incluso no custo do Hardware					
Solução de Prevenção de Ameaças e Spam para E-Mail em Nuvem – Office 365 e Google Workspace	Item não solicitado					
					Total da solução	**R$ 41.191.200,00**

* Foi considerado que 10% do valor do item refere-se ao suporte, aplicou-se regra de três sobre o mesmo para obter a estimativa de 36 meses. O restante do valor refere-se ao Hardware e sua instalação. O percentual de 10% foi obtido na ata através da ATA DE REGISTRO DE PREÇOS nº 2025/03636 - GOVERNO DO ESTADO DO CEARÁ EMPRESA DE TECNOLOGIA DA INFORMAÇÃO DO CEARÁ - ETICE.

iii) ATA DE REGISTRO DE PREÇOS nº Nº 00006/2024 - Ministério da Cultura

Item	ATA DE REGISTRO DE PREÇOS nº Nº 00006/2024 - Ministério da Cultura				
	Descrição	Métrica	Qtde	Valor unitário	Total 36 meses
Next Generation Firewall – Data Center Tipo 1	Item não solicitado				
Next Generation Firewall – Sede Tipo 3	Item não solicitado				
Next Generation Firewall – Data Center Tipo 2	Item não solicitado				
Next Generation Firewall – Data Center Tipo 3	Item não solicitado				
Next Generation Firewall – Nuvem Privada	Item não solicitado				
Solução de Gerenciamento Centralizado e Relatórios para até 50 equipamentos	Item não solicitado				
Instalação Firewall - Sede	Item não solicitado				
Instalação Firewall - Data Center	Item não solicitado				
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall - Sede	Item não solicitado				
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall - Data Center	Item não solicitado				
Solução de Prevenção de Ameaças e Spam para E-Mail em Nuvem – Office 365 e Google Workspace	Aquisição de licenças de soware de solução de prevenção contra vazamento de dados - Data Loss Preven on DLP, com garan a e suporte para 36 meses Modelo: Forcepoint Classifica on powered by Getvisibility (CLASSIFY) & Forcepoint DLP Suite (IP Protec on) (FDLPSIP). Fabricante: FORCEPOINT	UN	1150	R$ 2.375,00	**R$ 2.731.250,00**
				Total da solução	**R$ 2.731.250,00**

iv) CONTRATO ADMINISTRATIVO Nº 16/2023 - Hospital das Forças Armadas (HFA)

Item	CONTRATO ADMINISTRATIVO Nº 16/2023 - HOSPITAL DAS FORÇAS ARMADAS						
	Descrição	Métrica	Qtde	Valor unitário	Valor unitário corrigido (Dez/2023 a Mai/2025 - IPCA)	Total 36 meses	Total com serviços de instalação e suporte inclusos no Hardware
Next Generation Firewall – Data Center Tipo 1*	Firewall Palo Alto Networks PA-5220 (PAN-PA-5220-AC) para Alta Disponibilidade com licenciamento ADVURL (Advanced URL Filtering), TP (Threat Prevention), WF (WildFire), GP (Global Protect) e garantia da Fabricante para o período de 36 (trinta e seis) meses, incluindo todos os acessórios (SFP+ SR 10GigE transceiver), instalação física e lógica.	UN	3	R$ 1.845.000,00	R$ 1.998.368,76	**R$ 5.995.106,28**	**R$ 6.087.178,59**
Next Generation Firewall – Sede Tipo 3*	Firewall Palo Alto Networks PA-5220 (PAN-PA-5220-AC) para Alta Disponibilidade com licenciamento ADVURL (Advanced URL Filtering), TP (Threat Prevention), WF (WildFire), GP (Global Protect) e garantia da Fabricante para o período de 36 (trinta e seis) meses, incluindo todos os acessórios (SFP+ SR 10GigE transceiver), instalação física e lógica.	UN	4	R$ 1.845.000,00	R$ 1.998.368,76	**R$ 7.993.475,04**	**R$ 8.116.238,12**
Next Generation Firewall – Data Center Tipo 2	Item não solicitado						
Next Generation Firewall – Data Center Tipo 3	Item não solicitado						
Next Generation Firewall – Nuvem Privada	Item não solicitado						
Solução de Gerenciamento Centralizado e Relatórios para até 50 equipamentos	Item não solicitado						
Instalação Firewall - Sede	Incluso no custo do Hardware						
Instalação Firewall - Data Center*	Incluso no custo do Hardware						
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall - Sede*	Serviços de sustentação do ambiente de Segurança da Informação por um período de 36 (trinta e seis) meses, com suporte técnico remoto e on-site, monitoramento e gerenciamento centralizado da plataforma de segurança de Firewall da fabricante Palo Alto Networks, constante de 2 (dois) appliances modelo PAN PA-5220-AC.	Serviço	6	R$ 28.400,00	R$ 30.690,77	**R$ 184.144,62**	
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall - Data Center	Serviços de sustentação do ambiente de Segurança da Informação por um período de 36 (trinta e seis) meses, com suporte técnico remoto e on-site, monitoramento e gerenciamento centralizado da plataforma de segurança de Firewall da fabricante Palo Alto Networks, constante de 2 (dois) appliances modelo PAN PA-5220-AC.	Serviço	7	R$ 28.400,00	R$ 30.690,77	**R$ 214.835,39**	
Solução de Prevenção de Ameaças e Spam para E-Mail em Nuvem – Office 365 e Google Workspace**	Item não solicitado						
					Total da solução	**R$ 14.387.561,33**	

* Análise técnica: O FW Palo Alto 5220 pode ser usado em duas linhas de comparação, tanto para a linha do Firewall Sede Tipo 3 (CheckPoint 9300), quanto do Datacenter Tipo 1 (CheckPoint 9700).

v) ATA DE REGISTRO DE PREÇOS nº 00016/2023 - Instituto Federal de Educação, Ciência e Tecnologia de Sergipe

Item	ATA DE REGISTRO DE PREÇOS nº 00016/2023 - Instituto Federal de Educação, Ciência e Tecnologia de Sergipe						
	Descrição	Métrica	Qtde	Valor unitário	Valor unitário corrigido (Jun/2023 a Mai/2025 - IPCA)	Total 60 meses	Total 36 meses
Next Generation Firewall – Data Center Tipo 1	Item não solicitado						
Next Generation Firewall – Sede Tipo 3*	Solução de Gerência e Segurança de Rede NGFW em Cluster de Alta Disponibilidade Tipo A	UN	4	R$ 630.072,26	R$ 689.642,00	R$ 2.758.568,00	**R$ 1.655.140,80**
Next Generation Firewall – Data Center Tipo 2	Item não solicitado						
Next Generation Firewall – Data Center Tipo 3	Item não solicitado						
Next Generation Firewall – Nuvem Privada	Item não solicitado						
Solução de Gerenciamento Centralizado e Relatórios para até 50 equipamentos	Item não solicitado						
Instalação Firewall - Sede	Incluso no custo do Hardware						
Instalação Firewall - Data Center	Item não solicitado						
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall - Sede	Incluso no custo do Hardware						
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall - Data Center	Item não solicitado						
Solução de Prevenção de Ameaças e Spam para E-Mail em Nuvem – Office 365 e Google Workspace	Item não solicitado						
						Total da solução	**R$ 1.655.140,80**

* Análise técnica: O FW Fortigate 600F pode ser usado em comparação na linha do Firewall Sede Tipo 3 (CheckPoint 9300).

b) Propostas comerciai

i) MPE

3. Condições Comerciais

DADOS DE FATURAMENTO DO CLIENTE	**Razão Social:**	TJMG TRIBUNAL DA JUSTICA DO ESTADO DE MINAS GERAIS
	CNPJ:	21.154.554/0001-13
	Venda a:	Isento / Não contribuinte
	Contato:	Adriana de Andrade Moura
	E-mail:	adriana.moura@tjmg.jus.br
	Fone:	-
	Endereço:	Av. Afonso Pena, 4001 - Serra, Belo Horizonte - MG - **CEP:** 30130-924

FATURADO POR	CNPJ	COND. PAGAMENTO
MPE COMERCIO DE EQUIPAMENTOS PARA INFORMATICA E SOLUCOES LTDA.	07.234.508/0001-01	30 DDF

Descrição	Métrica	Qtde	Valor Unitário	Valor Total
Check Point - 9700 Appliance - Plus licenciamento NGTX período de 36 meses (1915686)	UN	3	**R$ 1.830.000,00**	**R$ 5.490.000,00**
Check Point - 9300 Appliance - Plus licenciamento NGTX período de 36 meses (1915676)	UN	4	**R$ 1.110.000,00**	**R$ 4.440.000,00**
Check Point -19100 Appliance - Plus licenciamento NGTX período de 36 meses (1915696)	UN	2	**R$ 3.050.000,00**	**R$ 6.100.000,00**
Check Point - 29100 Appliance - Plus licenciamento NGTX período de 36 meses (1915700)	UN	2	**R$ 4.780.000,00**	**R$ 9.560.000,00**
Check Point - CloudGuard Network com licenciamento NGTX (por core) por 36 meses (1915710)	UN	15	**R$ 225.000,00**	**R$ 3.375.000,00**
Check Point - NGSM 50 GWs com licenciamento SmartEvent and SmartReporter por 36 meses (1410964)	Serviço	2	**R$ 890.000,00**	**R$ 1.780.000,00**
Instalação Firewall Sede Comprasnet: Und Serviço Técnico = Serviço (1411017)	Serviço	6	**R$ 230.000,00**	**R$ 1.380.000,00**
Instalação Firewall Data Center Comprasnet: Und Serviço Técnico = Serviço (1411027)	Serviço	7	**R$ 380.000,00**	**R$ 2.660.000,00**
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall Sede - 36 Meses. Comprasnet: Und Serviço Técnico = Serviço (1411057)	Serviço	6	**R$ 480.000,00**	**R$ 2.880.000,00**
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall Data Center - 36 Meses. Comprasnet: Und Serviço Técnico = Serviço (1411067)	Serviço	7	**R$ 687.000,00**	**R$ 4.809.000,00**
Check Point - Harmony E-mail com licenciamento complete por 36 meses (1915720)	Serviço	1000	**R$ 1.730,00**	**R$ 1.730.000,00**

VALOR TOTAL: R$ 44.204.000,00

ii) **CONVERSYS**

Valores

Respondendo sua solicitação a empresa **CONVERSYS IT SOLUTIONS COMERCIO E SERVICOS DE TECNOLOGIA LTDA, CNPJ/MF 24.235.348/0001-26,** apresenta sua proposta comercial para venda de Solução de Segurança da Informação (Firewall), com serviços de instalação, suporte e assistência técnica, conforme descrição constante no Termo de Referência, pelo valor global de **R$ 10.319.176,00** (dez milhões, trezentos e dezenove mil, cento e setenta e seis reais).

Tabela de quantitativo dos itens que serão contratados:

Descrição	Métrica	Qtde	Valor Unitário	Valor Total
Check Point - 9700 Appliance - Plus licenciamento NGTX período de 36 meses (1915686)	UN	3	R$ 1.995.524,00	R$ 5.986.572,00
Check Point - 9300 Appliance - Plus licenciamento NGTX período de 36 meses (1915676)	UN	4	R$ 1.087.530,00	R$ 4.350.120,00
Check Point -19100 Appliance - Plus licenciamento NGTX período de 36 meses (1915696)	UN	2	R$ 3.134.380,00	R$ 6.268.760,00
Check Point - 29100 Appliance - Plus licenciamento NGTX período de 36 meses (1915700)	UN	2	R$ 4.983.270,00	R$ 9.966.540,00
Check Point - CloudGuard Network com licenciamento NGTX (por core) por 36 meses (1915710)	UN	15	R$ 138.400,00	R$ 2.076.000,00
Check Point - NGSM 50 GWs com licenciamento SmartEvent and SmartReporter por 36 meses (1410964)	Serviço	2	R$ 947.200,00	R$ 1.894.400,00
Instalação Firewall Sede Comprasnet: Und Serviço Técnico = Serviço (1411017)	Serviço	6	R$ 192.500,00	R$ 1.155.000,00
Instalação Firewall Data Center Comprasnet: Und Serviço Técnico = Serviço (1411027)	Serviço	7	R$ 278.500,00	R$ 1.949.500,00
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall Sede - 36 Meses. Comprasnet: Und Serviço Técnico = Serviço (1411057)	Serviço	6	R$ 195.500,00	R$ 1.173.000,00
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall Data Center - 36 Meses. Comprasnet: Und Serviço Técnico = Serviço (1411067)	Serviço	7	R$ 498.300,00	R$ 3.488.100,00
Check Point - Harmony E-mail com licenciamento complete por 36 meses (1915720)	Serviço	1000	R$ 1.150,00	R$ 1.150.000,00
			Total	**R$ 39.457.992,00**

iii) Simulação considerando o menor preço de cada item ofertado nas propostas recebidas

Menor preço da Propostas por item					
Descrição	**Métrica**	**Qtde**	**Valor Unitário**	**Valor Total**	**Total com serviços de instalação e suporte inclusos no Hardware**
Check Point - 9700 Appliance - Plus licenciamento NGTX período de 36 meses (1915686)	UN	3	R$ 1.830.000,00	R$ 5.490.000,00	R$ 7.820.400,00
Check Point - 9300 Appliance - Plus licenciamento NGTX período de 36 meses (1915676)	UN	4	R$ 1.087.530,00	R$ 4.350.120,00	R$ 5.902.120,00
Check Point -19100 Appliance - Plus licenciamento NGTX período de 36 meses (1915696)	UN	2	R$ 3.050.000,00	R$ 6.100.000,00	R$ 7.653.600,00
Check Point - 29100 Appliance - Plus licenciamento NGTX período de 36 meses (1915700)	UN	2	R$ 4.780.000,00	R$ 9.560.000,00	R$ 11.113.600,00
Check Point - CloudGuard Network com licenciamento NGTX (por core) por 36 meses (1915710)	UN	15	R$ 138.400,00	R$ 2.076.000,00	R$ 2.852.000,00
Check Point - NGSM 50 GWs com licenciamento SmartEvent and SmartReporter por 36 meses (1410964)	Serviço	2	R$ 890.000,00	R$ 1.780.000,00	R$ 1.780.000,00
Instalação Firewall Sede Comprasnet: Und Serviço Técnico = Serviço (1411017)	Serviço	6	R$ 192.500,00	R$ 1.155.000,00	-
Instalação Firewall Data Center Comprasnet: Und Serviço Técnico = Serviço (1411027)	Serviço	7	R$ 278.500,00	R$ 1.949.500,00	-
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall Sede - 36 Meses. Comprasnet: Und Serviço Técnico = Serviço (1411057)	Serviço	6	R$ 195.500,00	R$ 1.173.000,00	-
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall Data Center - 36 Meses. Comprasnet: Und Serviço Técnico = Serviço (1411067)	Serviço	7	R$ 498.300,00	R$ 3.488.100,00	-
Check Point - Harmony E-mail com licenciamento complete por 36 meses (1915720)	Serviço	1150	R$ 1.150,00	R$ 1.322.500,00	R$ 1.322.500,00
			Valor Total	**R$ 38.444.220,00**	**R$ 38.444.220,00**

iv) Custo médio obtido

Item	Média
Next Generation Firewall – Data Center Tipo 1	R$ 9.135.473,12
Next Generation Firewall – Sede Tipo 3	R$ 4.922.110,93
Next Generation Firewall – Data Center Tipo 2	R$ 8.204.803,27
Next Generation Firewall – Data Center Tipo 3	R$ 9.887.800,13
Next Generation Firewall – Nuvem Privada	R$ 1.951.938,05
Solução de Gerenciamento Centralizado e Relatórios para até 50 equipamentos	R$ 1.064.449,27
Instalação Firewall - Sede	Incluso no custo do Hardware
Instalação Firewall - Data Center	Incluso no custo do Hardware
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall - Sede	Incluso no custo do Hardware
Serviço de Monitoramento e Suporte Técnico 24x7 de Firewall - Data Center	Incluso no custo do Hardware
Solução de Prevenção de Ameaças e Spam para E-Mail em Nuvem – Office 365 e Google Workspace**	R$ 1.595.395,00
Total	**R$ 36.761.969,77**

Anexos II - Especificação dos Requisitos tecnológicos

A solução a ser CONTRATADA deverá atender, no mínimo, aos seguintes requisitos de negócio:

1. Arquitetura e Escalabilidade

1.1. Basear-se em tecnologias consolidadas, atualizadas e com arquitetura escalável;

1.2. Compatibilidade com ambientes híbridos (*on-premises* e nuvem pública como AWS e OCI);

1.3. Suporte nativo à alta disponibilidade (HA) e *failover* automático.

2. Funcionalidades de NGFW (Next-Generation Firewall)

2.1. Inspeção profunda de pacotes (*Deep Packet Inspection* – DPI);

2.2. Controle de aplicações com base em identidade e contexto;

2.3. Sistema de Prevenção de Intrusão (IPS) embarcado;

2.4. Filtragem de conteúdo e URLs maliciosos com categorias personalizáveis;

2.5. Inspeção de tráfego criptografado (TLS/SSL);

2.6. Suporte a protocolos de VPN seguros (IPSec, SSL) e funcionalidades de *Proxy* nativo;

2.7. Segmentação lógica baseada em identidade, grupo ou aplicação;

2.8. Suporte a *firewalls* virtuais (VM-based) com funcionalidades equivalentes aos *appliances* físicos.

3. Gerenciamento e Integração

3.1. Plataforma centralizada para gerenciamento unificado de políticas, *logs* e alertas;

3.2. *Dashboards* customizáveis e visibilidade em tempo real;

3.3. Integração via APIs abertas com soluções de XDR e MFA;

3.4. Integração com diretórios corporativos (LDAP, *Active Directory*, SAML);

3.5. Atualizações automáticas de assinaturas de ameaças e correções de segurança.

4. Proteção de *E-mail*

4.1. Solução especializada de *Email Security*, com foco especial nas contas de magistrados;

4.2. Detecção de ameaças com uso de inteligência artificial e *machine learning*;

4.3. *Sandboxing* em tempo real de *links* e anexos suspeitos;

4.4. Autenticação reforçada de remetentes (SPF, DKIM, DMARC);

4.5. Mecanismos de quarentena, isolamento de ameaças e resposta automática a incidentes;

4.6. Proteção contra *phishing*, *spear phishing*, *business email compromise* (BEC);

4.7. Integração com o ambiente do *Google Workspace* e visibilidade em tempo real dos eventos de segurança.

5. Licença Padrão

5.1. Entende-se por Licença Padrão a licença de uso do fabricante em caráter permanente e perpétuo para todas as funcionalidades e quantidades mencionadas neste documento, com exceção aos itens relacionados à Atualização de Assinaturas de Proteção.

5.2. Entende-se por Atualização de Assinaturas de Proteção todas as funcionalidades, manuais ou automatizadas, necessárias para manter a solução em seu nível de identificação e proteção mais atualizado, tais como: atualização de assinaturas de prevenção de intrusão, assinaturas de identificação de vírus, assinaturas de identificação de aplicações, listas de classificação de URLs, listas de geolocalização, listas de endereços IPs utilizados por *botnets*, listas de endereços IPs de reputação duvidosa etc.

5.3. Todos os equipamentos *firewall* devem possuir esta licença ativada.

6. Licença de Atualização de Segurança

6.1. Entende-se por Licença de Atualização de Segurança a licença de uso do fabricante que permita a utilização das funcionalidades e quantidades mencionadas neste documento para os itens relacionados à Atualização de Assinaturas de Proteção.

6.2. A licença deve permitir que todas as assinaturas, listas e demais métodos de detecção e prevenção de ameaças e de filtros de conteúdo e aplicação empregados pela solução sejam atualizados até suas últimas versões disponíveis.

6.3. As Licenças de Atualização de Segurança devem ter prazo de vigência de 36 (trinta e seis) meses, contados a partir da aplicação destas nos produtos.

7. *Hardware*

7.1. Deve ser fornecido em formato *appliance* físico.

7.2. Deve ser novo, sem uso, entregue em perfeito estado de funcionamento, sem marcas, amassados, arranhões ou outros problemas físicos, acondicionados em suas embalagens originais.

7.3. Não serão aceitos modelos de equipamento incluídos em listas de *End-of-Sale* (EOS) cuja data de fim de comercialização seja anterior à data de apresentação da proposta;

7.4. Não serão aceitos modelos que constem em listas de *End-of-Support* (EOS/EOL) cuja data de fim de suporte técnico seja anterior ao término da vigência contratual e/ou ao período de garantia e suporte exigido neste edital.

7.5. Deve ser apropriado para operação em ambientes tropicais, suportando condições ambientais com temperatura de operação entre 0°C e 40°C e umidade relativa do ar entre 5% e 95%, sem condensação.

7.6. Deve possuir MTBF (*Mean Time Between Failures*) superior a 10 anos, assegurando alta confiabilidade e durabilidade operacional.

7.7. Deve possuir fonte com alimentação nominal de 100~120VAC e 210~230VAC e frequência de 50 ou 60 Hz ou auto *ranging*. Deve vir acompanhado de cabo de alimentação, com *plug* tripolar 2P+T no padrão ABNT NBR 14136.

7.8. Deve possuir, no mínimo, 1 (uma) interface *Ethernet* dedicada para gerenciamento.

7.9. O plano de gerenciamento da solução deve ser apartado do plano de dados, com recursos de CPU, memória e interface de rede dedicados para esta função;

7.10. Deve ser fornecido acima de sua capacidade de base, em relação a processamento, memória e armazenamento interno.

7.11. Deve ser fornecido com todas as suas portas de comunicação, interfaces e afins habilitadas, operacionais e prontas para operação, com os seus respectivos *transceivers*.

8. Funcionalidades Básicas

8.1. Deve possuir MIB (*Management Information Bases*) própria contemplando, no mínimo, indicadores de estado do *hardware* e de performance do equipamento.

8.2. Deve suportar o envio de notificações via e-*mail*, SNMP *(Simple Network Management Protocol) traps* e mensagens de *log*.

8.3. Deve permitir o acesso ao equipamento via SSH e interface *web* HTTPS.

8.4. A comunicação entre a estação de trabalho do administrador e o firewall deve ser autenticada e criptografada.

8.5. Deve informar a utilização dos recursos de CPU, memória e atividade de rede.

8.6. Deve possuir visualização mínima sumarizada de aplicações, ameaças, URLs, endereços de origem, endereços de destino, levando-se em conta o quantitativo de sessões, de consumo de banda e categorização.

8.7. Deve possuir a funcionalidade de exportação automática dos *logs* para servidor *syslog* e para a solução de gerenciamento de *logs*.

8.8. Desejável possuir plano de gerenciamento segregado do plano de dados, inclusive com CPU e interfaces dedicadas.

8.9. Deve permitir a importação, criação e edição de regras *SNORT*.

8.10. Os *Firewalls* de segurança físico ou virtualizados, devem possuir processamento dedicado no equipamento de segurança para funções e ações de Gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problemas. Entre as funções, deve suportar no mínimo: acesso SSH, acesso *WEB*, alterações de política, comunicação *SNMP*.

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

9. Rede

9.1. Deve suportar os protocolos IPv4 e IPv6.

9.2. Deve suportar VLAN no padrão 802.1q.

9.3. Deve suportar Jumbo Frames.

9.4. Deve suportar sub interfaces *Ethernet* lógicas.

9.5. Deve suportar o protocolo NTP.

9.6. Deve implementar mecanismo de conversão de endereços NAT (*Network Address Translation*), de forma a possibilitar a realização de NAT estático (1-1), dinâmico (N-1), NAT pool (N-N) e NAT condicional (possibilitando que um endereço tenha mais de um NAT dependendo da origem, destino ou porta).

9.7. Deve permitir o registro de eventos de NAT com as informações de endereço interno, endereço público, data e hora do evento, portas de origem e destino.

9.8. Deve suportar tradução de porta (PAT).

9.9. Deve suportar as funcionalidades de roteamento estático e dinâmico em IPv4 e IPv6.

9.10. Deve suportar os protocolos RIP, OSPF v2, OSPF v3 e BGP v4.

9.11. Deve suportar os protocolos IGMP v2, IGMP v3, PIM-SM.

9.12. Deve suportar *Virtual Routing Redundancy Protocol* (VRRP) ou equivalente.

9.13. Deve ter compatibilidade com os protocolos SNMPv2 e SNMPv3, possibilitando o monitoramento via sistemas de gerenciamento de rede.

9.14. Deve permitir monitorar, via SNMP, falhas de *hardware*, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN, CPU, memória, status do *cluster* de Alta Disponibilidade e estatísticas de uso das interfaces de rede.

9.15. Deve suportar *Policy Based Routing* (PBR), possibilitando políticas de roteamento condicionado ao endereço IP de origem, endereço IP de destino e porta de comunicação.

9.16. Deve suportar no mínimo as seguintes funcionalidades: SLAAC (*address* auto *configuration*), NAT64, Identificação de usuários a partir do LDAP/AD, *Captive* Portal, IPv6 over IPv4 IPSec, Regras de proteção contra dos (*Denial of Service*), *Decriptografia* SSL e SSH, PBF (*Policy Based Forwarding*), QoS, DHCPv6 *Relay*, IPSEc, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS, *Neighbor Discovery* (ND), *Recursive* DNS *Server* (RDNSS).

10. Autenticação e Identificação de Usuários:

10.1. Deve promover a integração com serviços de diretório LDAP e *Active Directory*, baseados em caracteres da língua portuguesa, para a identificação, autenticação, autorização e registro de eventos de acessos ou ameaças.

10.2. Deve identificar de forma transparente os usuários autenticados por meio de serviço de diretório LDAP ou *Active Directory*.

10.3. Não será permitida a utilização de agentes instalados nos servidores LDAP, *Active Directory, proxies* internos e equipamentos dos usuários, nem configuração adicional no navegador.

10.4. Não será permitida a interceptação ou espelhamento do tráfego destinado aos servidores LDAP, *Active Directory* e *proxies* internos.

10.5. Deve possuir portal de autenticação (*captive* portal) para a identificação e autenticação de usuários não registrados ou não reconhecidos.

10.6. O portal de autenticação deve ser capaz de identificar e autenticar usuários cadastrados em serviço de diretório LDAP *e Active Directory*.

10.7. Deve permitir a criação de políticas de segurança baseadas em usuários e grupos de usuários pertencentes a um diretório LDAP ou ao *Active Directory*.

10.8. Deve registrar a identificação do usuário em todos os *logs* de eventos de acesso ou de ameaças gerados pelo equipamento.

10.9. Deve registrar os eventos dos usuários em tempo real, sem a utilização de processos em lote (*batches*) ou processos de correlação após a ocorrência do evento em questão.

10.10. Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura.

10.11. Desejável possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em servidores acessados remotamente, mesmo que não sejam servidores *Windows*.

10.12. Desejável identificar usuários através de leitura do campo x-*fowarded*-for, populando nos *logs* do *firewall* o endereço IP, bem como o usuário de rede responsável pelo acesso.

11. Geolocalização

11.1. Deve identificar os países de origem e destino de todas as conexões estabelecidas através do equipamento.

11.2. Deve-se identificar, no mínimo, 180 países.

11.3. Deve armazenar as listas de geolocalização no próprio equipamento.

11.4. Deve permitir a criação de políticas de segurança baseadas em geolocalização, permitindo o bloqueio de tráfego com origem ou destino a determinado país ou grupo de países.

11.5. Deve possibilitar a visualização dos países de origem e destino nos *logs* de eventos de acessos e ameaças.

12. VPN

12.1. Deve suportar VPN *site-to-site* em topologia *Full Meshed* (todos os *gateways* possuem links específicos para todos os demais *gateways*) e Estrela (*gateways* satélites se comunicam somente com um único *gateway* central).

12.2. Deve suportar criptografia 3DES, AES-128, AES-256.

12.3. Deve suportar integridade de dados com MD5, SHA-1 e SHA-256.

12.4. Deve suportar o protocolo IKE, fases I e II.

12.5. Deve suportar os algoritmos RSA e *Dif ie-He lman groups* 1, 2, 5 e 14.

12.6. Deve suportar Certificado Digital X.509.

12.7. Deve suportar NAT-T (NAT Transversal).

12.8. Deve permitir a criação de túneis VPN SSL/TLS e IPSec.

12.9. Deve suportar VPN *IPSec client-to-site* (acesso remoto).

12.10. Deve possuir cliente próprio para instalação nos dispositivos móveis dos usuários, sem custo adicional.

12.11. Deve permitir que o usuário realize a conexão VPN por meio de cliente instalado nos sistemas operacionais: *Windows*, Mac OS ou Linux do seu equipamento ou então por meio de interface *web* do tipo portal.

12.12. Caso o acesso seja feito por meio da interface Web, deverá ser compatível com, no mínimo, as versões atualizadas dos seguintes navegadores: *Microsoft Edge, Mozilla Firefox e Google Chrome.*

12.13. Deve suportar atribuição de endereço IP nos clientes remotos de VPN.

12.14. Deve suportar atribuição de DNS nos clientes remotos de VPN.

12.15. Deve suportar, no mínimo, os protocolos de roteamento estático e dinâmico OSPF e BGP.

12.16. O túnel IPSec VPN do cliente ao *gateway* (*client-to-site*) deve fornecer uma solução de autenticação única (*single-sign- on*) aos usuários, integrando-se com as ferramentas de *Windows login*.

12.17. O túnel IPSec VPN *client-to-site* deve também possuir autenticação em fator duplo (2FA) aos usuários.

12.18. Deve permitir criar políticas por usuário e grupos para tráfego de VPN *client-to-site*.

12.19. Deve suportar autoridade certificadora integrada ao *gateway* VPN ou à solução de gerenciamento centralizado.

12.20. Deve promover a integração com diretórios LDAP e *Active Directory* para a autenticação de usuários de VPN e regras de acesso.

12.21. Deve suportar os métodos de autenticação de VPN: usuário e senha de base interna do próprio equipamento, usuário e senha de diretório LDAP, usuário e senha do *Active Directory*, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao equipamento ou à solução de gerenciamento centralizado, certificação digital por meio de certificados emitidos por autoridade certificadora integrada ao *Active Directory*, certificação digital por meio de certificados emitidos por autoridade certificadora no padrão ICP-Brasil.

12.22. Deve suportar a integração com autoridades certificadoras de terceiros que possam gerar certificados no formato PKCS#12.

12.23. Deve suportar a solicitação de emissão de certificados a uma autoridade certificadora de confiança via SCEP (*Simple Certificate Enrollment Protocol*) ou CSR (*Certificate Signing Requests*).

12.24. Deve suportar a leitura e verificação de CRLs (*Certification Revogation Lists*).

12.25. Deve permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis de SSL.

12.26. Deve possuir mecanismos de checagem de conformidade do dispositivo remoto.

12.27. A checagem de conformidade deve permitir verificar, no mínimo, as seguintes informações no cliente remoto: sistema operacional e *patches* instalados, antivírus e versão instalada, *firewall* no *host*.

13. Qualidade de Serviço (QoS)

13.1. Deve permitir o controle de políticas de uso com base nas aplicações: permitir, negar, agendar, inspecionar e controlar o uso da largura de banda que utilizam cada aplicação ou usuário.

13.2. Deve suportar a criação de políticas de controle de uso de largura de bandas baseadas em: porta ou protocolo, endereço IP de origem ou destino, usuário ou grupo de usuários, aplicações (por exemplo, *Youtube* e *WhatsApp*).

13.3. Deve suportar a priorização em tempo real de protocolos de voz (VoIP) como H.323, SIP.

13.4. Deve suportar a marcação de pacotes *Dif Serv.*

13.5. Deve permitir o monitoramento do uso que as aplicações fazem por *bytes*, sessões e por usuário.

14. Balanceamento de *Links*

14.1. Deve suportar balanceamento de *link* por peso. Nesta opção deve ser possível definir o peso de tráfego que será escoado por cada um dos *links*. Deve suportar o balanceamento de, no mínimo, 4 (quatro) *links* WAN.

14.2. Deve permitir a configuração da funcionalidade de balanceamento em qualquer interface WAN, seja ela MPLS, Internet, 4G/LTE etc.

14.3. Deve possuir roteamento baseado em políticas e múltiplas saídas (e tipos de saídas) WANs.

14.4. Deve permitir a configuração de *failover* entre *links* principais e secundários. Estes limites podem ser configurados para forçar o *failover* caso apenas um ou todos os limites sejam atingidos simultaneamente.

14.5. Deve suportar a configuração de regras que permita o *failback* imediato.

14.6. Deve ser compatível com a solução de VPN, permitindo que suas características e análises sejam realizadas nas VPNs, assim como em *links* WAN.

14.7. Deve ser compatível com VPNs montadas em interfaces virtuais com roteamento dinâmico.

14.8. Deve realizar o gerenciamento de tráfego por tipo de aplicação.

14.9. Deve selecionar o melhor caminho baseado em tipo de tráfego e do *host* de origem.

14.10. Deve suportar o monitoramento de *link* com *ping* e TCP *echo*.

14.11. Deve suportar o monitoramento de *links* VPN (*interfaces virtuais*).

14.12. Deve permitir a exportação de informações via *netflow*.

15. Recursos de Segurança

15.1. Deve possuir, no mínimo, funcionalidades *Anti-Vírus, Anti-Bot, Anti-Malware, AntiSpyware*, Sistema de Prevenção de Intrusão (IPS), Filtro de Conteúdo *Web*, Controle de Aplicação, Prevenção de Perdas de Dados (DLP). E sistemas de prevenção de ameaças Zero Day.

15.2. Deve suportar o funcionamento nos modos *snifer* (para inspeção de tráfego gerado por uma porta de rede espelhada), *layer-2, layer-3,* de forma simultânea em uma única instância de *firewall*.

15.3. Deve aplicar novas políticas de segurança sem provocar indisponibilidade de serviço ou descontinuidade das conexões ativas.

15.4. Deve possuir capacidade de melhoria e análise das regras atuais, baseadas em camada 3 e 4 (porta/protocolo), indicando como a referida regra deverá ser configurada em camada 7 (aplicação).

15.5. O fluxo de análise de regras legadas deve permitir a visualização de quais aplicações estão em uso. Caso não possua essa funcionalidade, será permitida a integração com ferramentas que executam esta função.

15.6. Deve suportar as atualizações automáticas das bases de assinaturas utilizadas na identificação de vírus, intrusões (IPS) e aplicações sem a necessidade de intervenção manual pelo administrador, sem perda das conexões ativas e sem reinicialização do equipamento.

15.7. Deve suportar as atualizações automáticas das listas de geolocalização e das listas e categorias de URLs sem a necessidade de intervenção manual pelo administrador, sem perda das conexões ativas e sem reinicialização do equipamento.

15.8. Deve possuir proteção contra-ataques, no mínimo, dos tipos: IP *Spoofing*, Negação de Serviço (DoS e DDoS), SYN *Flood Attack*, ICMP *Flood Attack* e UDP *Flood Attack*, *Buffer Overflow, Port Scanning, Man-in-the-Middle.*

15.9. Deve identificar, decriptografar e analisar o tráfego SSL tanto em conexões de entrada (*inbound*) quanto de saída (*outbound*), com suporte a HTTP/2 e TLS 1.2 e 1.3.

15.10. Deve permitir a decriptografia da área útil do pacote de dados (*payload*) para fins de controle de acesso à Internet e proteção contra ameaças.

15.11. Deve permitir a diferenciação de conexões pessoais (bancos, *shopping* etc) e conexões não pessoais por meio de classificação automática.

15.12. Deve possuir funcionalidade de *backup* e *restore* da configuração e das políticas de segurança através do carregamento de arquivo de configuração previamente salvo.

15.13. Deve armazenar os *backups* localmente, ou na solução de gerenciamento centralizado, e permitir que sejam transferidos para equipamentos externos por meio dos protocolos FTP ou SCP.

15.14. Deve possuir a capacidade de identificar ataques de *Advanced Persistent Threat* (APT) ou Zero-Day

15.15. Deve possuir a capacidade de emular um ambiente operacional isolado e seguro (*Sandbox*), na nuvem do fabricante, para execução e observação de código malicioso, sem a utilização de assinaturas, com base na atividade, como, por exemplo, operações de arquivo, alterações de registro e sistema etc.

15.16. Deve suportar a análise nos seguintes sistemas operacionais: *Windows, Linux, MacOS e Android.*

15.17. Deve suportar a análise dos tipos de arquivos: documentos *Microsoft Office,* dll, exe, pdf, gzip, tar, zip.

15.18. Deve suportar a análise dos protocolos HTTP/HTTPS, FTP e SMTP.

15.19. Desejável que a análise de *links* em *sandbox* seja capaz de classificar sites falsos na categoria de *phishing* e atualizar a base de filtro de URL da solução.

15.20. Para ameaças trafegadas em protocolo SMTP e POP3, é desejável que a solução seja capaz de mostrar nos relatórios o remetente, destinatário e assunto dos e-*mails*, permitindo identificação ágil do usuário vítima do ataque.

15.21. Deve permitir visualizar os resultados das análises de *malwares* de dia zero nos diferentes sistemas operacionais suportados.

15.22. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso- negativo na análise de *malwares* de dia zero.

15.23. Deve atualizar a base com assinaturas para bloqueio dos *malwares* identificados em *sandbox* de maneira automática, com frequência de pelo menos 30 minutos.

15.24. Desejável permitir o envio para análise em *sandbox* de *malwares* bloqueados pelo antivírus.

15.25. Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-*mails* permitindo identificação ágil do usuário vítima do ataque.

15.26. O sistema de análise *"In Cloud"* 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).

15.27. Suportar a análise de arquivos do pacote *office* (.doc, .docx, .xls, .xlsx, .ppt, .pptx), arquivos *java* (.jar e class), *Android APKs MacOS* (*mach*-O, DMG e PKG), *Linux* (ELF), RAR e 7-ZIP no ambiente de *sandbox*.

15.28. A solução deve analisar os arquivos do tipo *malware* em ambiente *sandbox* para baremetal, a fim de evitar técnicas de evasão.

15.29. A solução deve possuir a capacidade de analisar em *sand-box os links (http e https*) presentes no corpo de e-mails trafegados em SMTP e POP3.

16. Filtro de Pacotes

16.1. Não deve possuir restrições ao número de máquinas ou usuários protegidos.

16.2. Deve informar o número de sessões simultâneas.

16.3. Deve suportar a implementação tanto em modo transparente *(layer-2)* quanto em modo *gateway (layer-3).*

16.4. Deve suportar *Statefull Packet Inspection* de tráfego IPv4 e IPv6.

16.5. Deve suportar controle de acesso para serviços e protocolos pré-definidos, bem como possibilitar a adição de novos serviços e protocolos.

16.6. Deve suportar os protocolos H.323, SIP.

16.7. Deve implementar mecanismo de proteção contra-ataques de falsificação de endereços IP (*anti-spoofing*).

16.8. Deve implementar mecanismo de captura de pacotes, de forma manual ou automática, quando uma ameaça for detectada.

16.9. Deve identificar os usuários para qualquer protocolo ou aplicação baseada em TCP, UDP e ICMP.

16.10. Deve suportar a utilização simultânea de políticas de segurança em IPv4 e IPv6.

16.11. Deve suportar a implementação de políticas de segurança baseadas em: portas, protocolos, usuários, grupos de usuários, endereços IP, redes CIDR/VLSM, horário ou período de tempo, e suas combinações.

16.12. Deve suportar a consulta a fontes externas de endereços IP, domínios e URL's podendo ser adicionados nas políticas de firewall para bloqueio ou permissão do tráfego.

16.13. Desejável possuir mecanismos de otimização de regras. De forma que com base na análise de tráfego o sistema automaticamente faça sugestões e melhorias nas regras existentes.

16.14. 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.

17. Filtro de Conteúdo

17.1. Deve prover o controle e proteção de acesso à Internet por meio do reconhecimento de aplicações, independente de porta e protocolo, e da classificação de URLs.

17.2. Deve ser capaz de identificar aplicações, independentemente das portas e protocolos, bem como das técnicas de evasão utilizadas.

17.3. Deve ser capaz de identificar se as aplicações estão utilizando sua porta padrão.

17.4. Deve ser capaz de identificar aplicações encapsuladas dentro de protocolos, como HTTP e HTTPS.

17.5. Deve ser capaz de identificar aplicações criptografadas usando SSL.

17.6. Deve ser capaz de identificar um mínimo de 1.400 (mil e quatrocentas) aplicações, incluindo, mas não se limitando a: *peer-to-peer*, *streaming* e *download* de áudio, *streaming* e *download* de vídeo, *update* de *software*, *instant messaging*, redes sociais, *proxies*, *anonymizers*, acesso e controle remoto, VOIP e *e-mail.*

17.7. Deve ser capaz de identificar, no mínimo, as seguintes aplicações: *Bittorrent, Youtube, Livestream, Skype, Viber, WhatsApp, Snapchat, Facebook, Facebook Messenger, Instagram, Twitter, Linkedin, Dropbox, Google Drive, One Drive, Logmein, Teamviewer, MS-RDP, VNC, Ultrasurf, TOR, Webex.*

17.8. Deve armazenar a base de assinaturas no próprio equipamento.

17.9. Deve classificar as aplicações em categorias.

17.10. Deve permitir o agrupamento de aplicações em grupos personalizados.

17.11. Deve identificar os usuários que estão utilizando as aplicações.

17.12. Deve permitir o bloqueio de aplicações que não estejam utilizando suas portas padrão.

17.13. Deve suportar a implementação de políticas de segurança baseadas em: aplicações, categorias de aplicações, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.

17.14. Deve proteger contra o roubo de credenciais, usuários e senhas identificadas através da integração com *Active Directory* submetidos em sites não corporativos. Deve ainda permitir criação de regra onde usuários do *Active Directory* só possam enviar informações de login para sites autorizados na solução.

17.15. Deve permitir a utilização ou bloqueio individualizado das aplicações, como *BitTorrent e Skype*, para determinados usuários ou grupos de usuários.

17.16. Deve permitir o registro de todos os fluxos autorizados/bloqueados das aplicações, incluindo o usuário identificado.

17.17. Deve permitir o controle de uso de banda de *download* ou *upload* utilizada pelas aplicações (*traffic shaping*) baseado em: endereço IP ou rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.

17.18. Deve ser capaz de efetuar a classificação de conteúdo de páginas *web* em HTTP e HTTPS, baseado em listas de categorias.

17.19. Deve possuir funcionalidades de tratamento de conteúdo *web*, devendo sua base de dados conter, no mínimo, 10 (dez) milhões de sites internet *web* já registrados e classificados, distribuídos em, no mínimo, 60 (sessenta) categorias ou subcategorias pré-definidas ou suas semelhantes: conteúdo adulto, chat, drogas ilegais, jogos de azar, jogos, pirataria, *proxy* remoto, redes sociais, *streaming* média, violência, pornografia, racismo, *malware*.

17.20. Deve permitir a inclusão de URLs customizadas por política (*whitelist*).

17.21. Deve armazenar as listas de categoria no próprio equipamento.

17.22. Deve identificar os usuários que estão acessando as páginas *web*.

17.23. Deve suportar a implementação de políticas de segurança baseadas em: URLs, categorias de URLs, endereço IP de origem ou destino, rede CIDR/VLSM de origem ou destino, usuário ou grupo de usuários, horário ou período de tempo, e suas combinações.

17.24. Deve alertar o usuário quando uma URL for bloqueada, por meio de página de bloqueio que possa ser customizada, e que informe, no mínimo, o motivo do bloqueio e a categoria na qual a URL foi classificada.

17.25. Deve permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado, informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão "Continuar" para possibilitar o usuário continuar acessando o site).

17.26. Deve permitir registrar todos os acessos autorizados ou bloqueados às páginas *web*, incluindo sua classificação e o usuário identificado.

17.27. Desejável permitir habilitar aplicações SaaS apenas no modo corporativo e bloqueá-las quando usadas no modo pessoal.

17.28. Desejável identificar o uso de táticas evasivas, ou seja, ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas.

17.29. Deve permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

17.30. Deve permitir bloquear o acesso a sites de busca (*Google, Bing, Yahoo*), caso a opção *Safe Search* esteja desabilitada.

17.31. Deve suportar base ou cache de URL’s local no *appliance*, evitando *delay* de comunicação/validação das URL’s.

17.32. Desejável que a categorização de URL’s analise a URL ao menos até o nível de diretório.

17.33. Deve prover análise em tempo real de páginas maliciosas e dessa forma permitir a proteção em tempo real antes mesmo da atualização das bases de dados de URLs. Caso o fabricante

não possua esta funcionalidade em sua plataforma será permitida a composição da solução, sem ônus a este órgão.

18. Prevenção de Intrusão (IPS)

18.1. Deve possuir tecnologia de detecção e prevenção de ataques e intrusões baseada em assinatura.

18.2. Deve possuir, no mínimo, um conjunto de 10.000 (dez mil) assinaturas de detecção e prevenção de ataques.

18.3. Deve detectar protocolos independentemente da porta utilizada, identificando aplicações conhecidas em portas não-padrão.

18.4. Deve possuir, no mínimo, os seguintes mecanismos de detecção e prevenção: assinaturas de vulnerabilidades e *exploits*, assinaturas de ataques, validação de protocolos, detecção de anomalias, IP defragmentation, remontagem de pacotes TCP, nível de severidade do ataque.

18.5. Deve ser capaz de inspecionar tráfego criptografado usando SSL.

18.6. Deve ser capaz de inspecionar integralmente todos os pacotes de dados, independentemente de seus tamanhos.

18.7. Deve identificar os usuários relacionados aos eventos de intrusão.

18.8. Deve identificar os usuários relacionados aos eventos de bloqueio.

18.9. Deve permitir a criação de políticas de segurança que alertem, sem bloquear, sobre a ocorrência de um determinado ataque ou ameaça.

18.10. Deve permitir a criação de políticas de segurança que bloqueiem uma determinada ameaça.

18.11. Deve permitir a criação de políticas de segurança que bloqueiem um determinado ataque por meio de uma ação de DROP/RESET.

18.12. Deve permitir registrar todos os eventos de IPS, incluindo o usuário identificado.

18.13. Deve identificar e bloquear a comunicação com *botnets*.

18.14. Deve bloquear *malwares* e *spywares*.

18.15. Deve inspecionar e bloquear vírus nos seguintes tipos de tráfego, no mínimo: HTTP, HTTPS, SMTP, POP3, FTP e SMB.

18.16. Deve suportar proteção contra vírus em conteúdo HTML e *javascrip*, *software* espião (*spyware*) e *worms*.

18.17. Deve suportar a inspeção de vírus em arquivos comprimidos utilizando o algoritmo *deflate* (zip, gzip etc).

18.18. Deve suportar bloqueio de *download* de pelo menos 45 tipos de arquivos.

18.19. Deve armazenar as bases de assinaturas no próprio equipamento.

18.20. Deve possuir a capacidade de detectar e prevenir contra ameaças em tráfego HTTP/2.

18.21. Console de Gerenciamento Centralizado

18.22. Deve ser fornecida em *appliance* virtual, compatível *VMware vSphere* ESXi 6.0 ou superior, ou baseado em *software*, compatível com *Windows Server* 2012 R2 ou superior, ou em *appliance* físico com suporte à fixação em bastidor (*rack*) padrão EIA- 310 com largura de 19’

(dezenove polegadas) e altura de até duas unidades de *rack* (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

18.23. Deve ser acessada via interface *web* ou através de um *software* cliente, com interface gráfica, instalado no *Windows* ou *Linux*.

18.24. Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.

18.25. Deve permitir o gerenciamento centralizado dos equipamentos de *firewall* sejam eles virtuais ou físicos em uma mesma console, permitindo os seguintes requisitos:

a) Coleta de *logs*;

b) Análise de *logs*;

c) Gerenciamento de *firewalls*;

d) Correlação de *logs*.

18.26. Deve estar licenciada e permitir a gerência centralizada de, no mínimo, 15 equipamentos.

18.27. Deve estar licenciada para o limite máximo de usuários, objetos, regras de segurança, NAT e endereços IP suportados pela solução.

18.28. As comunicações entre a CGC (*Centralized Gateways Controller*) e os *firewalls* e entre a CGC e as estações dos administradores do sistema devem ser criptografadas e autenticadas.

18.29. Deve possuir capacidade plena para executar todas as configurações necessárias nos *firewalls*, incluindo ajustes de políticas, regras, objetos de rede, interfaces, perfis de segurança e demais parâmetros operacionais.

18.30. Deve possibilitar a aplicação simultânea de configurações em todos os *firewalls* gerenciados pela solução.

18.31. Deve permitir a criação e distribuição de políticas de segurança de forma centralizada, suportando organização hierárquica de regras.

18.32. Deve suportar, por meio da interface gráfica de gerenciamento, a criação e administração de políticas de filtro de pacotes, prevenção de intrusão, controle de aplicação, filtragem de URLs, monitoração de *logs*, *debugging*, *troubleshooting* e captura de pacotes.

18.33. Deve ser capaz de gerenciar os *firewalls* em unidades remotas, fora da rede local.

18.34. Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou *Active Directory*.

18.35. Será permitido que a solução de gerenciamento centralizado possua um "*appliance* virtual" específico para atendimento às necessidades de identificação e autenticação de usuários.

18.36. Deve possuir a capacidade de definir administradores com diferentes perfis de acesso. Os perfis de acesso devem ser, no mínimo, de leitura/escrita e somente leitura,

18.37. Deve permitir a criação de perfis customizados.

18.38. Deve permitir, de forma granular, assinalar permissões para os administradores criarem outros usuários, alterar e ler configurações etc.

18.39. Deve permitir múltiplos administradores acessando o equipamento simultaneamente, sem restrição para leitura e escrita.

18.40. Deve suportar o bloqueio de alterações, evitando o conflito de configurações entre diferentes administradores efetuando alterações simultaneamente.

18.41. Deve registrar, em *log* de auditoria, as ações dos usuários administradores com o horário da alteração.

18.42. Deve suportar a identificação e utilização de usuários nas políticas de segurança.

18.43. Deve suportar agrupamento lógico de objetos ("*object grouping*") para criação de regras.

18.44. Deve possibilitar o gerenciamento (incluindo a criação, alteração, monitoração e exclusão) de objetos de rede. Deve ainda permitir detectar se e onde, na base de regras, está sendo utilizado determinado objeto de rede. Os tipos de objetos devem permitir especificar de forma distinta grupos e objetos de rede e serviços, diferenciando-os e agrupando-os conforme suas características ou descrição de maneira a permitir o reaproveitamento dos mesmos em diferentes políticas.

18.45. Deve possibilitar a especificação de política por tempo, ou seja, permitir a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora).

18.46. Deve garantir que quando houver novas versões de *software* dos equipamentos, seja realizada a distribuição e atualização remota, de maneira centralizada.

18.47. Deve ser capaz de testar a conectividade dos equipamentos gerenciados.

18.48. Deve suportar configuração das funcionalidades de alta disponibilidade dos dispositivos físicos.

18.49. Deve permitir localizar em quais regras um objeto está sendo utilizado.

18.50. Deve permitir a identificação e exclusão de regras e objetos que estão aplicadas nos dispositivos, mas não afetam o desempenho e a segurança da rede (regras e objetos em desuso sob o ponto de vista lógico).

18.51. Deve suportar a geração de alertas automáticos via SNMP e *syslog*.

18.52. Deve informar a utilização dos recursos de CPU, memória e atividade de rede dos equipamentos gerenciados.

18.53. Deve informar o número de conexões simultâneas dos equipamentos gerenciados.

18.54. O gerenciamento da solução deve suportar acesso via SSH, cliente, *WEB* (HTTPS) e API aberta.

18.55. As consoles de gerenciamento centralizado, gerenciamento de *logs*, relatoria centralizada, poderão ser entregues em um único *appliance*, desde que atenda a todas as exigências deste documento.

19. Console de Gerenciamento de *Logs*

19.1. Deve ser fornecida em *appliance* virtual, compatível *VMware vSphere* ESXi 6.0 ou superior, ou baseado em *software*, compatível com *Windows Server* 2012 R2 ou superior, ou em *appliance* físico com suporte à fixação em bastidor (*rack) padrãoEIA*- 310 com largura de 19’ (dezenove polegadas) e altura de até duas unidades de *rack* (2U), acompanhado de todos os acessórios necessários (cabos, suportes, gavetas, braços, trilhos etc).

19.2. Deve possuir relatórios de utilização dos recursos por aplicação, URLs, ameaças e etc.

19.3. Deve possuir visualização sumarizada de todas as aplicações, ameaças e URLs que foram identificadas e controladas pela solução.

19.4. Deve permitir a criação de relatórios customizados.

19.5. Deve ser capaz de receber *logs* de todos os *firewalls* especificados.

19.6. Deve possibilitar a filtragem dos *logs* do equipamento por, no mínimo: aplicação, endereço IP de origem e destino, país de origem e destino, usuário e horário.

19.7. Deve possibilitar o registro dos fluxos de dados relativos a cada sessão, armazenando: endereços IP de origem e destino dos pacotes, traduções NAT, portas e protocolos de origem e destino, usuário identificado, ação sobre o pacote (permitido ou negado).

19.8. Deve possuir relatórios com informações consolidadas sobre: as mais frequentes fontes de conexões bloqueadas com seus destinos e serviços; os mais frequentes ataques e ameaças de segurança detectados com suas origens e destinos; os serviços de rede mais utilizados, as aplicações maiores consumidoras de banda de Internet; os usuários maiores consumidores de banda de Internet; e os sítios na Internet mais visitados.

19.9. Deve possuir funcionalidade de exportação de relatórios e *logs* para o computador local ou via FTP, SFTP ou SCP.

19.10. Deve permitir a geração automática e agendada dos relatórios.

19.11. Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.

19.12. Deve estar licenciada e permitir a correlação de todos os eventos gerados por todos os equipamentos e contextos virtuais que compõem a solução.

19.13. O *appliance* virtual deve estar licenciado de maneira irrestrita quanto ao armazenamento, possibilitando armazenar o volume de *logs* que julgar necessário, utilizando recursos computacionais próprios.

19.14. Deve ser acessada via interface *web* ou através de um *software* cliente, com interface gráfica, instalado no *Windows* ou *Linux*.

19.15. Será permitida a entrega do “Console de Gerenciamento de *Logs*” como *software* agregado ao “Console de Gerenciamento Centralizado” ou ao “Console de Relatoria Centralizada”.

20. Console de Relatoria Centralizada

20.1. Deve ser fornecida em *appliance* virtual, compatível com *VMware vSphere ESXi* 6.5 ou superior, ou baseado em *software*, compatível com *Windows Server* 2012 R2 ou superior.

20.2. Deve ser acessada via interface web ou através de um *software* cliente, com interface gráfica, instalado no *Windows* ou no *Linux*.

20.3. Deve estar licenciada em caráter permanente/perpétuo para todas as funcionalidades e quantidades mencionadas.

20.4. Deve estar licenciada e permitir a gerência centralizada de relatórios, para no mínimo, 10 equipamentos.

20.5. As comunicações entre a Console de Relatoria e os *firewalls* e entre a Console de Relatoria e as estações dos administradores do sistema devem ser criptografadas e autenticadas.

20.6. Deve ser capaz de gerar relatórios de equipamentos em unidades remotas, fora da rede local.

20.7. Deve permitir a autenticação dos administradores através de contas locais e bases externas LDAP ou *Active Directory*.

20.8. A console deve suportar acesso via SSH, cliente e *WEB* (HTTPS).

20.9. Deve coletar *logs* dos *Firewalls*, do "Console de Gerenciamento Centralizado" e do "Console de Gerenciamento de *Logs*".

20.10. Deve garantir a geração de relatórios com mapas geográficos, ou modo tabela, gerados em tempo real, para a visualização de origens e destinos do tráfego.

20.11. Deve permitir a extração de relatórios.

20.12. Deve possuir relatórios pré-definidos.

20.13. Deve permitir a geração de relatórios de *logs* de tráfego de dados.

20.14. Deve permitir a geração de relatórios de *logs* para auditoria das configurações de regras, objetos e acessos.

20.15. Deve possibilitar o envio de maneira automática de relatórios por *e-mail.*

20.16. Deve permitir o agendamento da geração de relatórios.

20.17. Deve ter a capacidade de definir filtros nos relatórios.

20.18. Deve gerar alertas automáticos, via e-*mail*, *snmp* e *syslog* baseados em eventos de ocorrência como *log*, severidade de *log*, entre outros.

20.19. Deve permitir a criação de painéis (*dashboards*) customizados para visibilidades do tráfego de aplicativos, categorias de url, ameaças, serviços, países, origem e destino.

20.20. Deve possibilitar a visualização na interface gráfica de usuário (gui) da "console de relatoria centralizada as seguintes informações do sistema: *logs* diários recebidos, alertas gerados, entre outros.

20.21. Será permitida a entrega do "Console de Relatoria Centralizada" como *software* agregado ao "Console de Gerenciamento Centralizado" ou ao "Console de Gerenciamento de *Logs*".

21. Características Específicas da Solução de *Firewall* "Datacenter - Tipo 3"

21.1. *Throughput* de 40 Gbps com as funcionalidades de *firewall*, prevenção de intrusão, controle de aplicação, *anti-malware* e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.

21.2. Em relação ao filtro de pacotes, deve possuir o *Throughput* de no mínimo 60 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir.

21.3. Em relação ao túnel IPSec VPN, o *throughput* mínimo deverá ser de no mínimo 95 Gbps, com a inspeção e controle de aplicação e usuários ativada.

21.4. Deve permitir, no mínimo, 42.000.000 (quarenta e dois milhões) de conexões ou sessões simultâneas.

21.5. Deve permitir, no mínimo, 1.100.000 (um milhão e cem mil) novas conexões ou sessões por segundo.

21.6. Deve permitir, no mínimo, 4000 VLANs.

21.7. Deve suportar afixação em bastidor (*rack*) padrão EIA-310 com largura de 19’ (dezenove polegadas) e altura de até duas unidades de *rack* (2U), incluindo *kit* tipo trilho para adaptação se necessário e cabos de alimentação.

21.8. Deve possuir 2 (duas) fontes de alimentação independentes, redundantes e *hotswappable*.

21.9. Deve possuir, no mínimo, 12 (doze) interfaces de rede 10Gbps SFP+.

21.10. Deve possuir, no mínimo, 4 (quatro) interfaces de rede 10/25 Gbps para utilização de *transceivers* padrão SFP28.

21.11. Deve suportar a expansão, no mínimo, 2 (duas) interfaces 40/100 Gbps para utilização de *transceivers* padrão QSFP+/QSFP28.

21.12. O equipamento deverá dispor de 01 (uma) interface de rede dedicada exclusivamente ao gerenciamento.

21.13. Deverá conter 01 (uma) interface do tipo console ou equivalente, para acesso direto ao equipamento em situações de contingência ou inicialização.

21.14. Deverá incluir uma interface dedicada e física para gerenciamento fora de banda (*Out-of-Band Management – OOBM*), permitindo o acesso remoto mesmo em situações em que o equipamento esteja desligado ou não responsivo.

21.15. Caso o equipamento não possua nativamente tal interface, será permitida a utilização de *hardware* externo e específico (ex: módulo de gerenciamento *Lights-Out*), desde que atenda aos requisitos de operação independente.

21.16. Não serão aceitas soluções baseadas em instâncias ou configurações exclusivamente por *software*.

21.17. A solução deverá contar com mecanismo de dedicação de recursos de processamento exclusivamente para funções de gerenciamento, assegurando a disponibilidade de acesso administrativo mesmo em cenários de alta utilização da CPU. Entre as funcionalidades mínimas exigidas estão:

a) Acesso via SSH;
b) Interface de gerenciamento via *Web* (GUI);
c) Aplicação e modificação de políticas de segurança;
d) Comunicação e coleta de dados por meio de protocolo SNMP.

21.18. Deve possuir, disco *Solid State Drive* (SSD), no mínimo, 900 GB redundante.

21.19. Deve possuir, no mínimo, 75 sistemas virtuais lógicos (Contextos) no *firewall* Físico.

21.20. A capacidade de *throughput* e a quantidade e tipos de interfaces mencionadas devem ser comprovadas por meio de *datasheet* oficial e público do fabricante, disponível na internet.

21.21. Não serão aceitas declarações genéricas de performance ou capacidade sem respaldo em documentação oficial.

21.22. Alta Disponibilidade

21.22.1. Deve possibilitar a operação em alta disponibilidade (HA) no equipamento, permitindo uma arquitetura ativo/ativo e ativo/passivo com no mínimo 2 (dois) membros, com sincronismo de estados integrado.

21.22.2. Deve suportar o balanceamento de carga na arquitetura ativo/ativo.

21.22.3. Deve sincronizar sessões TCP/IP, tabelas NAT, tabelas FIB, associações de segurança das VPNs e todas as configurações necessárias para a manutenção da continuidade dos serviços.

21.22.4. Deve monitorar a falha dos *links* de comunicação.

21.22.5. Deve ser capaz de identificar e iniciar automaticamente um procedimento de *failover* sempre que ocorrer: a falha de um dos membros do *cluster*, a falha de qualquer componente ou processo crítico de um dos membros do *cluster*, a falha de um dos *links* de comunicação monitorados.

21.22.6. Deve ser capaz de realizar os procedimentos de *failover* sem perda das conexões ativas e sessões estabelecidas de forma transparente para o usuário.

21.22.7. Deve suportar a operação em cluster com no mínimo 2 equipamentos.

21.22.8. Desejável possuir 2 *fans* independentes, redundantes e *hotswappable*.

21.22.9. Deve possuir discos de sistema e de *logs* independentes e redundantes (RAID).

22. Características Específicas da Solução de *Firewall* "Datacenter - Tipo 2"

22.1. *Throughput* de 30 Gbps com as funcionalidades de *firewall*, prevenção de intrusão, controle de aplicação, *anti-malware* e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.

22.2. Em relação ao filtro de pacotes, deve possuir o *Throughput* de no mínimo 35 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir.

22.3. Em relação ao túnel IPSec VPN, o *throughput* mínimo deverá ser de no mínimo 65 *Gbps*, com a inspeção e controle de aplicação e usuários ativada.

22.4. Deve permitir, no mínimo, 18.000.000 (dezoito milhões) de conexões ou sessões simultâneas.

22.5. Deve permitir, no mínimo, 730.000 (setecentas e trinta mil) novas conexões ou sessões por segundo.

22.6. Deve permitir, no mínimo, 4000 VLANs.

22.7. Deve suportar afixação em bastidor (*rack*) padrão EIA-310 com largura de 19' (dezenove polegadas) e altura de até duas unidades de *rack* (2U), incluindo *kit* tipo trilho para adaptação se necessário e cabos de alimentação.

22.8. Deve possuir 2 (duas) fontes de alimentação independentes, redundantes e *hotswappable*.

22.9. Deve possuir, no mínimo, 08 (oito) interfaces de rede 10Gbps SFP+.

22.10. Deve possuir, no mínimo, 4 (quatro) interfaces de rede 10/25 Gbps para utilização de *transceivers* padrão SFP28.

22.11. Deve suportar a expansão, no mínimo, 2 (duas) interfaces 40/100 Gbps para utilização de *transceivers* padrão QSFP+/QSFP28.

22.12. O equipamento deverá dispor de 01 (uma) interface de rede dedicada exclusivamente ao gerenciamento.

22.13. Deverá conter 01 (uma) interface do tipo console ou equivalente, para acesso direto ao equipamento em situações de contingência ou inicialização.

22.14. Deverá incluir uma interface dedicada e física para gerenciamento fora de banda (*Out-of-Band Management – OOBM*), permitindo o acesso remoto mesmo em situações em que o equipamento esteja desligado ou não responsivo.

22.15. Caso o equipamento não possua nativamente tal interface, será permitida a utilização de *hardware* externo e específico (ex: módulo de gerenciamento *Lights-Out*), desde que atenda aos requisitos de operação independente.

22.16. Não serão aceitas soluções baseadas em instâncias ou configurações exclusivamente por *software*.

22.17. A solução deverá contar com mecanismo de dedicação de recursos de processamento exclusivamente para funções de gerenciamento, assegurando a disponibilidade de acesso administrativo mesmo em cenários de alta utilização da CPU. Entre as funcionalidades mínimas exigidas estão:

a) Acesso via SSH;
b) Interface de gerenciamento via *Web* (GUI);
c) Aplicação e modificação de políticas de segurança;
d) Comunicação e coleta de dados por meio de protocolo SNMP.

22.18. Deve possuir, disco *Solid State Drive* (SSD), no mínimo, 900 GB redundante.

22.19. Deve possuir, no mínimo, 50 sistemas virtuais lógicos (Contextos) no *firewall* Físico.

22.20. A capacidade de *throughput* e a quantidade e tipos de interfaces mencionadas devem ser comprovadas por meio de *datasheet* oficial e público do fabricante, disponível na internet.

22.21. Não serão aceitas declarações genéricas de performance ou capacidade sem respaldo em documentação oficial.

22.22. Alta Disponibilidade

22.22.1. Deve possibilitar a operação em alta disponibilidade (HA) no equipamento, permitindo uma arquitetura ativo/ativo e ativo/passivo com no mínimo 2 (dois) membros, com sincronismo de estados integrado.

22.22.2. Deve suportar o balanceamento de carga na arquitetura ativo/ativo.

22.22.3. Deve sincronizar sessões TCP/IP, tabelas NAT, tabelas FIB, associações de segurança das VPNs e todas as configurações necessárias para a manutenção da continuidade dos serviços.

22.22.4. Deve monitorar a falha dos *links* de comunicação.

22.22.5. Deve ser capaz de identificar e iniciar automaticamente um procedimento de *failover* sempre que ocorrer: a falha de um dos membros do *cluster*, a falha de qualquer

componente ou processo crítico de um dos membros do *cluster*, a falha de um dos *links* de comunicação monitorados.

22.22.6. Deve ser capaz de realizar os procedimentos de *failover* sem perda das conexões ativas e sessões estabelecidas de forma transparente para o usuário.

22.22.7. Deve suportar a operação em *cluster* com no mínimo 2 equipamentos.

22.22.8. Desejável possuir 2 *fans* independentes, redundantes e *hotswappable*.

22.22.9. Deve possuir discos de sistema e de *logs* independentes e redundantes (RAID).

23. Características Específicas da Solução de *Firewall* "Datacenter Tipo 1"

23.1. *Throughput* de 15 Gbps com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, *anti-malware* e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.

23.2. Suporte a, no mínimo, 14.000.000 (quatorze milhões) de conexões ou sessões simultâneas;

23.3. Suporte a, no mínimo, 520.000 (quinhentos e vinte mil) novas conexões ou sessões por segundo;

23.4. Armazenamento de, no mínimo, 900GB SSD;

23.5. Possuir, no mínimo, 4 (quatro) interfaces de rede 1Gbps UTP;

23.6. Possuir, no mínimo, 10 (dez) interfaces de rede 10 Gbps SFP+;

23.7. Capacidade para suportar, pelo menos, 20 contextos virtuais;

23.8. Possuir fonte de alimentação redundante;

23.9. Possuir 1 (uma) interface de rede dedicada ao gerenciamento;

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

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

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

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

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

24. Características Específicas da Solução de *Firewall* "Tipo Perímetro Interno"

24.1. *Throughput* de 08 Gbps com as funcionalidades de firewall, prevenção de intrusão, controle de aplicação, *anti-malware* e prevenção de ameaças avançadas (dia zero) habilitados simultaneamente. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito.

24.2. Suporte a, no mínimo, 7.000.000 (sete milhões) de conexões ou sessões simultâneas;

24.3. Suporte a, no mínimo, 290.000 (duzentas e noventa mil) novas conexões ou sessões por segundo;

24.4. Armazenamento de, no mínimo, 400GB SSD;

24.5. Possuir, no mínimo, 8 (oito) interfaces de rede 1Gbps UTP;

24.6. Possuir, no mínimo, 6 (seis) interfaces de rede 10 Gbps SFP+;

24.7. Capacidade para suportar, pelo menos, 12 contextos virtuais;

24.8. Possuir fonte de alimentação redundante;

24.9. Possuir 1 (uma) interface de rede dedicada ao gerenciamento;

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

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

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

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

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

25. Características Específicas da Solução de *Firewall* "Tipo *Cloud*"

25.1. O licenciamento da solução deverá ser baseado no número de cores virtuais (vCPUs) alocados, permitindo dimensionamento conforme a capacidade computacional de até 14 core.

25.2. A solução deverá ser compatível, no mínimo, com os seguintes *hypervisores* de mercado:

a) *VMware* ESXi;

b) *Microsoft* Hyper-V;

c) KVM (*Kernel-based* Virtual *Machine*).

25.3. Em relação ao filtro de pacotes, deve possuir o *Throughput* de no mínimo 60 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir.

25.4. A solução deverá possibilitar expansão modular por meio da aquisição de novas licenças, permitindo a criação e gerenciamento de *pools* de *gateways* virtuais, com escalabilidade horizontal;

25.5. A solução virtualizada deverá oferecer integração nativa com plataformas de redes definidas por *software* (SDN), suportando ao menos as seguintes tecnologias: *VMware* NSX e *VMware* ESXi.

25.6. A solução deve ser composta por appliance dedicado à proteção de rede, com funcionalidades de *firewall* de próxima geração (NGFW), integrando segurança avançada e controle de tráfego.

25.7. As funcionalidades da plataforma de segurança podem operar em múltiplas instâncias, desde que todos os requisitos desta especificação técnica sejam integralmente atendidos.

25.8. A solução deve possuir mecanismo para identificação do volume de conexões trafegadas por regra de *firewall*, permitindo análise de uso e priorização com base em tráfego real.

25.9. Deve suportar os seguintes tipos de NAT (*Network Address Translation*):

a) NAT Dinâmico (*Many-to-One*);
b) NAT Estático (*One-to-One*);
c) Tradução de Porta (PAT);
d) NAT de Origem;
e) NAT de Destino;
f) Suporte simultâneo a NAT de Origem e NAT de Destino.

25.10. Implementar suporte a *Network Prefix Translation* (NPTv6) ou NAT66, garantindo integridade de roteamento IPv6 e prevenindo assimetria de roteamento.

25.11. Suporte a NAT64 e NAT46, permitindo interoperabilidade entre redes IPv4 e IPv6.

25.12. Os dispositivos de proteção de rede devem oferecer, no mínimo, as seguintes funcionalidades:

a) 1024 VLAN *Tags* (IEEE 802.1Q);
b) Agregação de *links* (IEEE 802.3ad / LACP);
c) *Policy-Based Routing* (PBR) ou *Policy-Based Forwarding* (PBF);
d) Roteamento *multicast* com PIM-SM (*Protocol Independent Multicast - Sparse Mode*);
e) Serviços de DHCP *Relay* e DHCP *Server*;
f) *Jumbo Frames*.

25.13. Capacidade de enviar *logs* simultaneamente para múltiplos sistemas externos de monitoramento.

25.14. Prover mecanismo de proteção contra *spoofing* de endereços IP, por meio da vinculação de tráfego à interface de rede de origem, com base na topologia, não sendo aceita a utilização exclusiva de tabelas de roteamento para este fim.

25.15. Para IPv4, deve suportar roteamento estático e dinâmico com os seguintes protocolos: RIPv2, OSPFv2 e BGP.

25.16. O *firewall* deve suportar operações simultâneas em múltiplos modos de interface, em uma única instância:

a) Modo Transparente;
b) Modo *Sniffer* (monitoramento/análise de tráfego);
c) Modo Camada 2 (L2 *Bridge*);
d) Modo Camada 3 (L3 *Routing*).

25.17. Suporte a OSPF *Graceful Restart*, assegurando continuidade durante falhas ou reinicializações de processos de roteamento.

25.18. Suporte à autenticação integrada via *Kerberos*, para ambientes com *Active Directory*.

25.19. Cada regra de *firewall* deve operar simultaneamente para endereçamento IPv4 e IPv6, sem duplicação da base de objetos ou regras.

25.20. Não serão aceitas soluções que exijam a duplicação das interfaces de origem e destino para aplicação de regras ou políticas.

25.21. Deverá ter as seguintes funcionalidades de:

25.21.1. Controle de Aplicações *Web* e URL:

a) Ferramenta nativa para controle e visibilidade de aplicações *web* e URLs, com suporte à criação de políticas baseadas em usuários, grupos, IPs e redes.
b) Suporte à descriptografia de tráfego TLS 1.2, permitindo inspeção profunda mesmo em conexões HTTPS.
c) Detecção e controle de aplicações independentemente de portas ou protocolos, com reconhecimento de no mínimo 3.000 aplicações (ex: redes sociais, P2P, VoIP, e-*mail*, streaming, *proxies*, etc)
d) Criação de políticas com base em assinaturas, heurística ou decodificação de protocolo.
e) Possibilidade de criação de assinaturas customizadas para aplicações internas, sem necessidade de intervenção do fabricante.
f) Atualização automática das assinaturas de aplicação.
g) Capacidade de categorização e recategorização de URLs localmente ou via fabricante.
h) Suporte à definição de limites de banda (*download/upload*) por aplicação, IP, grupo ou usuário (LDAP/AD).
i) Controle por agendamento (ativação/desativação de políticas em horários predefinidos).
j) Integração com *Microsoft Active Directory* sem necessidade de agentes, utilizando múltiplos métodos de identificação.
k) Compatibilidade com soluções de terceiros, desde que todos os requisitos técnicos sejam atendidos.

25.21.2. Filtro de Conteúdo *Web* (*URL Filtering*):

a) Criação de políticas baseadas em categorias de URLs e horários específicos (data, hora, dia da semana).
b) Controle granular por usuário, grupo, IP ou rede.
c) Bloqueio de sites impróprios com verificação de buscas em mecanismos como *Google, Bing e Yahoo,* mesmo com *"Safe Search"* desabilitado.
d) Suporte à base local de cache de URLs (ou *appliance* externo não open-source, se necessário).
e) Permitir categorias de URLs personalizadas e personalização da página de bloqueio.
f) Opção de interação com o usuário via *pop-up* ou página de confirmação, conforme políticas de segurança da organização.

25.21.3. Autenticação e Identificação:
a) Suporte a *Captive* Portal nativo, sem necessidade de cliente nas estações, exigindo autenticação antes do acesso à internet.
b) Recebimento de eventos de autenticação de controladoras *wireless*, 802.1x e NAC via RADIUS, para correlação de IPs e usuários.

25.21.4. Prevenção de Vazamento de Dados (DLP):
a) Reconhecimento nativo de tipos de arquivos e dados sensíveis, incluindo: Números de cartão de crédito (PCI), Arquivos PDF, executáveis, planilhas, apresentações, documentos e bancos de dados.
b) Definição de direção do tráfego na política de inspeção (*upload*, *download* ou ambos).
c) Notificação ao usuário via redirecionamento ou mensagem ao detectar arquivos em violação de políticas.
d) Inspeção e prevenção de vazamento mesmo em tráfego HTTPS.

25.22. Deverá ter as seguintes funcionalidades de prevenção de ameaças:

25.22.1. A solução de segurança deve incluir nativamente, no firewall, módulos integrados de:
a) Prevenção contra Intrusão (IPS);
b) Antivírus;
c) *Anti-Malware*.

25.22.2. Capacidades e Funcionalidades mínimas:
a) Detecção de, no mínimo, 7.000 assinaturas de ataques pré-definidos.
b) Sincronização automática dos módulos (IPS, Antivírus, *Anti-Malware*) em ambientes de alta disponibilidade ativo/ativo e ativo/passivo.
c) Mecanismo de *fail-open* baseado em *software*, configurável por *thresholds* de CPU e memória, para evitar indisponibilidade em caso de sobrecarga.
d) Políticas granulares para antivírus e *anti-malware*, permitindo segmentação por IP de origem/destino, serviços e suas combinações.

25.22.3. Funcionalidades do IPS:
a) Análise de:

- Estado de conexões;
- Decodificação e anomalias de protocolo;
- Remontagem de pacotes TCP;
- Pacotes malformados.

b) Detecção e bloqueio de *portscans*.

c) Bloqueio de ataques conhecidos com possibilidade de adição de assinaturas personalizadas, inclusive em formato *SNORT*.

d) Assinaturas específicas contra *buffer overflow*.

e) Inspeção e bloqueio de *malware* nos protocolos HTTP, HTTPS e SMTP.

f) Bloqueio por tipo de arquivo e comunicação com *botnets*.

g) Referência cruzada com base de CVE (*Common Vulnerabilities and Exposures*).

25.22.4. Monitoramento e Visibilidade:

a) Registro detalhado no console centralizado, incluindo:

- Nome da ameaça e assinatura;
- Aplicação;
- Usuário;
- IP de origem/destino;
- Ação aplicada;
- País de origem da ameaça.

b) Suporte à captura de pacotes (PCAP) para eventos IPS e *Anti-Malware*.

c) Suporte à inspeção de arquivos comprimidos (ZIP, GZIP, etc.).

d) Capacidade de detecção e prevenção de ameaças desconhecidas.

e) Criação de políticas baseadas em Geo Localização, com bloqueio de tráfego por país.

f) Visualização em tempo real dos países de origem e destino nos registros de *log*.

g) Detecção e bloqueio de atividades *callback* de *malware*.

25.23. Deverá ter as seguintes funcionalidades de controle de qualidade de serviço:

25.23.1. A solução de segurança deve suportar a criação de políticas de QoS personalizadas, com base nos seguintes critérios:

- Endereço de origem;
- Endereço de destino;
- Portas e serviços.

25.23.2. As políticas de QoS devem permitir a definição de classes de tráfego com os seguintes parâmetros:

- Banda garantida (mínima);
- Banda máxima (limitadora);
- Fila de prioridade.

25.23.3. A solução deve disponibilizar estatísticas em tempo real *(Real-Time*) sobre o consumo e desempenho de cada classe de QoS definida.

25.24. Deverá ter as seguintes funcionalidades de VPN:

25.24.1. A solução de segurança deve atender aos seguintes requisitos para conectividade VPN:

a) Suporte a conexões VPN nos modos *Site-to-Site e Client-to-Site*.

b) Compatibilidade com IPSec VPN e SSL VPN.

c) A VPN IPSec deve oferecer suporte aos seguintes recursos e algoritmos criptográficos:

- 3DES, AES-128 e AES-256;
- SHA-1 e Autenticação HMAC;
- *Diffie-Hellman* grupos 1, 2, 5 e 14;
- Protocolo de negociação IKE (*Internet Key Exchange*);
- Autenticação baseada em certificados IKE (PKI).

d) Suporte a Autoridades Certificadoras (CA) internas e externas (de terceiros).

e) Permitir a configuração e gerenciamento de túneis VPN por meio de interface gráfica (GUI), seja via console do fabricante ou interface *web*, de forma intuitiva e segura.

25.25. Deverá ter as seguintes funcionalidades de proteção contra ameaças avançadas:

25.25.1. A solução deve incluir mecanismos avançados de inspeção, análise e bloqueio de *malwares* desconhecidos e ataques do tipo APT (Ameaças Persistentes Avançadas), com os seguintes requisitos mínimos:

a) Inspeção em tempo real de artefatos suspeitos utilizando ambiente de *sandboxing* proprietário (na nuvem do fabricante ou appliance dedicado).

b) Bloqueio efetivo de *malwares* zero-*day*, oriundos de tráfego *web* (HTTP/HTTPS) e e-mails (SMTP/TLS), sem entrega parcial do conteúdo durante a análise.

c) Inspeção de tráfego criptografado SSL, com capacidade de identificar e bloquear ameaças ocultas.

d) Suporte à emulação de ataques em diferentes ambientes operacionais: *Windows* 7, 8.1 e 10, e versões do *Microsoft Office* 2003, 2010, 2013 e 2016.

e) Atualizações da base de ameaças de forma automática e agendável (diária, semanal ou mensal).

f) Compatibilidade com diferentes topologias de implantação: *Inline*, MTA *(Message Transfer Agent*) e *Mirror*/TAP.

g) Emulação baseada em máquinas virtuais completas, com diferentes SOs e sem dependência exclusiva de assinaturas.

h) A funcionalidade de *sandboxing* deve operar independentemente de *engines* antivírus, podendo ser ativada de forma autônoma.

i) As máquinas virtuais devem estar completamente instaladas, licenciadas e atualizadas pelo fabricante, sem intervenção manual do administrador.

j) Suporte à emulação de arquivos com até 30 MB.

k) Capacidade de criação de exceções por VLAN, sub-rede e IP.

l) Detecção e bloqueio de *malwares* desconhecidos nos seguintes tipos de arquivos: pdf, docx, xlsx, pptx, zip, rar, exe, rtf, entre outros formatos de documentos e pacotes *Office*.

m) Criação de *whitelists* por *hash* MD5.

n) Disponibilizar recursos de monitoramento administrativo, incluindo:

- Quantidade de arquivos em emulação e emulados;
- Estatísticas por período: último dia, última semana e últimos 30 dias com dados de:
- Arquivos escaneados;
- Arquivos identificados como maliciosos.

26. Características Específicas da Solução de "Proteção de *E-mail*"

26.1. A solução deve possuir mecanismos de proteção multi-camadas contra as ameaças em serviços de *e-mail* em nuvem (SaaS):

a) Prevenção de ameaças avançadas (APT) ou dia zero (zero *day*).

b) Proteção contra *phishing*.

c) Possibilidade de identificar *e-mails* de *spam*.

d) Análise e detecção de vazamento de dados (DLP).

e) Gerar visibilidade de aplicações SaaS não autorizadas *(Shadow IT*).

f) Integração nativa com aplicações SaaS: *Google Workspace*.

g) Arquitetura unificada para visibilidade de logs e gerenciamento de políticas.

h) Limpeza e extração contra conteúdo malicioso em anexos (CDR).

26.2. Fazer integração via API da ferramenta de segurança para aplicações SaaS.

26.3. Durante integração deve fazer query na base de dados de usuários sem a necessidade de agentes para ter visibilidade dos usuários e grupos.

26.4. Durante a integração inicial com o *Microsoft 365*, deve ser possível determinar qual grupo ou usuários farão parte das políticas de segurança para inspeção dos *e-mails* e outras aplicações SaaS.

26.5. A solução de prevenção de ameaças avançadas, deve possuir funcionalidades de *sandboxing*, antivírus, reputação de URL e *anti-phishing*;

26.6. Nas configurações de políticas de segurança, deve possuir as opções de detectar e prevenir.

26.7. Deve identificar os grupos ou usuários que serão inspecionados e ter uma lista de exclusão baseado na conta do *Microsoft 365.*

26.8. Criação de alertas para administradores da ferramenta para qualquer *malware* identificado, assim como *phishing*. Tornando também opcional o alerta do usuário de destino sobre possíveis *malwares*.

26.9. A solução de *sandboxing*, deve ser na nuvem do próprio fabricante, sendo ela proprietária.

26.10. A funcionalidade de análise de ameaças avançadas e de dia zero deve implantar mecanismo de *sandboxing* resistente a evasões.

26.11. Na solução de prevenção de ameaças avançadas, deve apresentar nos *logs* as seguintes informações:

a) Todas as funcionalidades de segurança que identificaram a ameaça.

b) Nome do arquivo identificado.

c) Deve informar o MD5, SHA-1 e SHA-256 para fazer pesquisas e comparar com outras fontes de terceiro. Ex.: Vírus Total.

d) Dentro do *log*, deve possuir *link* onde é possível em um *click* direcionar a pesquisa do arquivo ou URL direto no vírus total.

e) Quando detectado e bloqueado algum arquivo ou URL maliciosa, deve permitir que o administrador consulte através da plataforma externa do "Vírus total" (*www.virustotal.com*) se alguma *engine* de *Antivirus* baseada em assinatura é capaz de identificar o ataque apontado pela ferramenta de prevenção de ameaças.

f) Identificar o usuário que recebeu o e-*mail* malicioso.

26.12. Cada *log* de *sandboxing*, quando identificada uma ameaça, deve apresentar informações detalhadas do arquivo malicioso para análise:

a) Tamanho do arquivo.

b) Tipo do arquivo.

c) Lista de *hash* que o arquivo *possu*.

d) Veredito do ataque.

e) Risco de segurança.

f) Nível de confiança.

g) Classificação do ataque, ou seja, se é uma família já conhecida. Ex.: *Trojan*.

h) Apresentar no próprio relatório o *malware* identificado, evidências do ataque já no *Framework* do *MITRE ATT&CK*, classificando as devidas táticas e técnicas do ataque.

i) Lista dos arquivos encontrados dentro o *malware* identificado. Ex.: Pode ser um arquivo ZIP com outros arquivos ou executáveis que possuem outros arquivos associados a ele.

j) Atividades suspeitas no computador do *Sandboxing* que vai simular a ação humana como: eventos no *file system*, chave de registro, eventos de rede apresentando possíveis URL's ou IP's.

k) Vídeo da máquina virtual dentro da solução de *Sandboxing*, apresentando o comportamento humano.

26.13. A solução, deve possuir *engine* onde no momento que encontrado um conteúdo malicioso no arquivo *office* ou PDF, a mesma deve reconstruir o arquivo removendo o conteúdo malicioso, sendo capaz de converter arquivos reconstruídos para o formato PDF para melhor segurança, ou manter-se em formato original de acordo com política estabelecida.

26.14. Deve possuir console de gerenciamento web na nuvem, sem a necessidade de infraestrutura específica e já incluída nos custos de licenciamento da solução.

26.15. Deve inspecionar todos os arquivos em tempo real nos serviços SaaS de *e-mail*, verificando a presença de *malwares* ou dados sensíveis.

26.16. Deve inspecionar todos os arquivos previamente existentes com no mínimo de 7 dias retroativos à data inicial da integração dos serviços SaaS de *e-mail*, verificando a presença de *malwares*;

26.17. Toda integração deve ser feita através de API, sem a necessidade de integração com nenhuma solução de *proxy* local ou agentes.

26.18. Deve possuir integração nativa com a nuvem de inteligência de ameaças (*Threat Intelligence)* do fabricante para prevenção de ameaças e checagem de reputação.

26.19. Identificar nos *e-mails phishing* e apresentar os seguintes parâmetros nos eventos:

a) Remetente.
b) Destinatário.
c) Destinatários copiados.
d) Título do *e-mail*.
e) Tipo de conteúdo, exemplo HTML.
f) Data e horário do recebimento do *e-mail*.
g) Alias do usuário.
h) Quando identificado um *phishing*, deve apresentar informações como:
    - Indicadores da detecção como *phishing.*
    - Análise do ataque.
    - Reputação de quem enviou.
    - Nível de confiança para determinar se é alto ou não.
    - Informações que são identificadas no cabeçalho do *e-mail* como falta do DMARC e assinatura DKIM.

26.20. Caso tenha alguma URL no corpo do *e-mail* que foi caracterizada como *phishing*, a mesma deve ser apresentada nos *logs*.

26.21. A solução deverá realizar análise dos *links* enviados no corpo do *e-mail*. Essa análise deverá apresentar o motivo do "porquê" foi caracterizado como suspeito ou malicioso.

26.22. A solução deve apresentar uma visualização prévia da URL suspeita.

26.23. O administrador deve ter a opção de solicitar na ferramenta a reclassificação referente a um evento de prevenção de ameaças que não corresponde ao *log* apresentado.

26.24. Deverá prover mecanismo de proteção para *links*, onde a solução deverá validar a URL antes de redirecionar para o usuário.

26.25. Pesquisar no log do evento de *phishing*, outros e-mails baseados no ataque recebido que possuam os mesmos critérios como quem enviou, título de *e-mail* e outros tópicos.

26.26. A solução deverá apresentar quais os indicadores que a Inteligência Artificial identificou e caracterizou o evento.

26.27. Solução de DLP, deve criar regras granulares baseada em escopo de *e-mail* e deve permitir selecionar os tipos de dados que serão usados na política.

26.28. Deve permitir a criação de tipo de dado customizado baseado em expressão regular, *template*, dicionário de palavras e outros.

26.29. O mecanismo de DLP deverá ter capacidade de detectar informações sensíveis entre todas as plataformas SaaS integradas, com pelo menos as soluções *Microsoft* 365 e *Google Workspace.*

26.30. Relatório sumarizado contendo todas as funcionalidades de segurança.

26.31. Listar a quantidade de objetos escaneados e a quantidade de ameaças identificadas.

26.32. Possuir mecanismo de quarentena onde o administrador consegue visualizar todos os *e-mails* que foram identificados como maliciosos.

26.33. Permitir a restauração do e-mail em quarentena através da ferramenta.

26.34. Deverá permitir que o usuário solicite a liberação de um *e-mail* em quarentena.

26.35. Visibilidade dos eventos através de usuários que estão integrados na ferramenta de forma automática.

26.36. Deve ser possível selecionar o usuário e identificar todos os eventos de segurança baseado por período e funcionalidade de segurança.

26.37. Visibilidade correlacionada de todos os eventos de segurança.

26.38. Deve inspecionar todos os arquivos previamente existentes nos serviços SaaS após a integração inicial, seja em *e-mail* ou compartilhamento de arquivos, verificando a presença de *malwares* ou dados sensíveis.

26.39. Deve identificar tentativas de acesso anômalas aos serviços SaaS, tal como o acesso simultâneo com uma mesma credencial a partir de localizações geograficamente distantes.

26.40. Gerenciamento e Visibilidade:

26.40.1. Deve possuir uma *dashboard* que permita ao administrador de segurança ter visibilidade consolidada das ameaças identificadas nos diferentes serviços SaaS, incluindo eventos de *malware*, URLs maliciosas, *phishing*, *Shadow* IT e DLP.

26.40.2. Deve prover uma interface para visualização detalhada dos eventos maliciosos identificados nos serviços SaaS.

26.40.3. A solução deverá ser capaz de oferecer integração com ferramentas de XDR.

26.40.4. Deve ser possível especificar o serviço SaaS afetado, o vetor de entrega da ameaça e o detalhamento das ações de mitigação adotadas.

26.40.5. A gerência centralizada deve permitir visibilidade sumarizada de todas as atividades maliciosas identificadas pela solução de diferentes funcionalidades suportadas pela ferramenta como: *Malwares*, *Phishing*, DLP, *Shadow* IT e anomalias. Sendo possível fazer *drill-drow* e navegar nos *logs* para análise das atividades suspeitas.

26.40.6. Deve possuir gráficos e filtros que permitam ao administrador identificar rapidamente as ameaças identificadas nos serviços SaaS.

26.40.7. A gerência centralizada deve permitir visualizar a quantidade de usuários que estão ativos na solução de e-mail, assim como a quantidade de *e-mails* e arquivos inspecionados.

26.40.8. Deve possuir relatórios analíticos com as estatísticas dos serviços SaaS utilizados, incluindo quantidade de usuários do serviço, volume de e-*mails*, volume de arquivos e os respectivos eventos maliciosos por funcionalidade de proteção.

26.40.9. A solução deve fornecer relatórios de atividades para cada aplicação SaaS (*Google Workspace*).

26.40.10. Deve dispor de sumário total de risco identificados, entre eles:

a) DLP.

b) Malware.

c) *Phishing*.

d) Anomalia.
e) *Malwares* suspeitos.
f) *Phishing* suspeitos.
g) Spam.
h) Shadow IT.

26.40.11. Deve permitir a configuração de políticas independentes para cada serviço SaaS.

26.40.12. Deve permitir múltiplas regras de segurança para cada serviço SaaS, aplicando proteções diferenciadas baseados em usuários ou grupos de usuários.

26.40.13. Quando identificado um evento na solução Prevenção de ameaças, o administrador deve ter as seguintes opções de ação baseado em cada *log*:
a) Alertar o usuário sobre a ameaça.
b) Liberar o arquivo inspecionado e bloqueado.
c) Reportar para o fabricante que não é um arquivo malicioso.
d) Desconsiderar evento.
e) Analisar o relatório do incidente.

26.40.14. As regras devem permitir a geração de alertas por *email* para os administradores para os casos de *malware, phishing* e DLP, bem como a customização das mensagens de alerta.

26.40.15. Quando identificado um evento de *phising*, o administrador deve ter as seguintes opções de ação:
a) Categorizar como SPAM.
b) Alertar usuários que é um *phishing*.
c) Quarentenar *e-mail.*
d) Criar exceção.

26.40.16. Quando identificado um evento de Anomalia, o administrador deve ter as seguintes opções de ação:
a) Desconsiderar evento.
b) Adicionar exceção a partir do evento.

26.40.17. Quando identificado um evento na solução de *ShadowIT*, o administrador deve ter as seguintes opções:
a) Aprovar aplicação.
b) Desconsiderar evento.

26.40.18. A solução deve possuir painel de Quarentena baseado nas aplicações SaaS, *Google Workspace*, permitindo o administrador ter acesso aos itens que foram colocados em quarentena.

26.40.19. A quarentena deve permitir que o administrador possa tomar ação para as requisições de restauração do e-*mail Google Workspace.*