PODER JUDICIÁRIO
TRIBUNAL REGIONAL FEDERAL DA 6ª REGIÃO
Subsecretaria de Infraestrutura

ESTUDO TÉCNICO PRELIMINAR - ETP (LEI 14.133/2021) 0990939

CONTRATAÇÃO DE SERVIÇOS E/OU AQUISIÇÃO DE BENS PERMANENTES E DE CONSUMO

Introdução

ETP foi elaborado conforme:

- a ordem dos elementos indicados no § 1º Art. 18 Lei 14.133/2021 (Nova Lei de Licitações e Contratos);

- o guia de suporte ao preenchimento de ETP 0366701, com orientações sobre conceitos, elaboração de textos e referências normativas.

Observação: conforme § 2º Art. 18 Lei 14.133/2021, ETP deverá conter ao menos os itens**I, IV, VI, VIII e XIII** e, quando não contemplar os demais, deverão ser incluídas as devidas justificativas.

I - Descrição da necessidade da contratação, considerado o problema a ser resolvido sob a perspectiva do interesse público

A atual infraestrutura de TIC que atende ao TRF6 foi preparada para o funcionamento de uma Seccional, razão pela qual o recebimento de sistemas anteriormente centralizados no TRF1 como o PJe, o SEI, Acordo 58, SIREA, eSiest, bancos de dados, entre outros, representou um consumo de recursos não previstos quando das aquisições, conforme cenário de escassez reportado por meio dos autos 0000724-85.2022.4.06.8000.

Diante do crescimento dos sistemas do TRF6, inúmeras aplicações anteriormente hospedadas no TRF1 passaram a ser publicadas na internet, o que representou o estabelecimento de um tráfego de conexões não dimensionado para a SJMG. Assim, a atual solução de segurança se mostrou insuficiente face à demanda cada vez maior de acessos, incluindo as vias automatizadas por robôs.

Destaca-se que as appliances de firewall Check Point 13500 alcançaram o chamado fim de utilização em junho de 2022 (vide relato do fabricante), o que obrigou a migração das operações para um modelo Open Server no ano de 2022, conforme Segundo Termo Aditivo ao Contrato n. 0035/2020 do TRF1 (Documento SEI TRF1 16656397).

Uma solução de segurança possui uma garantia recomendada de 04 anos com posterior substituição após a vigência, nos termos da Resolução CJF nº 477/2018, em razão da obsolescência técnica dos equipamentos. Por tal razão e considerando que os firewalls do TRF6 possuem mais de 8 anos de uso, além de não atenderem à atual demanda técnico-operacional, torna-se necessária a substituição dos equipamentos para adequação às necessidades de funcionamento do TRF6.

Outro ponto a se destacar é a dificuldade de tratamento dos acessos aos sistemas, em razão da indisponibilidade de WAF. Assim, os sistemas do TRF6 dependem de configurações individualizadas para o controle dos acessos automatizados frequentemente realizados por meio de robôs e bots, alguns dos quais de caracteres maliciosos.

Há, ainda, um elemento essencial à infraestrutura: a disponibilidade. Todos os sistemas do TRF6 devem estar disponíveis para funcionamento em regime de 24 x 7 (vinte e quatro horas, sete dias por semana), o que pode acarretar em situações de falhas em horários sem acompanhamento por equipe especializada e, consequentemente, em atraso para o início do atendimento. Considerando que os sistemas e serviços de TI do TRF6 sustentam a área finalística da instituição, torna-se cada vez mais importante que estejam hospedados em ambiente de infraestrutura tecnológica protegida e que garanta a disponibilidade e integridade das informações.

A contratação visa a adquirir uma solução de segurança de alta complexidade diante da necessidade de implantação aderente à LGDP, em substituição ao atual sistema obsoleto de proteção de perímetro de rede com a inclusão de novas funcionalidades de proteção de rede que compõem a plataforma de segurança de nova geração. A nova solução incluirá recursos de reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões, sistemas de detecção de invasão e sistemas de prevenção de intrusão, aplicações antimalware, inspeção de pacotes SSL/TLS, já que o tráfego é frequentemente criptografado para evitar a detecção e bloqueio de ameaças. Também permitirá o combate à falsificação de tráfego de acesso, o que dificulta a identificação e o bloqueio com base em assinaturas ou padrões específicos em razão do caráter aparentemente legítimo, ao parque tecnológico do TRF6.

Por tudo exposto, busca-se com a presente contratação:

a) Atualizar o parque tecnológico do TRF6;

b) Obter serviços de alta disponibilidade;

c) Aumentar a velocidade de operação entre os equipamentos;

d) Otimizar o desempenho da rede de dados;

e) Garantir a estabilidade operacional das comunicações do TRF6 e suas subseções judiciárias;

f) Aumentar a proteção de rede do TRF6, possibilitando a inspeção de tráfego com maior granularidade que a atualmente realizada;

g) Melhorar o desempenho e eficácia no controle de acesso ao perímetro de rede através de equipamentos com níveis de processamento e capacidade mais adequados;

h) Aumentar a disponibilidade das aplicações, evitando o comprometimento da capacidade do firewall em eventuais situações de ataque;

i) Possuir viabilidade para realizar futuras expansões da capacidade e granularidade da rede do Tribunal;

j) Possibilitar a ampliação da segmentação da rede com o objetivo de reduzir os riscos de segurança;

k) Aumento da resiliência em caso de ataques;

l) Diminuir o tempo de análise e resolução de problemas.

II - Demonstração da previsão da contratação no plano de contratações anual, sempre que elaborado, de modo a indicar o seu alinhamento com o planejamento da Administração

- Resolução CNJ nº 370, de 28 de janeiro de 2021 - Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
- Resolução CJF nº 685, de 15 de dezembro de 2020 - Plano Estratégico de Tecnologia da Informação da Justiça Federal;
- Portaria PRESI 125/2023 - Plano Estratégico Regional da Justiça Federal da 6ª Região para o ciclo 2023-2026.

Macrodesafio: Fortalecimento da Estratégia Nacional de TIC e de Proteção de Dados

Objetivos Estratégicos da Justiça Federal:

1) Aperfeiçoar e assegurar a efetividade dos serviços de TI para a Justiça Federal

Indicadores	Metas
1 - Índice de satisfação dos clientes internos com os serviços de TI.	1 - Atingir, até 2025, 85% de satisfação dos clientes internos de TI.
2 - Índice de satisfação dos clientes externos com os serviços de TI.	2 - Atingir, até 2026, 80% de satisfação dos clientes externos de TI.

III - Requisitos da contratação

Definição dos requisitos (Art. 18, § 1º, III, da Lei n. 14.133/2021)

1. Requisitos de Negócio

1.1. Assegurar a efetividade dos serviços de TI para o TRF6, através da continuidade dos serviços de segurança de dados e aplicações e de proteção contra ameaças;

1.2. Assegurar a proteção dos dados dos sistemas e dos usuários do TRF6 de acordo com a Política de Segurança da Informação do CJF, aplicável em razão da falta de norma própria.

2. Requisitos de Garantia

2.1. A garantia da solução deve permitir reparar eventuais falhas e substituir peças com defeito por outras de configuração idêntica ou superior;

2.2. A garantia da solução deve permitir a atualização dos produtos licenciados assim que novas versões e releases dos softwares que fizerem parte da solução contratada estiverem disponíveis.

3. Requisitos Técnicos

3.1. Os serviços de suporte deverão ser capazes de atender às demandas de compatibilidade da solução de segurança com a infraestrutura computacional existente no TRF6.

3.2. As especificações dos itens

4. Requisitos de Suporte

4.1. Será prestado serviço de suporte técnico durante toda a vigência do contrato, com direito a atualizações de versões da solução que incorporem correções de defeitos e melhorias implementadas pelos fabricantes.

5. Requisitos de Manutenção

5.1. A solução proposta deverá possuir garantia do fabricante de 05 anos para entrega de peças on-site;

5.2. Atendimento 24x7 nas dependências do TRF6;

5.3. Substituir componentes e peças defeituosos ou com falhas, trocas periódicas das peças internas, discos e demais componentes que apresentarem problemas técnicos durante a vigência do contrato, utilizando de produtos originais, novos e de primeiro uso, garantidos pelo fabricante;

5.4. Prestar os serviços dentro dos parâmetros e rotinas estabelecidos no processo de contratação, com observância às recomendações aceitas pela boa técnica, normas e legislação, bem como observar conduta adequada na utilização dos materiais, equipamentos, ferramentas e utensílios;

5.5. Possibilitar o suporte técnico e especializado, remoto ou presencial, entre o CONTRATANTE e o fabricante sem novos ônus ou custos contratuais;

5.6. Executar todas as atividades de instalação, atualização, configuração e migração de acordo com o planejamento aprovado pela área técnica;

5.7. Realizar manutenção corretiva, que compreende providências para reparar e corrigir os componentes da solução contratada em seu pleno estado de funcionamento, removendo definitivamente os defeitos eventualmente apresentados;

5.8. Garantir o funcionamento do ambiente com relação à solução instalada pela CONTRATADA, incluindo todos os serviços necessários para manutenção da disponibilidade da solução, inclusive de configurações e fornecimento de “firmwares”, “fixes” e “releases”, durante toda a vigência do contrato;

5.9. Os serviços serão solicitados mediante a abertura de um chamado efetuado por técnicos da contratante, via chamada telefônica local, a cobrar ou 0800, e-mail, website ou chat do fabricante ou à empresa autorizada (em português – para o horário comercial – horário oficial de Brasília) e constatada a necessidade, o fornecedor deverá providenciar o deslocamento do equipamento, bem como seu retorno ao local de origem sem qualquer ônus ao contratante.

6. Requisitos de Instalação

6.1. A realização dos serviços deve ser planejada de acordo com disponibilidade de ambas as partes. O planejamento anterior ao serviço deverá ser realizado de forma on-site nas dependências da CONTRATANTE;

6.2. O planejamento dos serviços de instalação deve resultar num documento tipo SOW (em tradução livre, escopo de trabalho). Neste documento devem conter a relação, descrição e quantidades dos produtos fornecidos, descrição da infraestrutura atual e desejada, detalhamento dos serviços que serão executados, premissas do projeto, locais e horários de execução dos serviços, condições de execução dos serviços, pontos de contato da CONTRATADA e CONTRATANTE, cronograma de execução do projeto em etapas, com responsáveis e data e início e fim (se aplicável), relação da documentação a ser entregue ao final da execução dos serviços, responsabilidade da CONTRATADA, plano de gerenciamento de mudanças, itens excluídos no projeto e termo de aceite. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes;

6.3. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, devendo a CONTRATADA sugerir as configurações de acordo com normas técnicas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas;

6.4. Após a instalação, a solução deverá ser monitorada on-site nas dependências da CONTRATANTE pelo prazo mínimo de 8 (oito) horas corridas, observando as condições de funcionamento e performance dos equipamentos, sendo possível o troubleshooting em caso de problemas ou não conformidades na operação;

6.5. Ao final da instalação, deverá ser realizado o repasse de configurações hands-on, de forma on-site nas dependências da CONTRATANTE apresentando as configurações realizadas. A CONTRATANTE disponibilizará o local adequado para a transferência do conhecimento e acesso a solução em produção;

6.6. Os serviços deverão ser realizados por pessoal técnico experiente e certificado pelo fabricante da solução. Em momento anterior à instalação, a CONTRATANTE poderá solicitar os comprovantes da qualificação profissional do(s) técnico(s) que executará(ão) os serviços, sendo direito da mesma a sua aceitação ou exigência de troca de profissional no caso de este não satisfazer às condições supramencionadas;

6.7. Ao término dos serviços deve ser criado um relatório detalhado contendo todos os itens configurados no projeto (relatório as-built), etapas de execução e toda informação pertinente para posterior continuidade e manutenção da solução instalada, como usuários e endereços de acesso,

configurações realizadas e o resumo das configurações dos equipamentos. Este relatório deve ser enviado com todas as informações em até 15 dias após a finalização dos serviços;

6.8. Nos valores cotados devem estar inclusas todas as despesas com deslocamento, alimentação e estadia para realização dos serviços (onsite) nos locais de presença da CONTRATANTE. Os funcionários da CONTRATADA deverão possuir todo o ferramental necessário ao exercício das suas atividades;

6.9. A CONTRATADA deverá garantir a confidencialidade das informações, dados e senhas compartilhadas da CONTRATANTE;

6.10. A execução dos serviços ocorrerá na sede da CONTRATANTE;

6.11. Durante as atividades realizadas na prestação do serviço, o técnico da CONTRATADA deverá demonstrar à equipe técnica de acompanhamento da CONTRATANTE como instalar e configurar os equipamentos e os softwares fornecidos (instalação assistida);

6.12. As atividades deverão ser realizadas dentro do horário comercial.

7. Requisitos de Conformidade

7.1. Deverá fazer parte do catálogo de produtos comercializados pelo fabricante e não ter sido descontinuado;

7.2. Deverá ser novo, sem uso, e constar no site do fabricante (documento oficial e público) como em linha de produção;

7.3. Deverá permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, durante a vigência CONTRATADA, irrestrita e sem necessidade de licenciamentos ou ônus adicionais.

8. Requisitos Temporais

8.1. Apresentar plano de implantação contendo os requisitos de instalação e cronograma de entrega, instalação, configuração e disponibilização da solução, em até 30 (trinta) dias corridos da assinatura do contrato;

8.2. Entregar os produtos no prazo máximo de até 90 (noventa) dias corridos, a contar da assinatura do contrato;

8.3. A entrega deverá ser formalizada mediante comunicação escrita da CONTRATADA ao CONTRATANTE;

8.4. Executar a conferência dos produtos especificados, conjuntamente com representantes da CONTRATADA, para emissão do Termo de Recebimento Provisório;

8.5. Antes de findar o prazo fixado a empresa CONTRATADA poderá formalizar, de forma devidamente fundamentada, pedido de sua prorrogação, cujas razões expostas serão examinadas pela administração do CONTRATANTE, que decidirá pela prorrogação do prazo ou aplicação das penalidades previstas;

8.6. A CONTRATADA receberá cópia do “Termo de Recebimento Provisório” após a entrega e conferência dos produtos em até 5 (cinco) dias úteis da confirmação de entrega, contados do primeiro dia imediatamente posterior à confirmação de entrega dos itens no CONTRATANTE, desde que não haja pendências de responsabilidade da CONTRATADA;

8.7. Concluir, no prazo de 30 (trinta) dias corridos, a contar da emissão do termo de recebimento provisório, a implantação e configuração dos produtos, em plena compatibilidade com o ambiente computacional do CONTRATANTE e em conformidade com a proposta técnica apresentada, cumprindo ainda todas as demais cláusulas de garantia e atendimento técnico constantes do contrato, nos prazos e termos ali estipulados;

8.8. A CONTRATADA receberá cópia do “Termo de Recebimento Definitivo”, que deverá ser providenciado pelo CONTRATANTE no prazo máximo de 10 (dez) dias úteis, após manifestação da CONTRATADA de conclusão dos serviços e comprovação de atendimento de todas as fases, desde que a CONTRATADA atenda a todas as solicitações e que não haja pendências de sua responsabilidade;

8.9. Os serviços de suporte e garantia deverão estar disponíveis para atendimento durante os 07 (sete) dias corridos da semana, 24 (vinte e quatro) horas por dia;

8.10. Considerar o horário das 07 horas às 20 horas como de horário normal de expediente, para os dias úteis.

9. Requisitos de Sustentabilidade Ambiental

9.1. A CONTRATADA será responsabilizada por qualquer prejuízo que venha causar ao TRF6 por ter suas atividades suspensas, paralisadas ou proibidas por falta de cumprimento de normas ligadas ao software e ainda aos serviços elencados no presente Termo de Referência;

9.2. A CONTRATADA deverá comprovar que os produtos ofertados atendem aos critérios de segurança, compatibilidade eletromagnética e eficiência energética, previstos no art. 3º, inciso II, do Decreto n. 7.174, de 12 de maio de 2010, regulamentado pela Portaria INMETRO n. 170, de 10 de abril de 2012;

9.3. Só será admitida a oferta de bens de informática e/ou automação que não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr (VI)), cádmio (Cd), bifenil polibromados (PBBs), éteres difenil-polibromados (PBDEs), conforme o art. 5º, inciso IV, da IN MPOG 01, de 19 de janeiro de 2010;

9.4. As comprovações dos dois itens anteriores, quando exigidas pela CONTRATANTE, poderá ser feita mediante apresentação de certificação emitida por instituição pública oficial ou instituição credenciada, ou por qualquer outro meio de prova, em especial laudo pericial, que ateste que os bens fornecidos cumprem com as exigências do edital, conforme art. 42, inciso III, da Lei 14.133, de 1º de abril de 2021;

9.5. A CONTRATADA deverá, para a execução do contrato, fornecer aos empregados os equipamentos de segurança que se fizerem necessários, para a execução de serviços, conforme disposto no art. 6°, inciso IV, da Instrução Normativa SLTI/MPOG n. 01, de 19 de janeiro de 2010;

9.6. A CONTRATADA deverá se atentar às normas em vigor atinentes à sustentabilidade expressas na 2ª edição do Manual de Sustentabilidade de compras e contratos do Conselho da Justiça Federal, instituído pela Portaria CJF n. 96, de 10 de fevereiro de 2023;

9.7. A CONTRATADA deverá respeitar a legislação vigente e as normas técnicas, elaboradas pela ABNT e pelo INMETRO para aferição e garantia de aplicação dos requisitos mínimos de qualidade e acessibilidade do software e ainda dos serviços elencados no Termo de Referência.

10. Requisitos Legais e Normativos Aplicáveis ao Objeto da Contratação

10.1. Política de Segurança da Informação do CJF - Resolução CJF 006/2008;

10.2. Lei n. 14.133, de 1º de abril de 2021;

10.3. Resolução CNJ 468, de 15 de julho de 2022.

IV - Estimativas das quantidades para a contratação, acompanhadas das memórias de cálculo e dos documentos que lhes dão economia de escala

A pesquisa de preços estimados para a elaboração do DOD 0751599, realizada a partir de preços públicos, levantou os valores abaixo detall

- Cenário 1 (equipamentos e licenciamentos):

Itens	Descrições	
01	Solução em alta disponibilidade (appliance) FW	
02	Licenciamentos Anuais FW	
03	Solução em alta disponibilidade (appliance) WAF Controle	
04	Licenciamentos Anuais WAF Controle	
05	Solução em alta disponibilidade (appliance) WAF Balanceador	
06	Licenciamentos Anuais WAF Balanceador	
09	Instalação	
10	Suporte	
11	Treinamento	
TOTAIS (R$) **		

- Cenário 2 (equipamentos, licenciamentos e serviços continuados):

Itens	Descrições	
01	Solução em alta disponibilidade (appliance) FW	
02	Licenciamentos Anuais FW	
07	SaaS Proteção (serviço continuado)	
08	Franquia Adicional	
09	Instalação	
10	Suporte	
11	Treinamento	
TOTAIS (R$) **		

** Valores estimados com base em contratações públicas similares, portanto ainda sem a adequação conforme as volumetrias do TRF6.

Atualmente, a solução de segurança de dados do TRF6 é composta pelo seguinte cenário:

1. Contrato nº 0035/2020 - TRF1 (3º termo aditivo -SEI TRF1 - 19188174)

1.1. Licenciamento Open Server Check Point R81.20 Jumbo:

1.1.1. Vigência até 05/11/2024;

1.1.2. Incluído suporte sob demanda às operações;

1.1.2. Valor anual: R$ 423.769,50.

2. Contrato nº 016/2023 (0298363):

2.1. Licenciamento de Antivírus ESET Protect Enterprise:

2.1.1. Vigência até 25/09/2028;

2.1.2. Incluído suporte sob demanda às operações;

2.1.2. Valor anual (suporte): R$ 6.000,00.

Considerando que a atual solução de segurança é precária, obsoleta e que não atende às necessidades de segurança e prote de dados que ofereça um melhor serviço de continuidade e integridade das operações e que minimize as exposições contra ameaças.

V - Levantamento de mercado, que consiste na análise das alternativas possíveis, e justificativa técnica e econômica da esco

Com base em opções disponíveis no mercado, foram levantadas as diferentes soluções de TIC que podem atender às necessidades do TRF6

5.1. Solução nº 1 - Utilização de Softwares Livres

5.1.1. No universo de softwares livres, existem diversas soluções. Ocorre que todo uso de software livre demanda esforços técnico

5.1.2. Cumpre registrar que o quadro de servidores da SECTI é reduzido e a demanda de serviços gerada pelos sistemas do TRF6 que já vinha defasado de mão de obra especializada.

5.1.3. É inegável que uma prestação de serviços eficiente está condicionada à existência de um contingente de pessoal capacitad de pessoal além de contribuir para que o serviço prestado seja ineficiente e moroso, faz com que haja acúmulo e sobrecarga de tr reforçar que os servidores da Secretaria de Tecnologia da Informação cumprem sua missão institucional com inegável zelo e esfor equipe tem trabalhado no decorrer dos sete dias da semana.

5.1.4. Pelo exposto e considerando que o TRF6 não conta com profissionais especializados e em quantidades necessárias para a não atende à necessidade.

5.2. Solução nº 2 - Utilizar a atual solução de segurança

5.2.1. Não é possível seguir com a atual solução de segurança, uma vez que depende de licenciamento vinculado a contrato do TR

5.2.2. A solução de Next Generation Firewall atual foi virtualizada em razão da descontinuidade do modelo de appliance Che 25/09/2024);

5.2.3. A atual solução não possui tratamento de aplicações e balanceamento de carga, o que impede a utilização dinâmica das con

5.2.4. Não há disponibilidade, ainda, de solução de gerenciamento de acessos, o que impede o controle rigoroso das operações rea

5.3. Solução nº 3 - Adquirir nova solução de segurança

5.3.1. De forma a viabilizar o atendimento às necessidades e de acordo com as tecnologias disponíveis no mercado, a nova soluçã

5.3.1.1. Solução de alta disponibilidade de Next Generation Firewall - NGFW, incluindo os respectivos licenciamentos e os serv

5.3.1.2. Solução de alta disponibilidade de Web Application Firewall - Appliance Virtual, incluindo os respectivos licenciamento

5.3.1.3. Solução de Serviço de Segurança de Borda (*Security Service Edge* - SSE), incluindo os respectivos licenciamentos e os

5.3.2. A equipe de planejamento realizou um comparativo entre os principais requisitos com base em dados disponibilizados no líderes de mercado.

5.3.2.1. A análise de contratações públicas similares permitiu identificar os modelos de produtos e serviços incompatíveis com

OBJETO	ÓRGÃO	FONTES	
SaaS Proteção	TRF3	0751373 0751375	Serviço não realiza a inspeção do tráfego
WAF Appliance	TRE-PI	0751378	Solução a ser adquirida em coparticipação 51.2024.4.06.8000.
WAF Appliance	Banco do Nordeste	0751429	Solução a ser adquirida em coparticipação 51.2024.4.06.8000.
WAF Appliance	TCE-MT	0751463	Solução a ser adquirida em coparticipação 51.2024.4.06.8000.
WAF Appliance	STJ	0751506	Solução a ser adquirida em coparticipação 51.2024.4.06.8000.
NGFW	UFF	0751530	Solução inferior tecnicamente às necessid
WAF Appliance	CAPES	0751540	Solução a ser adquirida em coparticipação 51.2024.4.06.8000.
SaaS Proteção	TCE-RR	0751548	Serviço não realiza a inspeção do tráfego
WAF Appliance Virtual	CIPP - Gov-CE	0751562	Solução inferior tecnicamente às necessid
ZTNA	UDESC	0837652	Solução inferior tecnicamente às necessid
ZTNA	MAP	0837723	Solução inferior tecnicamente às necessid

5.4. Análise e comparação entre as soluções de TIC avaliadas:

Requisito
A Solução encontra-se implantada outro órgão ou entidade Administração Pública Federal?
A Solução encontra-se implantada em outro órgão ou entidade da Justiça Federal?
A Solução está disponível no Portal do Software Público Brasileiro?
A Solução é um software livre ou software público?
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, e-MA
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do Modelo de Requisi Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário – MoReq-Jus?

5.5. Justificativa da solução de TIC escolhida, considerando o ciclo de vida do objeto.

5.5.1. A solução que melhor atende às necessidades do TRF6 é a solução nº 03,pelos seguintes fundamentos:

5.5.1.1. A solução de segurança proposta se encontra de acordo com as recomendações do Manual de Referência de Segura autorizados;

5.5.1.2. Permite a operação em alta disponibilidade;

5.5.1.3. Representa um relevante incremento da velocidade de operação entre os equipamentos e sistemas;

5.5.1.4. Otimiza o desempenho das aplicações;

5.5.1.5. Incrementa a proteção de rede do TRF6, possibilitando a inspeção de tráfego com maior granularidade que a atual;

5.5.1.6. Permite o controle de acesso ao perímetro de rede através de equipamentos com níveis de processamento e capacid

5.5.1.7. Aumenta a disponibilidade das aplicações, evitando o comprometimento da capacidade do firewall em eventuais situ

5.5.1.8. Viabiliza futuras expansões da capacidade e granularidade da rede do Tribunal;

5.5.1.9. Possibilita a ampliação da segmentação da rede com o objetivo de reduzir os riscos de segurança;

5.5.1.10. Aumenta consideravelmente a resiliência em caso de ataques;

5.5.1.11. Diminui consideravelmente o tempo de análise e resolução de problemas.

5.5.2. O ambiente do TRF6 atual conta apenas com uma solução de firewall com licenciamento renovado anualmente e em ope
13500.

5.5.2.1. A equipe técnica conta com apoio de suporte mantido por contrato celebrado pelo TRF1 e recentemente assumido
contratação seja concluída;

5.5.2.2. A falta da solução de WAF impede o controle e balanceamento das aplicações, o que demanda a necessidade de bloq

5.5.2.3. A falta de uma solução de SSE obriga a utilização de solução de acesso*open source* VPN sem quaisquer controle
segurança para a rede interna e aplicações do TRF6.

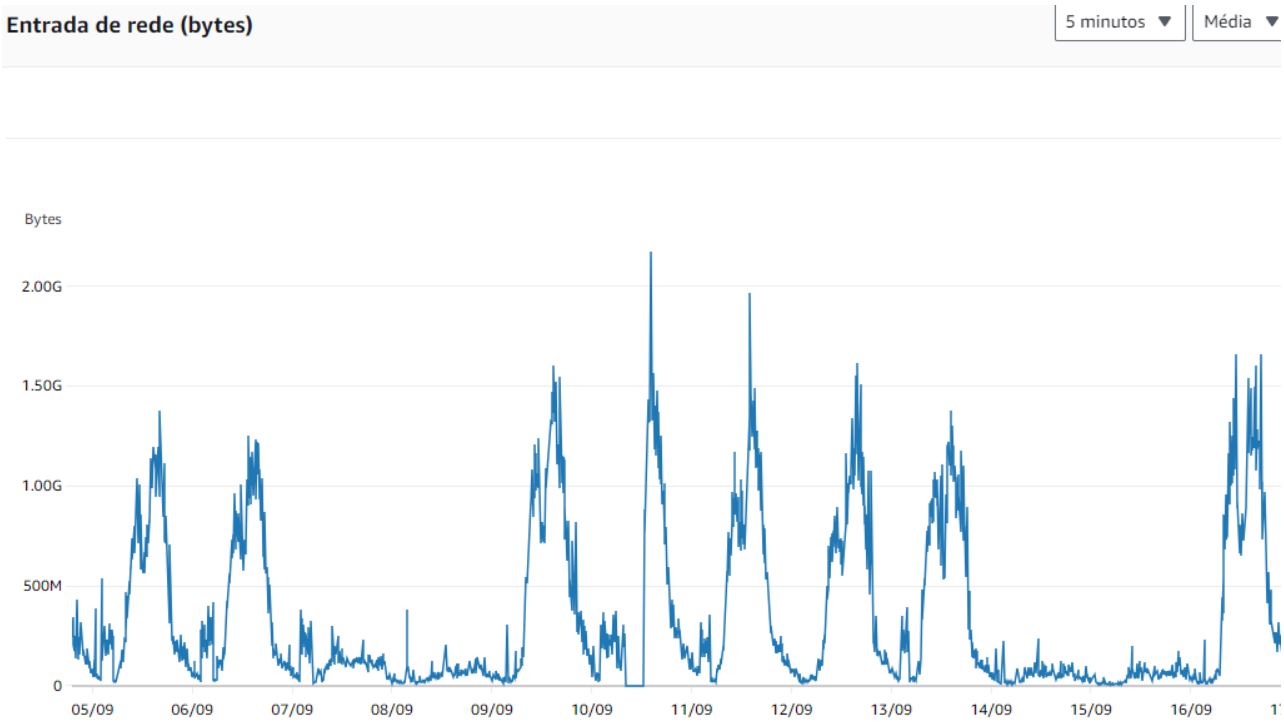
5.5.3. A previsão de contratação de soluções de WAF providas por meio de appliance virtual possibilita ao TRF6 a operação híbrida

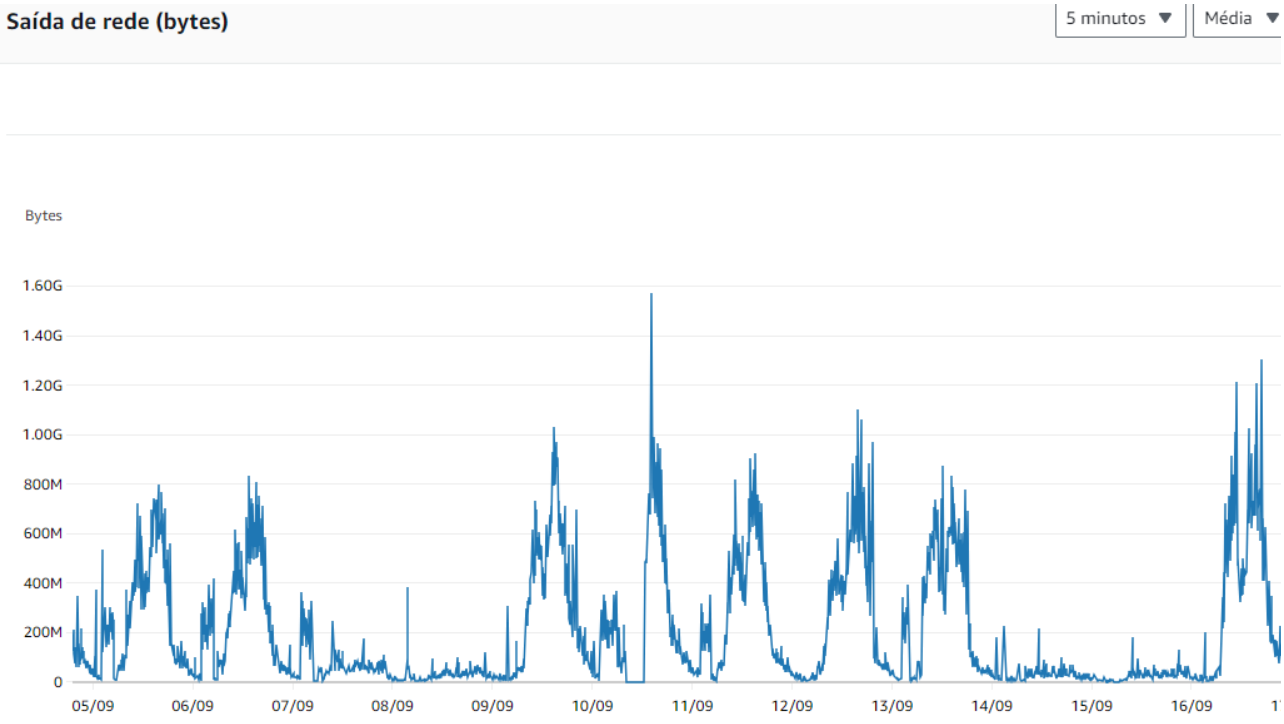
5.5.3.1. Em razão da coparticipação em contratação conduzida pelo CJF (0788920), a aquisição da solução de WAF e respecti
51.2024.4.06.8000.

5.5.4. A presente aquisição de solução de segurança incluiu as ferramentas de Serviço de Segurança de Borda (*Security Service Ed*

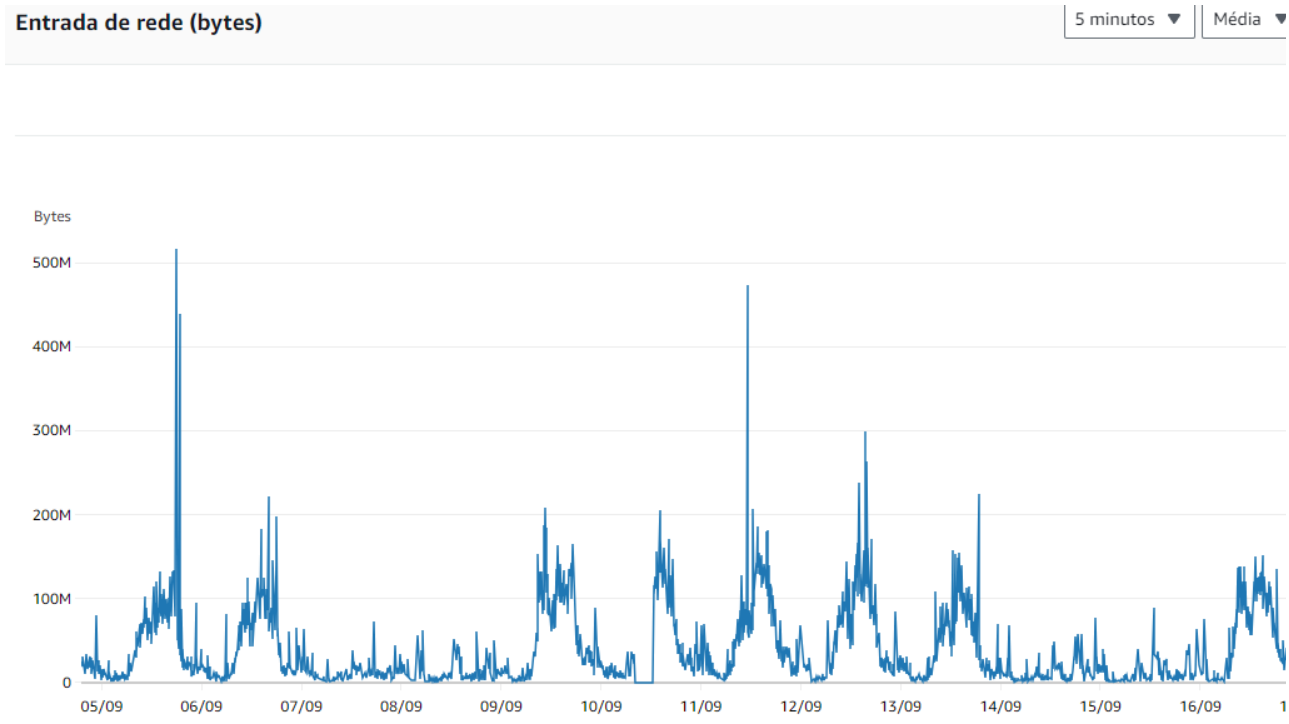
5.5.5. O dimensionamento das soluções foi realizado com base nos indicadores de tráfego e número de acessos simultâneos e tota

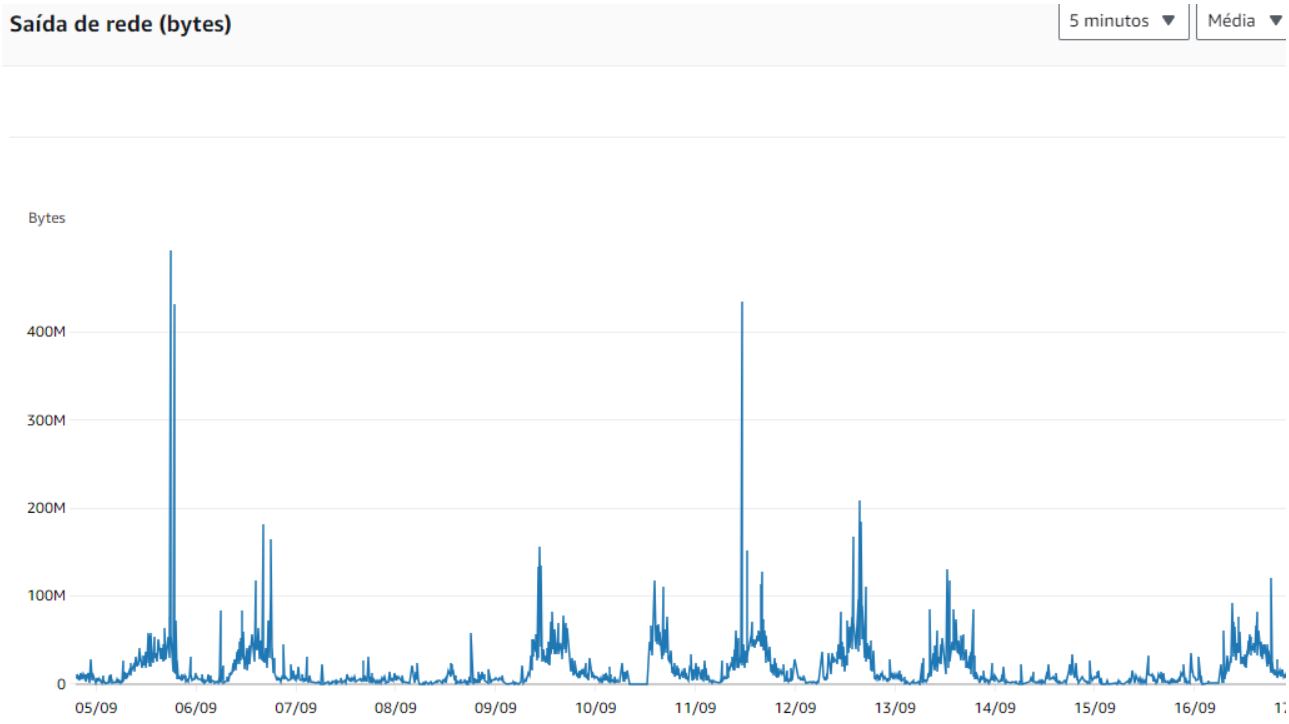
eproc 1G



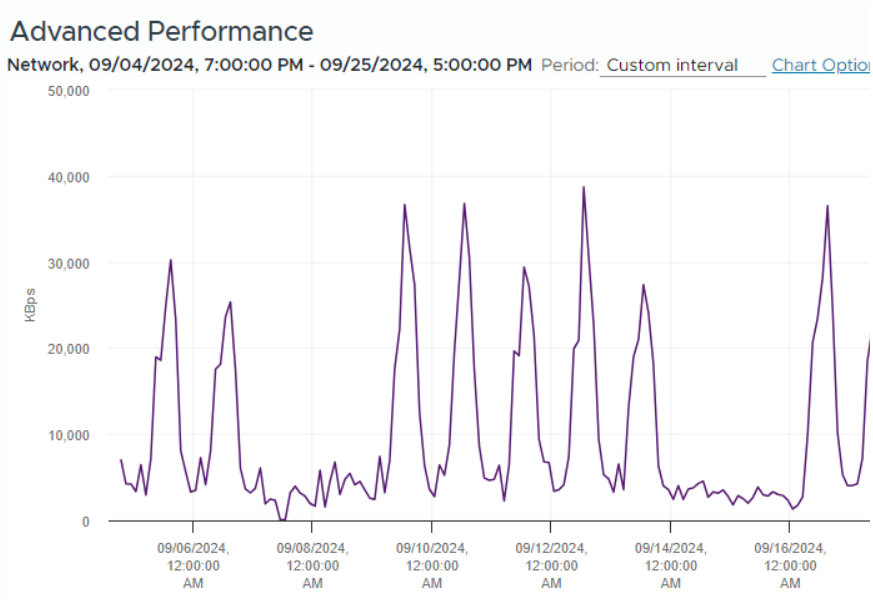


eproc 2G

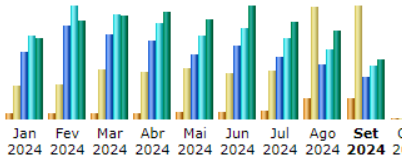

Entrada de rede (bytes)
5 minutos
Média
Bytes
500M
400M
300M
200M
100M
0
05/09
06/09
07/09
08/09
09/09
10/09
11/09
12/09
13/09
14/09
15/09
16/09


Saída de rede (bytes)
5 minutos
Média
Bytes
400M
300M
200M
100M
0
05/09
06/09
07/09
08/09
09/09
10/09
11/09
12/09
13/09
14/09
15/09
16/09

PJe 1G

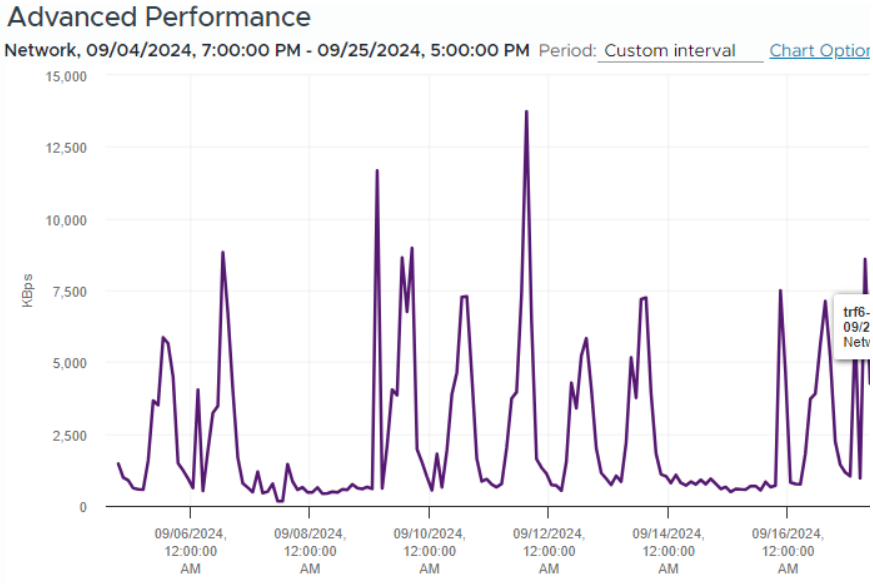


Histórico mensal

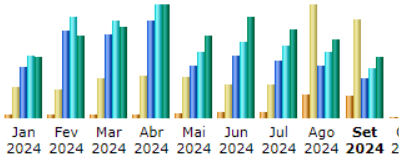


Mês	Visitantes únicos	Numero de visitas	Páginas	
Jan 2024	282,466	1,617,684	159,989,768	200
Fev 2024	279,897	1,638,735	223,614,352	271
Mar 2024	294,381	2,350,614	203,892,307	253
Abr 2024	266,606	2,250,684	188,101,855	232
Mai 2024	329,933	2,430,559	155,817,547	200
Jun 2024	358,789	2,221,693	175,565,838	217
Jul 2024	378,018	2,340,047	149,718,132	193
Ago 2024	1,013,989	5,420,881	130,438,491	168
Set 2024	1,007,870	5,423,532	100,601,439	129
Out 2024	0	0	0	
Nov 2024	0	0	0	
Dez 2024	0	0	0	
Total	4,211,949	25,694,429	1,487,739,729	1,86

PJe 2G

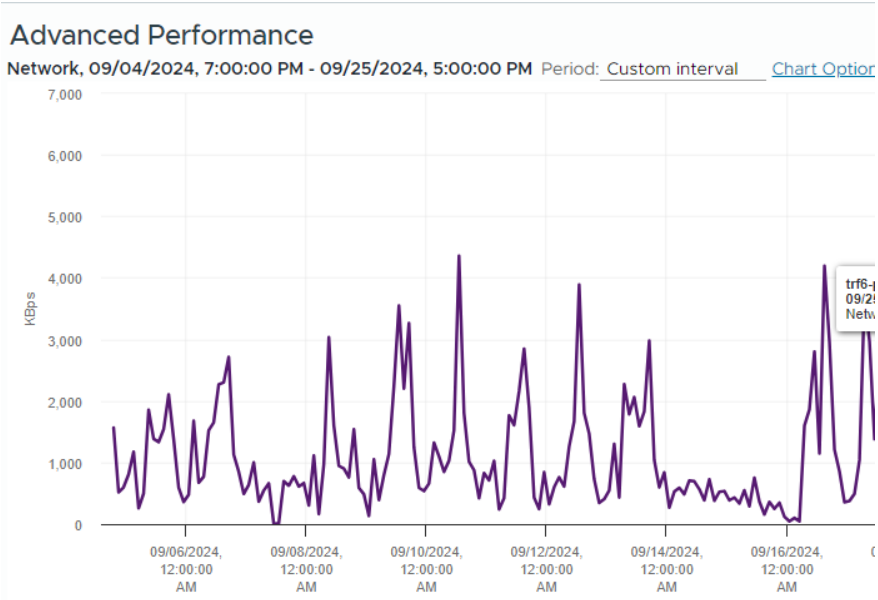


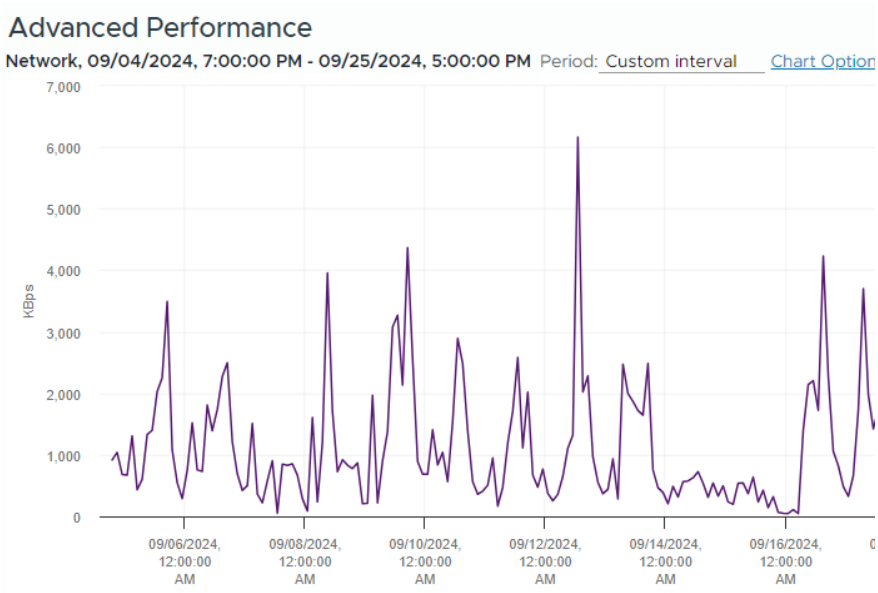
Histórico mensal

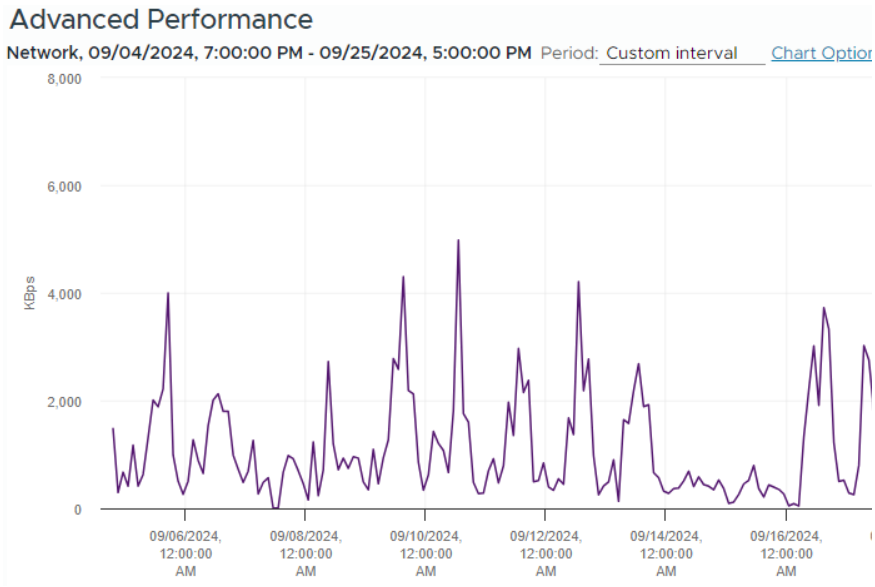


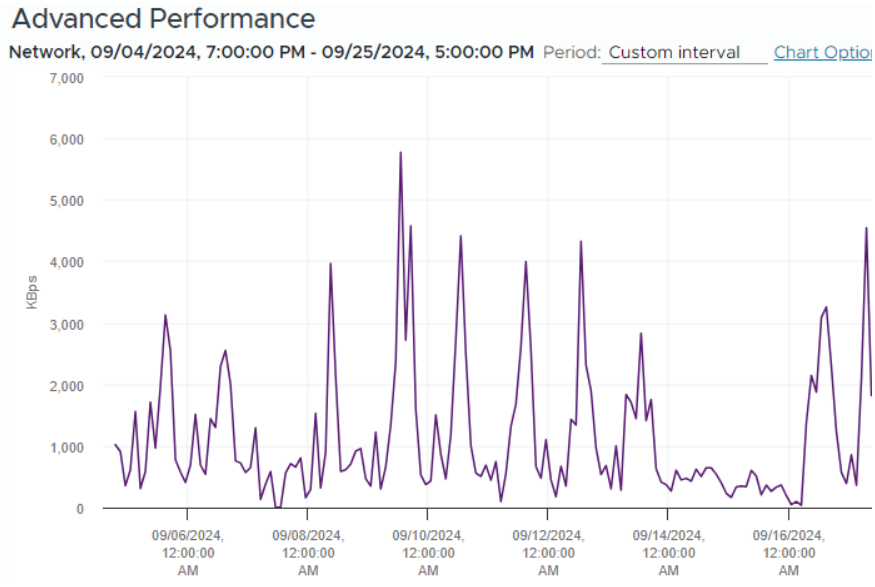
Mês	Visitantes únicos	Numero de visitas	Páginas	
Jan 2024	121,534	1,140,055	50,603,369	62,
Fev 2024	119,268	1,039,973	86,411,059	99,
Mar 2024	132,773	1,495,079	82,236,181	96,
Abr 2024	137,114	1,580,865	96,189,063	112
Mai 2024	185,189	1,532,332	51,570,086	65,
Jun 2024	214,194	1,225,425	61,991,629	75,
Jul 2024	223,385	1,252,687	56,493,473	71,
Ago 2024	880,687	4,226,360	51,612,950	65,
Set 2024	823,947	3,665,787	38,646,130	49,
Out 2024	0	0	0	
Nov 2024	0	0	0	
Dez 2024	0	0	0	
Total	2,838,091	17,158,563	575,753,940	698

MNI PJe 1G

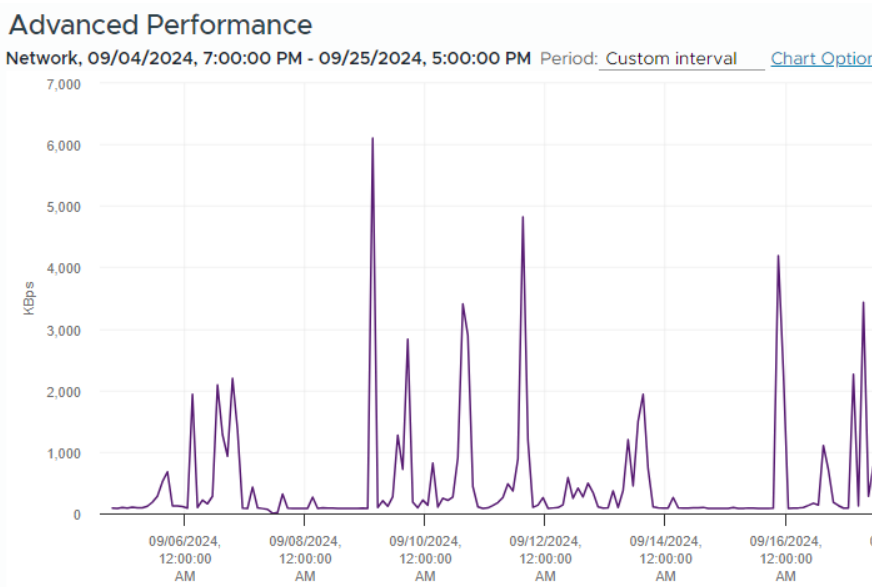


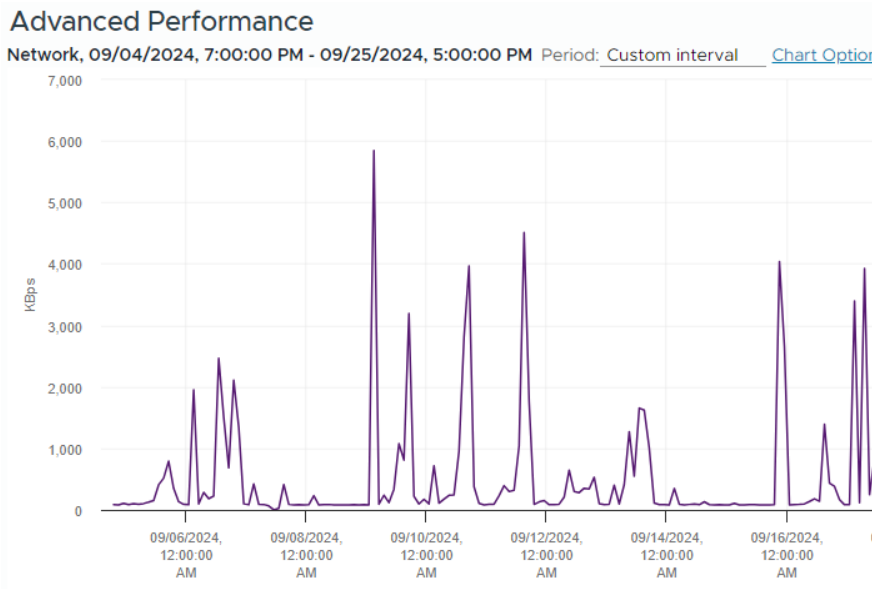



Advanced Performance
Network, 09/04/2024, 7:00:00 PM - 09/25/2024, 5:00:00 PM Period: Custom interval Chart Optio
8,000
6,000
4,000
2,000
0
KBps
09/06/2024, 12:00:00 AM
09/08/2024, 12:00:00 AM
09/10/2024, 12:00:00 AM
09/12/2024, 12:00:00 AM
09/14/2024, 12:00:00 AM
09/16/2024, 12:00:00 AM

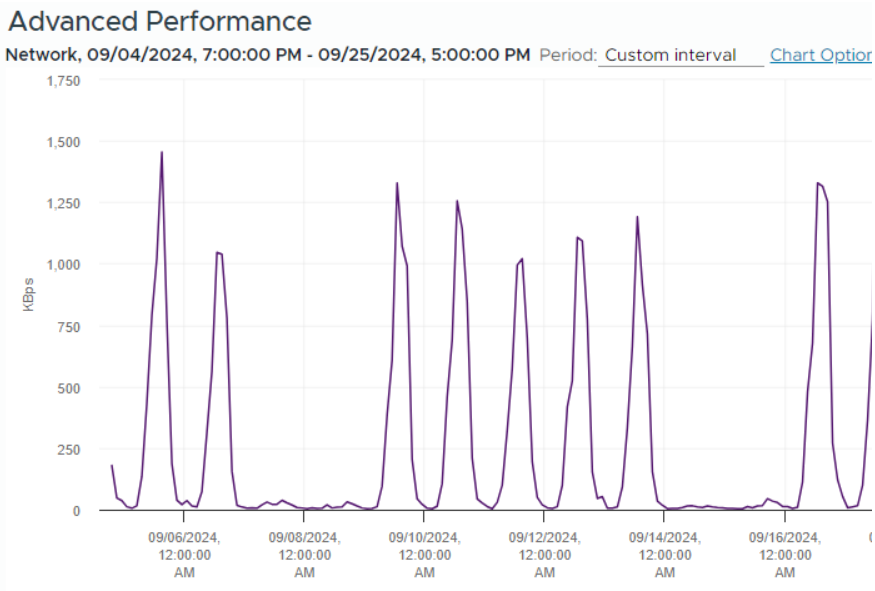

Advanced Performance
Network, 09/04/2024, 7:00:00 PM - 09/25/2024, 5:00:00 PM Period: Custom interval Chart Optio
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
KBps
09/06/2024, 12:00:00 AM
09/08/2024, 12:00:00 AM
09/10/2024, 12:00:00 AM
09/12/2024, 12:00:00 AM
09/14/2024, 12:00:00 AM
09/16/2024, 12:00:00 AM

MNI PJe 2G

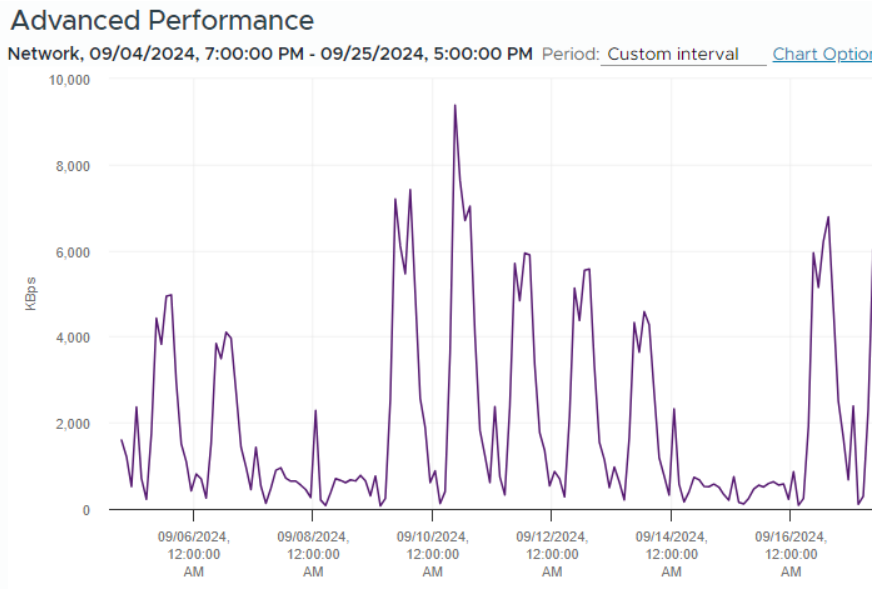

Advanced Performance
Network, 09/04/2024, 7:00:00 PM - 09/25/2024, 5:00:00 PM Period: Custom interval Chart Optio
7,000
6,000
5,000
4,000
3,000
2,000
1,000
0
KBps
09/06/2024, 12:00:00 AM
09/08/2024, 12:00:00 AM
09/10/2024, 12:00:00 AM
09/12/2024, 12:00:00 AM
09/14/2024, 12:00:00 AM
09/16/2024, 12:00:00 AM



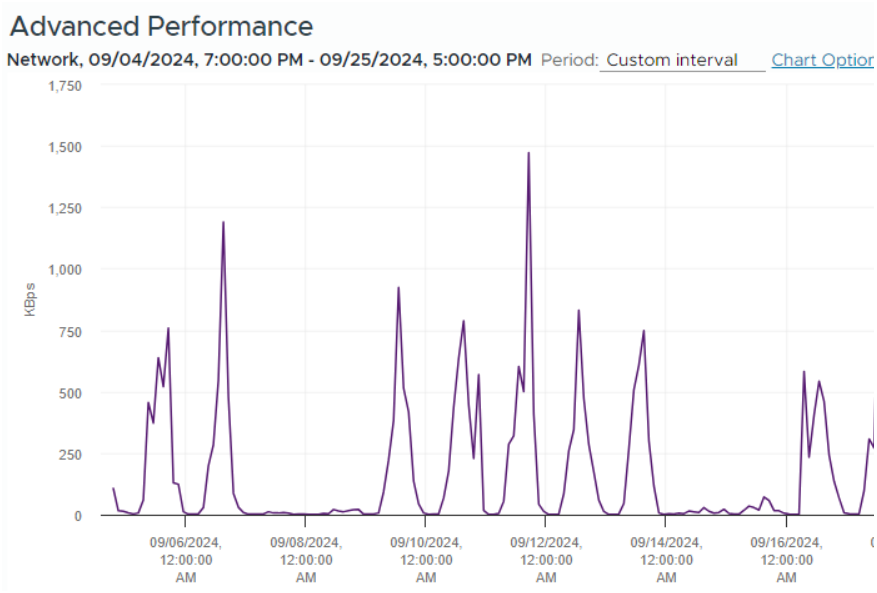
SEI



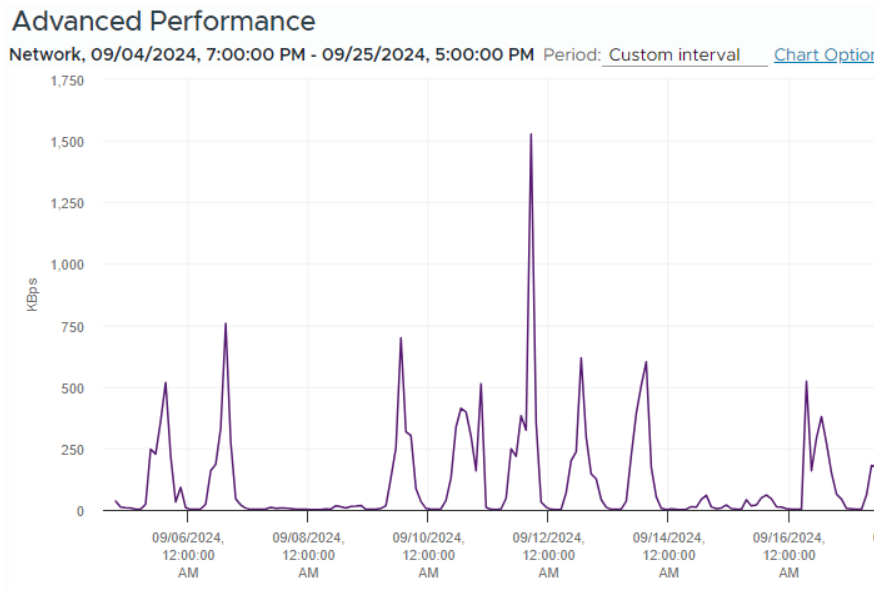
Portal



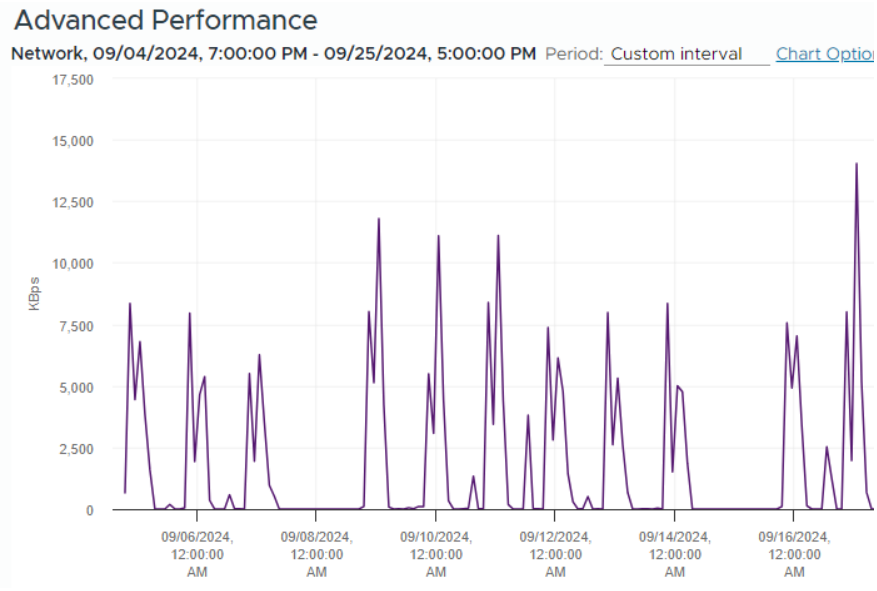
VPN



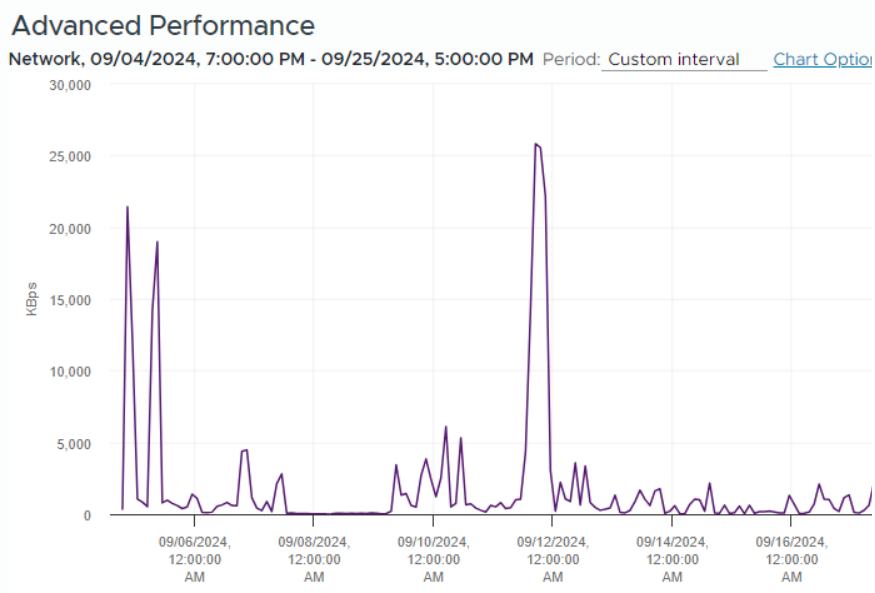
Servidor de Aplicação



Esiest



Proxy de Aplicações



VI - Estimativa do valor da contratação, acompanhada dos preços unitários referenciais, das memórias de cálculo e dos docu optar por preservar o seu sigilo até a conclusão da licitação

SOLUÇÕES / ÓRGÃOS	MJSP 0751481 (R$)	TRT2 0751491 (R$)	CFMV 0751498 (R$) *	STM 0751504 (R$)	TCU 0751517 (R$) *	MAP 0837732 (R$)	A 09
Solução em alta disponibilidade (appliance) FW	2.458.000,00	2.120.000,00				2.125.000,00	
Licenciamentos NGFW			1.777.346,67		2.075.850,00		
Instalação e Configuração		36.698,00					
Suporte Técnico		23.280,00 **	868.200,00		895.000,00		
Treinamento		65.210,00					
Web Application Firewall - Appliance Virtual				1.200.000,00			
Instalação e Configuração				74.900,00			
Suporte Técnico				678.000,00			
Treinamento				24.000,00			
Serviço de Segurança de Borda (Security Service Edge - SSE)							14.35
Instalação e Configuração							122
Suporte Técnico							
Treinamento							

* Valores de contratações públicas compatibilizados conforme as quantidades necessárias ao TRF6.

** Valores desconsiderados para o cálculo da média estimada em razão da relevante disparidade em relação aos demais.

LOTES	ITENS	CATMAT / CATSER	SERVIÇOS
01	01	484747	Appliances de Next Generation Firewall
	02	27472	Licenciamentos para operações de Next Generation Firewall p meses
	03	26972	Instalação e Configuração
	04	27740	Suporte Técnico por 60 (sessenta) meses
	05	3840	Treinamento
02	06	27472	Web Application Firewall - Appliance Virtual
	07	26972	Instalação e Configuração
	08	27740	Suporte Técnico por 60 (sessenta) meses
	09	3840	Treinamento
03	10	27742	Serviço de Segurança de Borda (Security Service Edge - SSE)
	11	26972	Instalação e Configuração
	12	27740	Suporte Técnico por 60 (sessenta) meses
	13	3840	Treinamento

VII - Descrição da solução como um todo, inclusive das exigências relacionadas à manutenção e à assistência técnica, quando

NECESSIDADES DE NEGÓCIO

a) Requisitos Técnicos da Solução

1. LOTE 1. FIREWALL

1.1. Características Gerais

1.1.1. A solução deverá ser composta de hardware e software licenciado do mesmo fabricante;

1.1.2. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de softwar

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

1.1.4. Na data da proposta, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-l

1.1.5. Todos os componentes devem ser próprios para montagem em rack “19” e deverão ser fornecidos pela Contratada, inc

1.1.6. Os gateways de segurança, bem como a gerência centralizada, deverão suportar monitoramento através de SNMP v2 e

1.1.7. Deve ser possível suportar arquitetura de armazenamento de logs redundante, permitindo a configuração de equipame

1.1.8. Devem possuir homologação da Agência Nacional de Telecomunicações (ANATEL) conforme determina a Resolução nº dos equipamentos.

1.1.9. Para atendimento do Inciso III, Art. 3o do Decreto 7.174/2010, quando da entrega dos equipamentos, o licitante de importação a eles referentes, sob pena de suspensão do(s) pagamento(s), rescisão contratual e multa;

1.1.10. Não serão aceitas soluções em hardware de computadores pessoais (Personal Computers – PC) ou servidores, sendo o

1.1.11. O fabricante deve ser parceiro do site www.cve.org, onde deverão estar indicados todos os CVE (Common Vulnerabiliti

1.1.12. O fabricante deverá manter em seu site todos os CVE identificados, seu detalhamento e correções disponibilizadas.

1.1.13. A solução deve estar posicionada entre os *challengers* e *leaders* no Quadrante Mágico do Gartner mais recente para so

1.1.13.1. O Gartner é um dos líderes mundiais em soluções de benchmarking de tecnologia e com o maior banco de dad

1.1.14. Deverá ser apresentado, ao menos um teste de laboratório (Nacional ou Internacional) que compare o seu produto proposta possua efetividade de segurança acima de 70%;

1.1.14.1. Para o teste especificado acima, poderá ser utilizado como referência os testes realizados pela organização s value map q2 2023”;

1.1.15. Com o objetivo de estabelecer efetividade de segurança dos firewalls de nova geração e assegurar que o fornecedo

proposto ou da mesma série proposta deverá:

1.1.15.1. Ser avaliado pela instituição NSS Labs (Network Security Services) no desempenho do Next Generation Firewall cento); OU

1.1.15.2. Ser avaliado pela instituição NetSecOpen; OU

1.1.15.3. Ser avaliado pela instituição Miercom Certified Perfomance Verified; OU

1.1.15.4. Ser avaliado pela instituição Miercom Certified Secure.

1.2. Capacidades e Quantidades - Solução em Appliance de Segurança de Perímetro de Próxima Geração

1.2.1. Throughput de, no mínimo, 15 Gbps (Threat Protection/Prevention SEM SSL/TLS) e no mínimo 5.8 Gbps(Threat Protectio

1.2.1.1. Firewall;

1.2.1.2. Detecção e Prevenção de intrusão (IDS/IPS);

1.2.1.3. Controle de aplicação;

1.2.1.4. Filtro de URL;

1.2.1.5. Antivírus;

1.2.1.6. Anti-spyware;

1.2.1.7. Anti-phishing;

1.2.1.8. Bloqueio de arquivos e logs;

1.2.1.9. Prevenção de ameaças avançadas de dia zero;

1.2.1.10. Inspeção SSL/TLS;

1.2.2. O fabricante deve possuir documentação pública, descrevendo o perfil de tráfego;

1.2.3. A documentação deverá ser específica para o modelo ofertado, sob pena de desclassificação;

1.2.4. Suporte a, no mínimo, 5M (cinco milhões) de conexões simultâneas;

1.2.5. Suporte a, no mínimo, 250.000 (Duzentos e cinquenta mil) novas conexões por segundo;

1.2.6. Throughput de, no mínimo, 11 (onze) Gbps, no mínimo, para conexões VPN;

1.2.7. Suportar e estar licenciado para acesso remoto Client-to-site ilimitado ou com a licença de maior capacidade;

1.2.8. Fonte de alimentação redundante e hot-swappable;

1.2.9. O firewall deverá possuir memória suficiente para aguentar a performance exigida no edital durante todo o tempo do c

1.2.10. No mínimo, 12 (doze) interfaces de rede 10Gbps SFP+;

1.2.11. No mínimo, 04 (quatro) interfaces de rede 10/100/1000;

1.2.12. No mínimo, 02 (duas) interfaces de 40G QSFP+;

1.2.13. Todas as interfaces devem vir acompanhadas do respectivo transceiver padrão Multimodo;

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

1.2.15. Possuir 1 (uma) interface de rede dedicada ao gerenciamento, não sendo permitido utilizar qualquer outra interface pa

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

1.2.17. Cada um dos appliances da plataforma de proteção de rede deve possuir discos Solid State Drive (SSD) redundantes c

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

1.2.19. Suporte a RFC 4291 de Arquitetura de endereçamento IPv6;

1.2.20. Deve suportar Dual stack ipv4/ipv6 e NAT64;

1.2.21. Deve suportar NAT64 e NAT46;

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

1.2.23. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IP v4 e v6 sem duplicação da base de objetos

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

1.2.25. Os valores de capacidade são considerados para cada equipamento, não sendo permitido a soma dos valores dos mer

1.3. Funcionalidades de Firewall

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

1.3.2. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos applian

1.3.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão ace

1.3.4. A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do apl

1.3.5. Realizar upgrade via SCP ou SFTP e https via interface WEB;

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

1.3.6.1. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based

1.3.6.2. Deverá suportar VXLAN;

1.3.7. Deve suportar os seguintes tipos de NAT:

1.3.7.1. Nat dinâmico (Many-to-1);

1.3.7.2. Nat estático (1-to-1);

1.3.7.3. Tradução de porta (PAT);

1.3.7.4. NAT de Origem;

1.3.7.5. NAT de Destino;

1.3.7.6. Suportar NAT de Origem e NAT de Destino simultaneamente;

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

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

1.3.10. Deverá permitir a criação de regras de firewall e NAT utilizando nos campos de origem e destino, objetos de serviços que não se caracterizam como FQDN;

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

1.3.12. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de

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

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

1.3.15. Suportar OSPF graceful restart;

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

1.3.17. Para o ECMP, a solução deve suportar o balanceamento do roteamento de forma simultânea usando os seguintes parâ

1.3.18. Autenticação integrada via Kerberos;

1.3.19. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções/ações d
falta de acesso do administrador para qualquer mitigação de falha e aplicação de política para solução de problema.

1.3.20. As regras Firewall devem suportar “hit count” para monitorar a quantidade de conexões que deram matches em cada

1.3.21. A solução deve ter a capacidade de operar através de uma única instância de Firewall de forma simultânea median
análise o trafego de rede), camada 2 (L2) e camada 3 (L3);

1.3.22. A solução deve permitir o agendamento de instalação de políticas para serem aplicadas em horários pré-definidos at
horários pré-definidos;

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

1.3.24. Deverá suportar redundância e balanceamento de links, tendo capacidade a no mínimo 3 links de internet;

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

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

1.4. Funcionalidades de Filtro de Conteúdo WEB

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

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

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

1.4.4. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-de

1.4.5. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e p

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

1.4.5.2. Reconhecer pelo menos 4.500 (quatro mil e quinhentas) aplicações diferentes, incluindo, mas não limitado: a t
voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

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

1.4.7. Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte aoHTTP/3 ou Perfect Forward Secrecy (conjun

1.4.8. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem

1.4.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e va

1.4.10. A fim de otimização de tempo operacional dos administradores, a solução deverá possuir pelo menos 30 categorias ou

1.4.11. Para solução de filtro de conteúdo e controle web, deve ser capaz de bloquear na mesma aplicação um conteúdo espe

1.4.12. Possuir mecanismo de controle de aplicação web e URL com configuração de bloqueio e liberação da aplicação prin
categorias do facebook, como facebook chat, vídeo, game, compartilhamento de arquivos ou outros. Ou seja, não deve ser
não só do Facebook, mas também bloqueará tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter , YouTube,

1.4.12.1. A solução precisa ser baseada em bloqueio de aplicações WEB que a própria base possui, assim a inspeção oco

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

1.4.14. Atualizar a base de assinaturas de aplicações automaticamente;

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

1.4.16. Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário
controlador de domínio, nem nas estações dos usuários. Assim, permitindo a criação de politicas de segurança baseadas nas

1.4.17. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por, pelo menos, checagem de assin

1.4.18. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a

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

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

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

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

1.4.23. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais
local;

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

1.4.25. Suportar armazenamento, na própria solução ou na plataforma de gerencia local, de URLs, evitando delay de comunic

1.4.26. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesm

1.4.27. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso
software livre;

1.4.28. Suportar a criação de categorias de URLs customizadas;

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

1.4.30. Permitir a customização de página de bloqueio;

1.4.31. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granula
nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

1.4.32. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC

1.4.33. Deve permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à int
(Captive Portal);

1.4.34. A solução deverá implementar uma análise avançada de URL em tempo real enviando a URL para o serviço de análise

1.4.35. A filtragem de URL em tempo real deverá ser ativada por meio de filtragem de URL.

1.5. Funcionalidades de Prevenção de Ameaças

1.5.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os móc

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

1.5.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Malware e Anti-Phishing quando implementado em alta disponibil

1.5.4. Deve suportar granularidade nas políticas de Antivírus, Anti-Phishing e Anti-malware, possibilitando a criação de diferen

1.5.5. A fim de não criar indisponibilidade no appliance de segurança, a solução de IPS deve possuir mecanismo de fail-
gerenciado automaticamente pelo SO;

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

1.5.6.1. Análise de padrões de estado de conexões, análise de decodificação de protocolo;

1.5.6.2. Análise para detecção de anomalias de protocolo;

1.5.6.3. IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;

1.5.7. Detectar e bloquear a origem de portscans;

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

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

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

1.5.11. Suportar bloqueio de arquivos por tipo;

1.5.12. Identificar e bloquear comunicação com botnets;

1.5.13. Deve suportar referência cruzada com CVE;

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

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

1.5.14.2. Severidade;

1.5.14.3. Tipo de ação a ser executada;

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

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

1.5.17. O IPS deve incluir um modo de solução de problemas que defina o perfil em uso para detectar apenas, sem modificar a

1.5.18. O administrador deve poder ativar automaticamente novas proteções, com base em parâmetros configuráveis (impact

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

1.5.19.1. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação toma

1.5.20. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS através da console de gerência centralizada;

1.5.21. Na própria interface de gerência, a solução de IPS deverá apresentar sumário de todos os equipamentos que estão ser

1.5.22. A solução de IPS, deve possuir mecanismo de análise baseado nas conexões realizadas para as aplicações, que ap
evitando qualquer tipo de ataque para aplicações que estão expostas no ambiente.

1.5.23. O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados na funcionalida

1.5.24. A solução deverá possuir pelo menos dois perfis pré-configurados pelo fabricante que permitam sua utilização assim q

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

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

1.5.27. Solução deve proteger contra os ataques do tipo DNS Cache Poisoning, e impedir que os usuários acessem endereços

1.5.28. O gerenciamento centralizado via interface gráfica deve possibilitar a configuração de captura dos pacotes por regras

1.5.29. A solução de IPS deve possuir engine com determinação de forma automática de qualquer nova assinatura que for bai

1.5.29.1. Deverá atuar em modo de prevenção ou detecção, de forma a evitar qualquer tipo de alteração na base de ass

1.5.30. O antivírus deve oferecer suporte à verificação de links dentro de e-mails.

1.5.31. A solução de anti-malware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede quar

1.5.32. A solução deve permitir criar regras de exceção de acordo com a proteção, a partir do log visualizado na interface grá

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

1.5.34. A solução deve permitir a criação de White list baseado no MD5 do arquivo;

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

1.5.36. Suportar rastreamento de vírus em arquivos pdf;

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

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

1.5.39. Em caso de falha no mecanismo de inspeção do Antivírus, deve ser possível configurar se as conexões serão permitida

1.5.40. A solução de Antivírus e Antimalware deve funcionar de forma independente, ou seja, caso sejam desabilitadas, elas
avançadas (zero-day);

1.5.41. A solução Antivírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS/SMB, de forma a conte

1.5.42. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloquea

1.5.43. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

1.5.44. Deverá possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos, s
bloquear o acesso do usuário.

1.5.45. A solução de Antimalware deve ser capaz de detectar e interromper o comportamento anormal suspeito da rede.

1.5.46. A solução deve possuir funcionalidade de identificação de bloqueio de trafego malicioso comunicando com C&C (comn

1.5.47. A solução Antivírus deverá suportar a análise de links no corpo de e-mails.

1.5.48. Modelos de deep learning em linha para prevenir tráfego C2 desconhecido e evasivo de ferramentas como Cobalt Strik

1.5.49. Modelos de machine learning baseados na nuvem, atualizados regularmente, para prevenir explorações desconhecida

1.5.50. Bloqueio de ataques de malware na camada de rede com detecções baseadas em assinaturas em linha;

1.5.51. Assinaturas personalizadas para vulnerabilidades de software e ataques de command-and-control;

1.5.52. Análise baseada em heurísticas, decodificação de protocolos, proteção contra anomalias de protocolo e assinaturas de

1.5.53. Inspeção e classificação do tráfego, detectando e bloqueando malware e exploits de vulnerabilidades em uma única p

1.5.54. Uso de AI, aprendizado de máquina e deep learning para detecção precisa de variantes avançadas de malware;

1.6. Funcionalidades de Controle de Qualidade de Serviço

1.6.1. Suportar a criação de políticas de QoS por: endereço de origem, endereço de destino e por porta;

1.6.2. O QoS deve possibilitar a definição de classes por: Banda garantida, banda máxima e fila de prioridade;

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

1.6.4. A solução deve permitir, por aplicação, o encaminhamento do tráfego para diferentes links de Internet, sejam eles loca Public APN) e Satélite;

1.6.5. Deve possibilitar a utilização de configuração inteligente de acessos WAN IP ativos-ativos sem a necessidade de switc apenas na configuração dos acessos principal e backup;

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

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

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

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

1.6.10. Redistribuição do tráfego balanceado, de forma inteligente, tendo em conta o congestionamento da largura de banda, definidas;

1.6.11. Habilitar a mesma interface WAN para enviar tráfego simultaneamente por meio de túneis IPSec SD-WAN e nativamen

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

1.6.13. Suportar políticas inteligentes usando configuração padrão de fábrica que executem redirecionamento automático e ir

1.6.14. Suportar o redirecionamento do tráfego de internet de pontos remotos para um ponto de internet centralizado, usando

1.6.15. Redirecionamento condicionado do tráfego de internet em caso de falha do link de internet local ou do link remoto cer

1.6.16. Suporte simultâneo ao redirecionamento do tráfego da Web de alguns aplicativos para a Internet centralizada, outros

1.6.17. Implementar o conceito de perfis de configuração e grupos de objetos para automatizar o processo de implementação

1.6.18. Usar probes artificiais baseadas em icmp, udp ou tcp para medir a qualidade da rede percebida pelo tráfego do usuári

1.6.19. Capacidade de realizar agregação de largura de banda automaticamente entre links de diferentes velocidades, levan de baixa velocidade;

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

1.6.21. Implementar um mecanismo de proteção de variação de latência (jitter) mesmo que a degradação esteja em todos os com controle de qualidade do SD-Wan;

1.6.22. Garantir o desempenho de aplicativos em um cenário de link de transporte duplo quando ambo os links estão degrada

1.6.23. Possuir um mecanismo de priorização (QoS) para proteger o tráfego de aplicativos clientes prioritários quando houver

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

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

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

1.6.27. Realizar medições de “Latência”/”Jitter”/”Queda de pacotes” em cada um dos túneis SDWAN independentemente, na

1.6.28. O Orquestrador pode estar na Nuvem ou até mesmo ser instalado em um servidor dedicado ou virtualizado, utilizando

1.6.29. No caso do Orchestrator estar na nuvem, a administração de atualizações, gerenciamento de alta disponibilidade e ha

1.7. Funcionalidades de VPN

1.7.1. Suportar VPN Site-to-Site e Cliente-To-Site;

1.7.2. Suportar IPSec VPN;

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

1.7.4. Suportar SSL VPN;

1.7.5. A VPN IPSEc deve suportar:

1.7.5.1. Algoritmos de criptografia 3DES, AES 128 e 256;

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

1.7.5.3. Algoritmo Internet Key Exchange (IKE) v1 e v2;

1.7.5.4. Autenticação via certificado IKE PKI;

1.7.5.5. Autenticação MD5, SHA-1, SHA-384,SHA-256, SHA-512;

1.7.6. A VPN SSL deve suportar:

1.7.6.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou

1.7.6.2. A funcionalidade de VPN SSL deve ser atendida com ou sem o uso de agente;

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

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

1.7.6.5. Atribuição de DNS nos clientes remotos de VPN;

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

1.7.7. A solução deve possuir checagem de conformidade e verificar, no mínimo, as seguintes informações no cliente remot ativos;

1.7.8. A solução deve permitir bloquear o acesso do usuários aos recursos via VPN caso o usuário não esteja em conformidade

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

1.7.10. A solução deve permitir a integração da ferramenta com provedores de identidade, atraves de SAML, para autenticaçã

1.7.11. Suportar leitura e verificação de CRL (certificate revocation list);

1.7.12. A tecnologia de VPN Client to Server deverá ser instalada na plataforma: iOS 10 ou superior e Android;

1.7.13. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows 7, Windows 10/11 e MacOS X.

1.8. Solução para Proteção Contra Ameaças Avançadas - Zero Day

1.8.1. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidc

1.8.2. A solução deverá ser composta por hardware e software específicos (appliance) com sistema operacional especializac para prevenção de ataques zero-day;

1.8.3. Não será aceito soluções que dependa da estrutura de hypervisor do contratante para a analise de ameaças de dia zerc

1.8.4. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS seja entregue parcialmente ao cliente.

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

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

1.8.7. Ameaças trafegadas em protocolo SMTP, de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails perr

1.8.8. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7,

1.8.9. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise compl este arquivo para o cliente;

1.8.10. O conteúdo enviado para a solução de Sandboxing deverá ser feito automaticamente, sem a necessidade da interaçãc

1.8.11. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana o

1.8.12. Toda análise dos arquivos deverá ser realizada em ambiente controlado Sandboxing em nuvem ou on-premisse em soluções em servidores genéricos ou software livre;

1.8.13. A funcionalidade de prevenção de ameaças avançadas deve ser habilitada e funcionar de forma independente das out

1.8.14. Toda análise deverá ser realizada em nuvem do próprio fabricante ou equipamento on-premisse do mesmo fabricante

1.8.15. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no forma

1.8.16. Deve implementar análise em sandbox, detecção e bloqueio de malwares em arquivos executáveis, DLLs, ZIP e cripto

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

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

1.8.19. O relatório das emulações deve apresentar de maneira detalhada as atividades executadas em filesystem, registros cada SO emulado;

1.8.20. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar inte

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

1.8.22. Capacidade de análise, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecı desconhecido: pdf, tar, zip, rar, seven-z, exe, dll, rtf, csv, scr, todos os tipos de arquivos do Microsoft Office, arquivos do Mac de script(BAT,JS,VBS,PS1,script do Shell e HTA), análise de links em mensagens de e-mail e arquivos criptografados (TLS/SSL);

1.8.23. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real e o bloqueio deve ser ime

1.8.24. Possibilitar remoção de conteúdo ativo dinâmicos como macros, URLs, Java scripts e outros dos arquivos baixados, per

1.8.25. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

1.8.26. A solução deve possuir mecanismo para identificar sites conhecidos e desconhecidos como phishing, analisando em te

1.8.27. A solução deve permitir bloquear o acesso do usuário caso o mesmo tente fazer o envio de suas informações em sites

1.8.28. O Mecanismo de classificação de anti-phishing deve atuar sem a necessidade de instalação de agente na máquina do

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

1.8.29.1. Número de arquivos emulados;

1.8.29.2. Número de arquivos com malware;

1.8.30. A solução de prevenção de ameaças avançada, deve possuir capacidade de apresentar em seus logs, visibilidade de com a ameaça detectada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada

1.8.31. A solução deve prover informação, seja por meio de relatório ou log, sobre as seguintes situações:

1.8.31.1. Quantidade arquivos emulados e ações aplicadas OU o tamanho máximo do arquivo emulado seja excedido;

1.8.31.2. Classificar dos arquivos minimamente com os tipos (limpos, suspeitos e maliciosos) ou o tempo máximo de emu

1.9. Módulo de Gerência

1.9.1. A solução de gerência deverá ser separada dos gateways de segurança, que irá gerenciar políticas de segurança gerenciado individualmente;

1.9.2. Deve ser compatível com VMware ESXi com espaço de armazenamento para LOGs de no mínimo, 200GB/LOG/DIA de in

1.9.3. Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deve ser ofertado, no m

1.9.4. Caso a solução possua módulo de relatórios estendida, deve ser também entregue junto com a solução;

1.9.5. Deve fornecer consultas de logs, geração de relatório das funcionalidades de segurança que estão ativadas nos NGF aplicação web, filtro URL, prevenção de ameaças (IPS, Antivírus, Anti-phishing, Anti-Malware e Sandboxing);

1.9.6. Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equip

1.9.7. O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo podendo esta

1.9.8. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos

1.9.9. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface d

1.9.10. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

1.9.11. Todos os logs da solução devem ser indexados e seu licenciamento deve ser o de maior capacidade.

1.9.12. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrent

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

1.9.14. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

1.9.15. Suportar backup das configurações e rollback de configuração para a última configuração salva;

1.9.16. Suportar validação de regras antes da aplicação;

1.9.17. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

1.9.18. Deve permitir a visualização dos logs de uma regra específica em tempo real e na mesma tela de configuração da reg

1.9.19. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;

1.9.20. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou

1.9.21. Deve apresentar eventos em um único portal (dashboard) e geração de relatório de todas as funcionalidades de apresentação onde consta todo os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção

1.9.22. A solução deve permitir o login de múltiplos usuários administradores simultâneos com perfil de escrita, possibilitando

1.9.23. A solução deve permitir a integração da ferramenta com provedores de identidade para autenticação dos administrad

1.9.24. A solução deve permitir revisar e aprovar alterações de políticas de segurança feitas por outros administradores.

1.9.25. A solução deve permitir criar perfis de administradores para realizar revisão/alteração das políticas de segurança, com

1.9.26. A solução deverá enviar a solicitação de aprovação de políticas de segurança por pelo menos uma das seguintes form

1.9.27. Permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco d

1.9.28. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passa

1.9.29. Deve ser possível exportar os logs em CSV ou TXT;

1.9.30. O visualizador de log deve ter um recurso de pesquisa de texto livre;

1.9.31. Deve possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

1.9.32. Possibilitar rotação do log;

1.9.33. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

1.9.33.1. Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda;

1.9.33.2. Principais aplicações por taxa de transferência de bytes,

1.9.33.3. Principais hosts por número de ameaças identificadas;

1.9.33.4. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categc vinculadas a este tráfego;

1.9.34. Deve permitir a criação de relatórios personalizados;

1.9.35. O gerenciamento centralizado deverá ser entregue como appliance virtual e dever ser compatível/homologado com/pa

1.9.36. A solução de gerenciamento deve possui a capacidade de gerenciar outros Firewalls de segurança do mesmo fabı (VMWare NSX ou Cisco ACI);

1.9.37. Possui capacidade de integração com soluções de terceiros via API e também suportar configurações através de RestA

1.9.38. Deve consolidar logs e relatórios de todos os dispositivos administrados;

1.9.39. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escı

1.9.40. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

1.9.41. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

1.9.42. Permitir que os relatórios possam ser salvos, enviados e impressos;

1.9.43. Deve permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, se

1.9.44. A solução deve prover, no mínimo, as seguintes funcionalidade para análise avançada dos incidentes:

1.9.45. Visualizar quantidade de tráfego utilizado de aplicações e navegação;

1.9.46. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

1.9.47. A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

1.9.48. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

1.9.49. Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma compl de eventos gerados e protegidos;

1.9.50. Deve permitir a integração com servidores de autenticação LDAP Microsoft Active Directory via Radius;

1.9.51. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuár

1.9.52. Geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais

1.9.53. A plataforma de gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navega centralizado possibilitando a procura correlacionada de logs em uma única tela, como, por exemplo, pesquisar logs de Antivír

1.9.54. O relatório das emulações (sandboxing) deve conter de maneira detalhada as atividades executadas em filesystem, r para cada SO emulado;

1.9.55. Possuir mecanismo para que logs antigos sejam removidos automaticamente;

1.9.56. Possuir a capacidade de personalização de gráficos como barra, linha e tabela;

1.9.57. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, a

1.9.58. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memó

1.9.59. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequé

1.10. Capacitação Técnica

1.10.1. O treinamento deverá ser completo para contemplar a instalação, customização, operação e administração da soluç online e ao vivo;

1.10.2. O treinamento deverá ser ministrado para turma especifica para a CONTRATANTE;

1.10.3. Serão aceitos cursos oficiais do fabricante da solução;

1.10.4. Deverá possuir módulos teóricos e práticos;

1.10.5. Os instrutores devem ser certificados pelo fabricante da solução para o treinamento;

1.10.6. O conteúdo dos cursos deverá abranger, minimamente, os seguintes tópicos:

1.10.6.1. Configuração – acesso e navegação na solução; comando de configurações básicas e avançadas; estrutura/arqu

1.10.6.2. Operação – comandos de gerenciamento e monitoramento da saúde dos recursos dos equipamentos; aplicação

1.10.7. Ao final do treinamento deve ser emitido certificado de conclusão para cada participante/aluno constando a carga hor

1.11. Instalação e configuração

1.11.1. Os serviços de instalação e configuração deverão ser executados por técnico(s) certificado(s) pelo fabricante;

1.11.2. Os serviços de instalação compreendem as atividades de planejamento, instalação física, instalação lógica e finalizaçã

1.11.3. Os serviços de configuração consistem em ajustar todos os parâmetros necessários (físicos e lógicos) para o funciona requisitos dessa especificação;

1.11.4. Caberá à CONTRATADA todo o processo de planejamento, a instalação, a configuração, a integração, os testes e Informação existente no local de instalação dos equipamentos;

1.11.5. A instalação compreenderá a migração das configurações e regras existentes no ambiente atual do CONTRATANTE, s disponibilidade.

1.12. Operação Assistida

1.12.1. A operação assistida deverá ocorrer durante 45 dias corridos a partir da instalação e configuração da solução na CONT

1.12.2. O serviço de operação assistida é composto por um conjunto de atividades que permitem o treinamento e a capacit corretiva, transferindo todo o conhecimento e experiência necessária para a operação da solução;

1.12.3. Durante os 45 dias corridos, será prestado todo o suporte necessário para a operacionalidade da solução, minimi tecnologia envolvida em regime de treinamento enquanto trabalha, até que a CONTRATANTE possa assumir as atividades cor

1.12.4. Durante a operação assistida também será necessário realizar, pela CONTRADADA, possíveis customizações e ajustes

1.12.5. Por padrão, a prestação da operação assistida ocorrerá presencialmente nas dependências da CONTRATANTE ou remo

1.12.6. A CONTRATADA deverá fornecer suporte técnico especializado em formato de Banco de horas para a solução ofertada

1.12.7. A CONTRATADA deverá realizar a prestação de serviço remoto no modelo de banco de horas com um total de 300h, pagamento somente se forem utilizadas.

1.13. Suporte, manutenção e atualização de versão

1.13.1. O suporte técnico compreende o diagnóstico e identificação de problemas, apoio técnico na utilização, correção de módulo disponível de forma nativa na solução de firewall, ou decorrente de qualquer adaptação (customização) e ajuste (tuni

1.13.2. O atendimento a um chamado de suporte deverá ocorrer por qualquer uma das seguintes formas: contato telefônico solução de firewall, com controle de acesso por senha;

1.13.3. O atendimento telefônico sempre que aplicável e viável, por meio de ligação local em Belo Horizonte/MG ou ligação in

1.13.4. A CONTRATANTE poderá efetuar um número ilimitado de chamados técnicos para a CONTRATADA, por qualquer uma

1.13.5. Na abertura ou registro de um chamado técnico, por qualquer uma das formas disponíveis, a CONTRATADA deverá in identificação completa do solicitante;

1.13.6. A CONTRATADA deverá retornar, via e-mail, a confirmação da abertura do chamado técnico, doravante denomin identificação do chamado, identificação do responsável da CONTRATADA pela abertura do chamado;

1.13.7. O atendimento ao chamado técnico pela CONTRATADA deverá ocorrer pelo menos por uma das seguintes formas fabricante da solução de firewall ou da CONTRATADA, presencial ou suporte por acesso remoto;

1.13.8. Caso acionado o suporte direto do fabricante, este deverá ter atendimento em português. Caso contrário, a CONTRATA

1.13.9. Um chamado técnico somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE, na f sistema oferecido pela CONTRATADA, caso esta forma seja utilizada;

1.13.10. Após apresentar uma solução de contorno para o chamado técnico, a CONTRATADA deverá retornar, via e-mail, a c chamado, data e hora de conclusão do atendimento, descrição dos serviços executados e/ou da solução apresentada;

1.13.11. Em caso de adoção de solução de contorno, sem prejuízo da solução definitiva cabível, a CONTRATADA deverá emiti solucionar o problema de forma definitiva;

1.13.12. Após apresentar uma solução definitiva para o CHAMADO TÉCNICO, a CONTRATADA deverá retornar, via e-mail, a c chamado, data e hora de conclusão do atendimento, descrição dos serviços executados e/ou da solução apresentada;

1.13.13. Deverá ser garantido à CONTRATANTE o pleno acesso ao sítio (site) dos fabricantes dos produtos que compõem a disponíveis para seus usuários;

1.13.14. Caberá exclusivamente à CONTRATANTE a decisão de implantar ou não quaisquer atualizações de software fornecid

1.13.15. A CONTRATADA deverá disponibilizar mecanismos para a atualização de software pelo download direto através da software em questão;

1.13.16. O serviço de manutenção consiste na correção de qualquer problema ou falha apresentados em componentes físicos

1.13.17. A atualização de software é uma alteração da versão anterior com o objetivo de implementar melhorias. Essas melh

1.13.18. O prazo de atualização de todo software fornecido deve ser igual ao período de garantia do produto. Durante a vigên

1.14. Garantia

1.14.1. O(s) equipamento(s) que compõe(m) a solução devem estar em linha de fabricação até a data de assinatura do contra

1.14.2. O serviço de Garantia contempla garantir o correto e pleno funcionamento de todos os itens adquiridos, seja hardware

1.14.3. A CONTRATADA deverá garantir a substituição de qualquer módulo defeituoso, incluindo hardware, software ou comp equipamento se for necessário;

1.14.4. Não haverá custos adicionais para a CONTRATANTE de substituição de quaisquer componentes durante o período de g

1.14.5. Prazo de garantia deverá ser de 60 meses.

2. LOTE 2. WEB APPLICATION FIREWALL APPLIANCE VIRTUAL

2.1. Características Gerais

2.1.1. Não serão aceitos produtos ou serviços do tipo demo, trial e open-source. A solução deve ser proprietária;

2.1.2. A solução de WAF deverá ser fornecida em appliance virtual;

2.1.3. O appliance virtual deverá ser compatível com VMWARE e KVM, além de estar disponível no marketplace da AWS, GCP

2.1.3.1. Caso não seja possível a instalação em ambiente *on premises*, o licenciamento poderá sere realizado em nuvem

2.1.4. A solução deve ser capaz de visualizar, via console, as informações de saúde e desempenho de todo o ambiente que a

2.1.5. Possuir suporte a SNMP v2c e v3;

2.1.6. Enviar mensagens por e-mail e traps SNMP;

2.1.7. Os componentes da solução poderão ser executados num mesmo appliance, ou poderão ser distribuídos em múl funcionamento e performance exigidas neste edital;

2.1.8. A solução deverá ter o pleno funcionamento independentemente de conexão (física ou lógica) com o fabricante, exceto

2.1.9. Suportar IPV6;

2.1.10. A solução deverá possuir a capacidade para suportar a adição de novos componentes (hardware e/ou software) escalá

2.1.11. Apresentar uma relação descritiva dos componentes fornecidos, incluindo seus códigos comerciais;

2.1.12. Não será aceito equipamento do tipo NGFW (Next Generation Firewall).

2.2. Características do Appliance

2.2.1. Deve ser capaz de executar todas as suas funções de aprendizado, análise e proteção de tráfego web considerando pel

2.2.2. A solução deve ter vários mecanismos de implantação (deployment) com pelo menos uma ponte transparente na linha (passivo) a fim de monitorar o tráfego sem fazer alterações na rede;

2.2.3. A solução deve permitir a integração nos modos proxy reverso explícito e proxy reverso transparente (Bridge L2);

2.2.4. A solução deve ter um impacto de milissegundos na latência da rede;

2.2.5. O sistema deve permitir a integração e envio de alertas para terceiros ou ferramentas de correlação (SIEM). Será perm RestAPI;

2.2.6. O equipamento deve suportar o protocolo de gerenciamento de rede SNMP a ser monitorado por ferramentas de tercei

2.2.7. Todos os componentes da solução de WAF com recursos para efetuar o balanceamento de carga entre aplicações dev outros fabricantes, podendo a CONTRATANTE realizar diligência junto ao mesmo para esta comprovação quando da recepção podem ser ofertadas no mesmo applicance ou em appliances distintos;

2.2.8. A solução de WAF com balanceamento de carga entre aplicações Web ofertada de maneira integrada deve ser compost

2.2.9. Caso a solução de WAF seja ofertada separadamente da solução balanceamento de carga entre aplicações Web, tanto dois applicances ou servidores cada;

2.2.10. A solução de WAF e a solução de balanceamento entre aplicações web devem ser do mesmo fabricante;

2.2.11. A capacidade de processamento da solução deverá seguir as melhores práticas de cada fabricante, considerando todo requisições nível 7, requisições SSL, transações e compressão;

2.2.12. Deve possuir CPU e memória suficientes para atender aos throughputs definidos no edital tanto para WAF quanto pa funcionalidades;

2.2.13. Os equipamentos que serão responsáveis pela inspeção de tráfego web e pelo balanceamento de carga para soluçõe pelo menos 1 (um) Gbps tanto para a funcionalidade de firewall de aplicação Web como para a funcionalidade de balanceame

2.2.14. As soluções de WAF com balanceamento ofertadas no mesmo appliance deverão suportar o throughput de pelo menos

2.3. Balanceamento, Cache e Aceleração Web

2.3.1. Deve suportar no mínimo 1 Gbps (um Gigabits por segundo) de inspeção de tráfego na camada 7. Para alcançar esse como por exemplo imagens, após a sua primeira inspeção. Todo conteúdo estático permitido em cache não será reinspeciona

2.3.2. A solução fornecida deverá operar em cluster oferecendo alta disponibilidade com tolerância a falhas, independenteme

2.3.3. Na falha de um dos elementos do cluster, não poderá haver nenhuma degradação ou indisponibilidade das aplicações;

2.3.4. Deve suportar configuração de mTLS em um virtual server de aplicação do TRF6;

2.3.5. Deve suportar configuração de mTLS por url e path de aplicação do TRF6;

2.3.6. A solução deve ser capaz de trabalhar com recursos de alta disponibilidade, permitindo a ligação de dois ou mais equip

2.3.7. Deve ser fornecido todos os recursos possíveis de redundância sem nenhuma despesa com licenças adicionais;

2.3.8. A solução deve permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:

2.3.8.1. Compartilhar a rede de heartbeat com a rede de dados;

2.3.8.2. Utilizar uma rede exclusiva para o heartbeat.

2.3.9. A solução deverá ser capaz de trabalhar no modo Ativo/Standby, com equipamento de mesmo fabricante;

2.3.10. A solução deverá ser capaz de trabalhar no modo Ativo/Ativo, mantendo o status das conexões;

2.3.11. Aceita-se como Ativo-Ativo a utilização de dois endereços Virtuais, onde cada endereço fica ativo em um elemento e e

2.3.12. A solução deve suportar múltiplas tabelas de rotas independentes;

2.3.13. O equipamento, quando habilitado para mais de uma função (Server Load Balancing (SLB), Aceleração Web, etc.), de memória) serão alocados para cada tipo de funcionalidade;

2.3.14. A solução deve possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos e

2.3.15. A solução deverá suportar e estar licenciado para todas as aplicações comuns de um Switch Layer 7 (sete):

2.3.15.1. Server Load-Balancing;

2.3.15.2. Firewall Load-Balancing;

2.3.15.3. Proxy Load-Balancing;

2.3.16. A solução deverá possuir recursos para balancear servidores do TRF6 com qualquer hardware, sistema operacional e t

2.3.17. Suportar Balanceamento apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cl

2.3.18. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego servidor real é enviada diretamente ao cliente;

2.3.19. A solução deve ser capaz de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests servidores e aumentando a performance do serviço;

2.3.20. A solução deve suportar e estar licenciado para os seguintes métodos de balanceamento para as aplicações do TRF6:

2.3.20.1. Round Robin;

2.3.20.2. Least Connections;

2.3.20.3. Weighted Percentage (por peso);

2.3.20.4. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;

2.3.21. Weighted Percentage dinâmico (baseado no número de conexões);

2.3.22. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI;

2.3.23. A solução deve ser capaz de balancear as novas sessões, preservando as sessões existentes no mesmo servidor e imp

2.3.23.1. Por cookie – inserção de um novo cookie na sessão;

2.3.23.2. Por cookie – utilização do valor do cookie da aplicação, sem adição de cookie;

2.3.23.3. Por endereço IP destino;

2.3.23.4. Por Endereço IP origem;

2.3.23.5. Por sessão SSL;

2.3.23.6. Através da análise da URL acessada;

2.3.23.7. Através da análise de qualquer parâmetro no header HTTP;

2.3.23.8. Através da análise de qualquer informação da porção de dados (camada 7);

2.3.24. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH ou utilizando algum protocolo ou sc

2.3.25. A solução deverá suportar os seguintes métodos de monitoramento dos servidores reais:

2.3.25.1. Layer 3 – ICMP;

2.3.25.2. Conexões TCP e UDP pela respectiva porta no servidor;

2.3.26. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, FTP, SMB, RADIU ser possível criar um monitor de forma manual;

2.3.27. A solução deverá possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico;

2.3.28. A solução deverá possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual;

2.3.29. A solução deverá possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores;

2.3.30. A solução deve possuir as seguintes funcionalidades de segurança ativas e licenciadas:

2.3.30.1. Network Address Translation (NAT);

2.3.30.2. Proteção contra Denial of Service (DoS);

2.3.30.3. Proteção contra Syn flood;

2.3.30.4. Implementar Listas de Controle de Acesso (ACL);

2.3.30.5. Permitir o controle da resposta ICMP por servidor virtual;

2.3.30.6. Realizar Limpeza de cabeçalho HTTP;

2.3.30.7. Análise em Camada 7 de Protocolos, com alertas para violações na camada de Protocolo HTTP.

2.3.31. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao

2.3.32. Deve ser possível definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate);

2.3.33. Deve ser possível definir compressão especificamente para certos tipos de objetos;

2.3.34. A solução deve possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipam

2.3.35. A solução deve ser capaz de ser configurada para recriptografar em SSL a requisição ao enviar para o servidor, permit

2.3.36. Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem u

2.3.37. Possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais

2.3.38. Garantir que o recurso de cache possa ajustado em relação a quantidade de memória que será utilizada para armazer

2.3.39. Possuir a capacidade para determinar qual o tamanho máximo do objeto a ser cacheado;

2.3.40. Possuir a capacidade para determinar qual o tamanho do menor objeto a ser cacheado;

2.3.41. Possuir a capacidade para determinar a URI (Uniform Resource Identifiers) que deve ser cacheada;

2.3.42. Possuir a capacidade para ler, alterar e ignorar o parâmetro cache-control no cabeçalho HTTP;

2.3.43. Possuir a capacidade para inserir e alterar o parâmetro age header no cabeçalho HTTP;

2.3.44. Suporte a otimização do protocolo TCP para ajustes a parâmetros das conexões clientes e servidor;

2.3.45. A solução deve suportar Internet Content Adaptation Protocol (ICAP);

2.3.46. Deve ser capaz de realizar DHCP relay;

2.3.47. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas;

2.3.48. A Solução deve ter suporte a sFlow;

2.3.49. A solução deve ter suporte a, no mínimo, TLS 1.2, SHA 2 Cipher e SHA256 hash;

2.3.50. A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de de conexões do servidor ou do grupo de servidores;

2.3.51. Deve ser possível configurar o tamanho máximo da fila;

2.3.52. Deve ser possível configurar o tempo máximo de permanência na fila;

2.3.53. A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede;

2.3.54. A solução deve realizar Controle de Banda Dinâmico para grupos de aplicações e rede;

2.3.55. A solução deve realizar Controle de Banda baseado em domínio de roteamento;

2.3.56. A solução deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL;

2.3.57. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica

2.3.58. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para method, http-referer, http-set-cookie, http-status, http-uri e http-version;

2.3.59. Deve ser possível tomar as seguintes ações através dessas políticas:

2.3.59.1. Bloqueio de tráfego;

2.3.59.2. Reescrita e manipulação de URL;

2.3.59.3. Registro de tráfego (log);

2.3.59.4. Adição de informação no cabeçalho HTTP;

2.3.59.5. Redirecionamento do tráfego para um membro específico;

2.3.59.6. Selecionar uma política específica para Aplicação Web.

2.3.59.7. Deverá possuir inteligência artificial para detecção além das assinaturas pré-definidas.

2.4. Características de Proteção de Aplicações Web

2.4.1. A solução pode executar automaticamente varreduras de rede que permitem a descoberta de novos servidores e servic

2.4.2. A solução deve proteger a infraestrutura web das aplicações de ataques contra a camada de aplicação (Camada 7);

2.4.3. A solução deve fornecer a possibilidade de bloquear transações WEB de maneira preventiva, antes que elas cheguem v

2.4.4. Deve ser capaz de correlacionar eventos ou violações de políticas;

2.4.5. A solução deve detectar, alertar e bloquear opcionalmente, em tempo real, qualquer comportamento malicioso conheci

2.4.6. A solução deve ter um modo de aprendizado que permita definir quais ações são esperadas e aceitas pelos usuários;

2.4.7. No modo de aprendizado, o sistema deve aprender a estrutura e os elementos do aplicativo e essas informações deve
deve aprender sobre: Hosts válidos, URLs, parâmetros, cookies, tipo de conteúdo dos parâmetros;

2.4.8. No modo de aprendizado, deve aprender além do comportamento esperado do usuário e essas informações devem est
aprender sobre: Caracteres aceitos, tamanho do valor esperado;

2.4.9. O modo de aprendizagem pode ser ativado e desativado manualmente para estender o tempo de reconhecimento do p

2.4.10. O modo de aprendizagem deve poder permanecer ativo mesmo quando está em modo de proteção ou bloqueio
manualmente. De tal forma que a configuração de segurança positiva é atualizada automaticamente e constantemente;

2.4.11. Com relação a quaisquer ataques ou outra atividade não autorizada, a solução deve ser capaz de tomar as med
quarentena temporária ou bloquear o usuário do aplicativo, colocar em quarentena temporária ou bloquear o endereço IP de

2.4.12. A solução deve ter um conjunto de padrões correspondentes aos ataques conhecidos. Esta base de dados de padrões

2.4.13. A solução deve permitir a definição para as regras e alarmes, condições lógicas em que o alarme ou o bloqueio não s
de tempo definido e associado a um contexto de conexão definível;

2.4.14. A solução deve ter a capacidade de proteger os serviços Web com base no SOAP;

2.4.15. A solução deve ter a capacidade de receber e usar certificados e pares de chaves pública / privada para servidores da

2.4.16. A solução deve poder inspecionar e monitorar todos os dados HTTP/S do aplicativo, incluindo cabeçalhos HTTP, campo

2.4.17. A solução deve inspecionar as solicitações e as respostas HTTP/S;

2.4.18. A solução deve ser capaz de validar todos os tipos de dados inseridos, incluindo URLs, formulários, cookies, consultas,

2.4.19. A solução deve ser capaz de identificar o usuário do aplicativo da Web. A identificação deve persistir até que o usuário

2.4.20. A solução deve ser capaz de identificar e manter um registro das sessões da Web no nível do aplicativo, por meio de c

2.4.21. A solução deve ser capaz de aplicar uma correção virtual (virtual patching) para proteger as vulnerabilidades detectad
do mercado) para receber os seus resultados ou relatórios, interpretar e sugerir mudanças para aplicar como correção virtual,

2.4.22. A solução deve suportar a detecção de ferramentas de download automático, bots, scripts, etc. através da geração d
por trás;

2.4.23. A solução deve ser capaz de implementar controles anti-scrapping de forma nativa, permitindo bloquear tentativas au

2.4.24. A solução deve ser capaz de reconhecer IPs de fontes mal-intencionadas (como redes TOR, proxies anônimos, sites
atualizadas periodicamente e deve ser possível integrar políticas de segurança como um critério;

2.4.25. Ser capaz de diferenciar entre as requisições legítimas realizadas por usuários humanos das requisições realizadas po

2.4.26. A solução deve fornecer proteção automatizada para todas as vulnerabilidades expressas no OWASP Top 10;

2.4.27. A solução deve permitir a geração de exceções para as políticas de segurança de validação de protocolo por URL ou IP

2.4.28. A solução deve permitir a inspeção das conexões SSL (SSL v3, TLS v1) implementadas nos servidores da web. Para iss

2.4.29. A solução deve validar se o conteúdo e a duração do protocolo HTTP, incluindo os cabeçalhos, corpo e cookies, estão
Web (GET, POST, PUT, etc.);

2.4.30. A solução deve permitir ações e alertar para violações de protocolos inferiores ao aplicativo, incluindo inspeção de pac

2.4.31. A solução deve proteger os aplicativos da Web contra ataques comuns, como:

2.4.31.1. Injeção SQL (SQL Injection);

2.4.31.2. Injeção de LDAP (LDAP Injection);

2.4.31.3. Comando do SO (SO Commanding);

2.4.31.4. Injeção SSI (SSI Injection);

2.4.31.5. Inclusão remota de arquivos (Remote File Inclusion);

2.4.31.6. Mail Command Injection;

2.4.31.7. Injeção de XML (XML Injection);

2.4.31.8. Injeção Xpath (XPath Injection);

2.4.31.9. Injeção Xquery (XQuery Injection);

2.4.31.10. Cross Site Scripting (XSS);

2.4.31.11. Cross Web Request Forgery (CSRF);

2.4.31.12. Web Scrapping;

2.4.31.13. Navegação forçada (Forceful Browsing).

2.4.32. Proteção de modificação de campos ocultos;

2.4.33. Permite a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas t

2.4.34. A solução deve suportar a definição de políticas diferentes que podem ser associadas a cada aplicativo individualment

2.4.35. Para cada aplicação protegida, o administrador deve ser capaz de configurar em que momento é feita a detecção (log

2.4.36. Para cada aplicativo da Web, deve ser possível desabilitar a prevenção de ataques (bloqueio) e deixar apenas a detec

2.4.37. No caso de um bloqueio, dependendo do modo de operação, a resposta (página) enviada ao usuário deve poder ser pe

2.4.38. A solução deve permitir que hosts ou clientes confiáveis sejam excluídos das medidas de proteção;

2.4.39. A solução deve suportar a identificação do IP de origem no caso de passar por proxy, interpretando o campo X-forward

2.4.40. A solução deve validar se o conteúdo e a duração do protocolo HTTP, incluindo os cabeçalhos, corpo e cookies, estão c

2.4.41. Deve possuir hardware dedicado para inspeção otimizada de tráfego criptografado com SSL e TLS;

2.4.42. A latência inserida no tráfego SSL não pode superar os 5ms (cinco milissegundos);

2.4.43. A solução deve suportar o uso de firewall camada 3 e 4 junto com firewall camada 7 no mesmo appliance para evitar p

2.4.44. A solução deve suportar responder por 1 endereço IP e vários endereços IPs por aplicação web;

2.4.45. Deve poder atuar como Web Application Firewall em modo WAF Positivo (permitindo apenas o que é conhecido e espe

2.4.46. Deve poder atuar como Web Application Firewall em modo WAF Negativo (bloqueando características conhecidas de a

2.4.47. Deve ser capaz de operar usando modelo positivo de segurança, por meio de aprendizado e de definição de regras d
tráfego que não coincide com essas regras (árvore de acesso válido);

2.4.48. Possuir as seguintes características:

2.4.48.1. Facilidade para liberação de regras aprendidas automaticamente que estejam gerando grande quantidade de fa

2.4.48.2. Facilidade para transformar um ataque detectado e considerado falso positivo como regra do firewall;

2.4.48.3. Facilidade para aplicar diferentes regras para diversas aplicações;

2.4.48.4. Capacidade para customizar regras de negação de serviço;

2.4.48.5. Capacidade para combinar detecção e prevenção na construção das regras;

2.4.48.6. Capacidade para desfazer a aplicação de uma regra.

2.4.49. Deve suportar o modelo de segurança positivo, devendo ser capaz de aprender qual perfil de tráfego é legítimo e bloq

2.4.50. Deve possuir políticas de segurança de aplicações web pré-configuradas na solução;

2.4.51. Deve permitir a criação de políticas diferenciadas por aplicação;

2.4.52. Deve possuir funcionalidade que ajuste dinamicamente o nível de proteção na detecção de ataques;

2.4.53. Deve ser possível utilizar uma política em múltiplas aplicações (uma para várias);

2.4.54. Deve ser possível utilizar uma política para cada aplicação (uma para uma);

2.4.55. Deverá possuir funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada a

2.4.56. O perfil aplicação aprendido de forma automatizada pode ser ajustado, editado ou bloqueado;

2.4.57. Deve identificar e criar um perfil de utilização das aplicações, mesmo que as páginas Web e conteúdos sejam dinâmic

2.4.58. Deve suportar WebSocket Traffic Filter;

2.4.59. Deve suportar o controle de política granular baseada no caminho do aplicativo (application path);

2.4.60. Deve permitir a aceitação de falsos positivos (exceção à política de segurança);

2.4.61. Deve permitir que ao detectar um falso positivo, o administrador aceite a requisição e atualize a política automaticam

2.4.62. Deve suportar a configuração de hosts confiáveis para permitir a execução de operações não permitidas pela política
de performance;

2.4.63. Deverá possuir proteção baseada em assinaturas para prover proteção contra-ataques conhecidos;

2.4.64. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção à re

2.4.65. As atualizações de assinaturas deverão passar por um período configurável de testes, onde nenhuma requisição que
não sendo necessário criar regras específicas a cada atualização de assinatura;

2.4.66. A solução deverá realizar bloqueios de ataques mesmo sem assinaturas atualizadas;

2.4.67. Deverá implementar consultas a bases de reputação externas;

2.4.68. A solução deve ser capaz de decifrar tráfego SSL a partir da importação de chaves criptográficas, para permitir a inspe

2.4.69. Inspeção de tráfego através da troca de chaves assimétricas entre cliente e WAF (proxy SSL);

2.4.70. A solução deve suportar SSL Offload de conexões;

2.4.71. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação. Essa inspeção poderá ser fe

2.4.72. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação;

2.4.73. Permitir a integração com Firewall de Database de outros fabricantes;

2.4.74. Deve possuir tecnologia de detecção de anomalias baseado nos IDs dos dispositivos, permitindo a detecção de DoS,
dispositivos;

2.4.75. A solução deverá permitir proteção contra envio de arquivos, considerando tamanho e tipo;

2.4.76. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar e aumentar a proteção

2.4.77. A solução deve se integrar com outras soluções de segurança como firewall, IPS e análise de logs de outros fabricante

2.4.78. Deverá armazenar os logs localmente ou exportar para Syslog server;

2.4.79. Possuir registro de logs com as seguintes características:

2.4.79.1. Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, en

2.4.79.2. Os registros de log de acesso e eventos devem ser armazenados em arquivo ou em banco de dados que pe
localmente ou carregados (upload) em servidor de log via FTP ou SCP ou armazenados em servidor externo de banco de

2.4.79.3. Permitir configurar a retenção dos logs por tempo e volume;

2.4.79.4. Ter capacidade para detecção, remoção ou codificação de dados sensíveis do log.

2.4.80. Deverá ser capaz de diferenciar acessos entre bots, Web scraping e usuários humanos para bloquear ataques automa

2.4.81. Deve oferecer um serviço baseado na reputação do endereço IP de origem, protegendo as aplicações de serem acessa

2.4.82. A Solução de Firewall de Aplicação deve suportar diferentes métodos de autenticação dos usuários das aplicações c Digest Authentication;

2.4.83. A solução deverá ser capaz de identificar e bloquear ataques através de:

2.4.83.1. Assinaturas, com atualização periódica da base pelo fabricante;

2.4.83.2. Regras de verificação personalizadas – política de segurança configurada;

2.4.83.3. Comportamento malicioso.

2.4.84. Deverá trabalhar com filtros de segurança:

2.4.84.1. De controle dos parâmetros das aplicações;

2.4.84.2. De proteção a sessão;

2.4.84.3. De controle de vulnerabilidades;

2.4.84.4. De controle de serviços Web;

6.2.4.84.5. De proteção a XML.

2.4.85. Permitir o bloqueio de ataques DoS/DDoS na camada 7, possuindo também a opção de apenas registrar o ataque, sem

2.4.86. Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS pois esses valores devem se

2.4.87. Possuir as seguintes formas de detecção de ataques DoS/DDoS na camada de aplicação:

2.4.87.1. Número de requisições por segundo enviados a uma URL específica;

2.4.87.2. Número de requisições por segundo enviados de um IP específico;

2.4.87.3. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportame

2.4.87.4. Número máximo de transações por segundo (TPS) de um determinado IP;

2.4.87.5. Aumento de um determinado percentual do número de transações por segundo (TPS);

2.4.87.6. Aumento do tempo de resposta (latência de aplicação) de uma determinada URL.

2.4.88. Deve permitir criar lista de exceção (whitelist) por endereço IP específico ou faixa de sub-rede;

2.4.89. Permitir a liberação temporária ou definitiva (whitelist) de endereços IP bloqueados por terem originados ataques dete

2.4.90. Deverá permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual;

2.4.91. Deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que

2.4.92. Permitir o bloqueio de determinados endereços IPs que ultrapassarem um número máximo de violações por minuto serão bloqueadas automaticamente;

2.4.93. A solução deve permitir o cadastro de robôs que podem acessar a aplicação;

2.4.94. Deve permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo c

2.4.95. Deve possuir mecanismo capaz de diferenciar entre bots e usuários humanos para bloquear ataques automatizados (r

2.4.95.1. O mecanismo deve implementar mecanismos de desafios de Cookies, JavaScript e Captcha para reforçar a iden

2.4.95.2. O mecanismo deve consultar base de dados de robôs já conhecidos; 4.108.3 O mecanismo deve permitir a inte

2.4.96. Deverá permitir adoção de critérios de decisão para bloqueio e alerta, considerando no mínimo 7 (sete) critérios simul

2.4.96.1. Tempo de resposta de uma página web;

2.4.96.2. Tamanho da resposta de uma página web;

2.4.96.3. User-agent (navegador);

2.4.96.4. Usuário;

2.4.96.5. IP de origem

2.4.96.6. País de origem

2.4.96.7. Assinatura de ataque;

2.4.96.8. Conteúdo do payload;

2.4.96.9. Conteúdo do cabeçalho;

2.4.96.10. Conteúdo do cookie;

2.4.96.11. Código de resposta do servidor web;

2.4.96.12. Nome do host (Host Header);

2.4.96.13. Número de ocorrências num intervalo de tempo;

2.4.96.14. Método HTTP;

2.4.96.15. Horário.

2.4.97. Ao detectar um ataque ou qualquer atividade não autorizada, deve ser possível bloquear:

2.4.97.1. Requisições e respostas;

2.4.97.2. Uma conexão TCP;

2.4.97.3. Uma rede específica;

2.4.97.4. Um endereço IP durante um intervalo de tempo específico.

2.4.98. A solução deve fornecer, para cada política de segurança, múltiplas opções de evento posteriores ao bloqueio da monitoração da gerência, executar um script definido pelo administrador e apresentar uma página de erro para o usuário;

2.4.99. Quando uma requisição for bloqueada pelo WAF, deve ser possível comunicar ao usuário sobre o fato através de u possível customizar a página HTML baseada em contextos como (Tipo de ataque, IP de Origem, Usuário e GeoLocalização) se

2.4.100. Deverá implementar proteção ao JSON (JavaScript Object Notation), REST (Representational State Transfer) e SOAP (S

2.4.101. Deverá implementar proteção a API;

2.4.102. Deverá implementar proteção WebSockets;

2.4.103. Deverá implementar proteção sobre microsservicos;

2.4.104. Deve possuir suporte a filtro e validação de funções XML específicas da aplicação;

2.4.105. Prevenir o vazamento de informações, permitindo o bloqueio ou a remoção dos dados confidenciais;

2.4.106. Deve prevenir que erros de aplicação ou infraestrutura sejam mostrados ao usuário;

2.4.107. A solução deverá permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle;

2.4.108. A solução deverá ser capaz de interpretar o campo X-Forwarded-For como endereço IP de origem original de um pac

2.4.109. Deverá proteger contra-ataques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs será

2.4.110. A Solução deverá proteger, no mínimo, contra os ataques listados abaixo:

2.4.110.1. AJAX/JSON web threats;

2.4.110.2. Anonymous Proxy access

2.4.110.3. Application tampering;

2.4.110.4. Broken access control;

2.4.110.5. Buffer overflow;

2.4.110.6. Cross-site scripting (XSS);

2.4.110.7. Known Worms;

2.4.110.8. Malicious Encoding;

2.4.110.9. SQL injection;

2.4.110.10. Web Services (XML) attacks

2.4.110.11. XML bombs/DoS;

2.4.110.12. Brute force;

2.4.110.13. Cookie Injection;

2.4.110.14. Cookie manipulation;

2.4.110.15. Cookie poisoning;

2.4.110.16. Cross site request forgery (CSRF);

2.4.110.17. Directory Traversal;

2.4.110.18. Forceful browsing;

2.4.110.19. Hidden fields manipulation;

2.4.110.20. HTTP Denial of Service;

2.4.110.21. HTTP Response Splitting;

2.4.110.22. Illegal Encoding;

2.4.110.23. Layer 7 DoS and DDoS;

2.4.110.24. Malicious Robots;

2.4.110.25. OS Command Injection;

2.4.110.26. Parameter and HPP tampering;

2.4.110.27. Remote File Inclusion;

2.4.110.28. Request smuggling;

2.4.110.29. Sensitive data Exposure;

2.4.110.30. Session hijacking;

2.4.110.31. Web scraping;

2.4.110.32. Web server software and operating system attacks;

2.4.111. Deverá mitigar ataques de Slow HTTP;

2.4.112. A solução deve possuir lista dinâmica de endereços IP globais com atividades maliciosas;

2.4.113. A solução deve encriptar dados e credenciais na camada de aplicação, sem ter a necessidade de atualizar a aplicaçã

2.4.114. Essas informações devem ser encriptadas para proteger o login e as credenciais dos usuários e com isso os dados da

2.4.115. Deve ajudar a prevenir contra ataques de Credencial Stuffing, onde bases de credenciais expostas na Internet são us

2.4.116. A solução deverá ser capaz de inspecionar e bloquear solicitações XML, SOAP e HTTP (versões HTTP 1.0, 1.1 e 2.0);

2.4.117. A solução deverá fazer checagem de:

2.4.117.1. Consistência de formulários;

2.4.117.2. Do cabeçalho do “user-agent” para identificar clientes inválidos; 4.131.3 Métodos HTTP utilizados (GET, POST,

2.5. Gerenciamento

2.5.1. A solução deve ser gerenciada centralmente (configurações, controle e atualizações), através de interface web ou cons

2.5.2. Possuir acesso controlado e autenticado por usuário, sendo que para a administração da solução deve-se usar uma con

2.5.3. O controle de acesso deve permitir a configuração de acesso por perfil às funções de Administração e Configuração de

2.5.4. Fornecer visualização e ações diferenciadas por perfis de acesso.

2.5.5. Permitir a visualização de painéis (dashboards).

2.5.6. Apresentar painéis gráficos (dashboards) com indicativos de situações diversas.

2.5.7. Deve possibilitar a CONTRATANTE, por meio do console de gerência, consultas sobre desempenho, problemas, configur

2.5.8. Deve armazenar as informações de desempenho do ambiente por um período mínimo de 30 (trinta) dias, manter informações dos elementos gerenciados deve ser de 05 (cinco) minutos, contendo no mínimo as seguintes informações:

2.5.8.1. Total de disponibilidade da Plataforma para um período mínimo 30 dias Por URL; Por conjunto de URL; Para todas

2.5.9. Deve possibilitar a geração de relatórios a qualquer tempo com as seguintes informações:

2.5.9.1. Total de GB (Gigabyte) consumido por domínio

2.5.9.2. Total de GB (Gigabyte) consumido no mês por todos os domínios;

2.5.9.3. Total de GB (Gigabyte) excedente, quando houver;

2.5.10. A solução deve permitir a emissão de relatórios gerenciais, conforme demanda da CONTRATANTE, com quantitativos e

2.5.11. A Plataforma deve possibilitar a consolidação de logs de toda a plataforma e seus recursos de forma global (todos os c

2.5.12. Armazenar em log a identificação de tentativas de ataques e eventos gerados pela Plataforma e seus recursos, com n

2.5.12.1. Endereços IP que originaram os ataques;

2.5.12.2. Horário do ataque;

2.5.12.3. Nome do ataque;

2.5.12.4. Qual campo foi atacado;

2.5.12.5. Quantas vezes esse ataque foi realizado;

2.5.12.6. Técnicas utilizadas;

2.5.12.7. Eventos detectados que apontem:

2.5.12.8. Comportamentos maliciosos;

2.5.12.9. Comportamentos suspeitos;

2.5.12.10. Exploits;

2.5.12.11. Correlações de eventos;

2.5.12.12. Acessos;

2.5.13. Deve permitir, para toda a Plataforma e soluções que a compõem, a retenção de logs consolidados a cada 5(cinco) mi

2.5.14. Deve prover a retenção de logs detalhados por no mínimo 72 (setenta e duas) horas, para toda a Plataforma e soluçõe

2.5.15. Deve permitir que os logs sejam rotacionados de forma que os registros mais antigos sejam apagados quando não hou

2.5.16. Deve possibilitar que por meio da console de gerência seja realizada a monitoração de logs e a investigação de logs;

2.5.17. Deve trabalhar com geolocalização para identificar a origem geográfica de um ataque;

2.5.18. Deve permitir exportar sob demanda os relatórios de logs em CSV;

2.5.19. Deve permitir o envio de logs para outros servidores de logs via syslog;

2.5.20. Deve permitir a configuração de alarmes personalizados, com base em investigações realizadas a partir dos logs;

2.5.21. Deve permitir apresentação dos dados consultados em vários formatos, incluindo tabela e gráficos;

2.5.22. Deve apresentar função de pesquisa por logs contendo no mínimo os seguintes critérios de pesquisa: Por dia, mês; Po

2.5.23. Deve permitir que sejam criados e aplicados filtros com base em qualquer característica do evento, tais como a origer

2.5.24. Deve possibilitar a geração de logs de auditoria detalhados, informando a configuração realizada, o administrador qu determinada regra foi usada (hits) em diferentes intervalos de tempo como dia, semana, mês ou intervalo customizável com auditoria;

2.5.27. Possibilitar a exportação de logs para provedores de armazenamento compatíveis com S3;

2.5.28. Possibilitar a exportação de logs através de requisições HTTP para endpoints personalizados;

2.5.29. O equipamento deve fazer backup diário em forma automática de todas as informações nele armazenadas, incluindo para um servidor remoto usando os protocolos SCP ou FTP;

2.5.30. Toda a configuração, administração e monitoramento da solução serão feitos através do console de administração;

2.5.31. A comunicação entre as estações de trabalho e o console de administração deve ser estabelecida através de um certificados digitais;

2.5.32. A solução de administração deve permitir a atribuição de perfis de administração pelos usuários e esses perfis devem

2.5.33. Capacidade de exportar logs para um formato SYSLOG ou SNMP TRAPS, para poder usar ferramentas de análise de ter

2.5.34. O gerenciador deve possuir controle de interface gráfica Web (GUI: Graphical user interface) e interface por linha de c

2.5.35. A interface gráfica de gerenciamento deve ser cross-platform, em Web via protocolo HTTP e HTTPS, com suporte a ace

2.5.36. Para interface gráfica do tipo Web, deve suportar no mínimo o navegador Mozilla Firefox e Chrome nas versões mais r

2.5.37. A interface por linha de comando (CLI) deve possibilitar configuração dos equipamentos;

2.5.38. Deve possuir auto complementação de comandos;

2.5.39. Deve permitir acesso via SSH, criptografado;

2.5.40. Possuir um comando que mostre o tráfego de utilização das interfaces (bps e/ou pps);

2.5.41. Permitir reinicialização do equipamento;

2.5.42. Implementar Debugging: CLI via console e SSH;

2.5.43. A solução de gerenciamento deve possuir, no mínimo, três níveis de usuários: Administrador; Usuário com permissões

2.5.44. A solução de WAF e a solução de balanceamento de carga entre aplicações web do TRF6 deverão permitir que mais c leitura/escrita;

2.5.45. A solução não deverá ter nenhum limite de licença para a quantidade de usuários ou dispositivos que poderão ser cc dos throughputs e quantidade de requisições solicitados;

2.5.46. Deverá permitir autenticação dos usuários em bases remotas como, no mínimo, Microsoft Active Directory, RADIUS e (

2.5.47. A interface gráfica de gerenciamento deverá permitir a atualização do sistema operacional e/ou a instalação de patche

2.5.48. Utilizar SCP ou HTTPS como mecanismo de transferência de arquivos de configuração e Sistema Operacional;

2.5.49. A interface Gráfica deverá permitir a reinicialização do equipamento;

2.5.50. A Solução de gerenciamento deve possuir uma única console que permita a organização, gerenciamento, configura equipamentos que compõem a solução de WAF com balanceamento;

2.5.51. A Gerência deve ter capacidade de obter e analisar eventos em tempo real;

2.5.52. A Solução de gerenciamento deve fornecer as seguintes funcionalidades no seu ambiente gráfico:

2.5.52.1. Adição, alteração ou remoção de aplicações a serem protegidas pelo firewall de proteção a aplicações Web;

2.5.52.2. Adição, alteração ou remoção de regras de balanceamento, aceleração e cache;

2.5.52.3. Obter e analisar eventos em tempo real e gerar relatórios durante a avaliação do tráfego;

2.5.52.4. Permitir utilizar as informações obtidas para refinar as políticas de segurança a qual gerou o evento;

2.5.52.5. Permitir a criação de listas de acesso baseadas em endereços IP. Deve ser possível definir os endereços IP de o

2.5.53. Deve manter internamente múltiplos arquivos de configurações do sistema;

2.5.54. Deve permitir a exportação e importação de regras e políticas para um novo dispositivo de forma simples;

2.5.55. Deve permitir o armazenamento de sua configuração em memória não volátil, no caso de uma queda e posterior resl de alimentação;

2.5.56. Deve suportar rollback de configuração e imagem;

2.5.57. Deve possuir ferramentas para depuração e gerenciamento em primeiro nível, tais como debug, traceroute, ping e log

2.5.58. O sistema operacional do dispositivo deverá permitir a utilização da ferramenta tcpdump, ou similar de qualidade permitindo que as capturas sejam armazenadas em formato libpcap;

2.5.59. A execução do tcpdump, ou ferramenta similar, não deve impactar no desempenho dos appliances. Permitir a definiçã

2.5.60. O armazenamento dos demais dias poderá ser local ou remoto;

2.5.61. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog;

2.5.62. Possuir agente de gerenciamento SNMP, MIB SNMP II, extensões MIB SNMP, MIB bridging (RFC 1493), que possua desc

2.5.63. Suporte ao protocolo NTP (Network Time Protocol) ou SNTP (Simple Network Time Protocol).

2.6. Capacitação Técnica

2.6.1. O treinamento deverá ser completo para contemplar a instalação, customização, operação e administração da solução e ao vivo;

2.6.2. O treinamento deverá ser ministrado para turma especifica para a CONTRATANTE;

2.6.3. Serão aceitos cursos oficiais do fabricante da solução;

2.6.4. Deverá possuir módulos teóricos e práticos;

2.6.5. Os instrutores devem ser certificados pelo fabricante da solução para o treinamento;

2.6.6. O conteúdo dos cursos deverá abranger, minimamente, os seguintes tópicos:

2.6.6.1. Configuração – acesso e navegação na solução; comando de configurações básicas e avançadas; estrutura/arqui

2.6.6.2. Operação e troubleshooting avançado – comandos de gerenciamento e monitoramento da saúde dos recursos d

2.6.7. É obrigatório relacionar a ementa dos cursos, carga horária e conteúdo programático. A abordagem do treinamento de participantes a empregar os recursos oferecidos;

2.6.8. Ao final do treinamento deve ser emitido certificado de conclusão para cada participante/aluno constando a carga horá

2.7. Software e Licenciamento

2.7.1. Todas as licenças que compõem a solução deverão ser de propriedade da CONTRATANTE e permitir a plena continuida

2.7.2. As assinaturas da solução de WAF devem ser atualizadas durante o período do contrato sem que seja necessário nenhu

2.8. Instalação e Configuração

2.8.1. O serviço de instalação e configuração deverá ser executado por técnico certificado pelo fabricante;

2.8.2. O serviço de instalação compreende as atividades de planejamento, instalação física, instalação lógica e finalização da

2.8.3. O serviço de configuração consiste em ajustar todos os parâmetros necessários (físicos e lógicos) para o funcionam requisitos dessa especificação.

2.9. Operação Assistida

2.9.1. A operação assistida deverá ocorrer durante 45 (quarenta e cinco) dias corridos a partir da instalação e configuração da

2.9.2. O serviço de operação assistida é composto por um conjunto de atividades que permitem o treinamento e a capacit corretiva, transferindo todo o conhecimento e experiência necessária para a operação da solução;

2.9.3. Durante os 45 dias corridos, será prestado todo o suporte necessário para a operacionalidade da solução, minimiz tecnologia envolvida em regime de treinamento enquanto trabalha, até que a CONTRATANTE possa assumir as atividades cor

2.9.4. Durante a operação assistida também será necessário realizar, pela CONTRADADA, possíveis customizações e ajustes f

2.9.5. Por padrão, a prestação da operação assistida ocorrerá presencialmente nas dependências da CONTRATANTE ou remot

2.10. Suporte, Manutenção e Atualização de Versão

2.10.1. O suporte técnico compreende o diagnóstico e identificação de problemas, apoio técnico na utilização, correção de módulo disponível de forma nativa na solução de WAF e balanceamento, ou decorrente de qualquer adaptação (customizaçã

2.10.2. O atendimento a um chamado de suporte deverá ocorrer por qualquer uma das seguintes formas: contato telefônico solução de WAF, com controle de acesso por senha;

2.10.3. O atendimento telefônico sempre que aplicável e viável, por meio de ligação local em Belo Horizonte/MG ou ligação i que compõem a solução de WAF;

2.10.4. A CONTRATANTE poderá efetuar um número ilimitado de chamados técnicos para a CONTRATADA, por qualquer uma

2.10.5. Na abertura ou registro de um chamado técnico, por qualquer uma das formas disponíveis, a CONTRATADA deverá in identificação completa do solicitante;

2.10.6. A CONTRATADA deverá retornar, via e-mail, a confirmação da abertura do chamado técnico, doravante denomi identificação do chamado, identificação do responsável da CONTRATADA pela abertura do chamado;

2.10.7. O atendimento ao chamado técnico pela CONTRATADA deverá ocorrer pelo menos por uma das seguintes formas fabricante da solução de WAF ou da CONTRATADA, presencial ou suporte por acesso remoto;

2.10.8. Caso acionado o suporte direto do fabricante, este deverá ter atendimento em português. Caso contrário, a CONTRAT

2.10.9. Um chamado técnico somente será considerado contingenciado ou concluído com o aceite da CONTRATANTE, na f sistema oferecido pela CONTRATADA, caso esta forma seja utilizada;

2.10.10. Após apresentar uma solução de contorno para o chamado técnico, a CONTRATADA deverá retornar, via e-mail, a c chamado, data e hora de conclusão do atendimento, descrição dos serviços executados e/ou da solução apresentada;

2.10.11. Em caso de adoção de solução de contorno, sem prejuízo da solução definitiva cabível, a CONTRATADA deverá emiti solucionar o problema de forma definitiva;

2.10.12. Após apresentar uma solução definitiva para o CHAMADO TÉCNICO, a CONTRATADA deverá retornar, via e-mail, a c chamado, data e hora de conclusão do atendimento, descrição dos serviços executados e/ou da solução apresentada;

2.10.13. Deverá ser garantido à CONTRATANTE o pleno acesso ao sítio (site) dos fabricantes dos produtos que compõem a disponíveis para seus usuários;

2.10.14. Caberá exclusivamente à CONTRATANTE a decisão de implantar ou não quaisquer atualizações de software fornecidc

2.10.15. A CONTRATADA deverá disponibilizar mecanismos para a atualização de software pelo download direto através da software em questão;

2.10.16. O serviço de manutenção consiste na correção de qualquer problema ou falha apresentados em componentes físicos

2.10.17. A atualização de software é uma alteração da versão anterior com o objetivo de implementar melhorias. Essas melhc

2.10.18. O prazo de atualização de todo software fornecido deve ser igual ao período de garantia do produto. Durante a vigên

2.11. Garantia

2.11.1. O(s) equipamento(s) que compõe(m) a solução devem estar em sua versão mais atual até a data de assinatura do cor solução;

2.11.2. O serviço de Garantia contempla garantir o correto e pleno funcionamento de todos os itens adquiridos necessários p contra novas vulnerabilidades e ameaças;

2.11.3. Prazo de garantia deverá ser de 60 meses.

3. LOTE 3. SERVIÇO DE SEGURANÇA DE BORDA (SERVICE SECURITY EDGE - SSE)

3.1. Características Gerais da Solução

3.1.1. O SSE deve possuir os seguintes componentes:

3.1.1.1. Acesso à Rede Zero Trust (ZTNA): O ZTNA;

3.1.1.2. Agente de segurança de acesso à nuvem (CASB);

3.1.1.3. Gateway seguro da web (SWG).

3.1.2. A solução deve ser fornecida com licenças para 4500 usuários, com validade de 60 meses, incluindo todas as funcional e a aplicativos para usuários remotos;

3.1.3. A solução deve ser construída com uma arquitetura nativa em nuvem e entregue como um serviço (SaaS), garantir usuários finais;

3.1.4. O serviço deve possuir infraestrutura de filtragem web (proxy) em datacenter localizado no território brasileiro, sendo p

3.1.5. A inspeção do conteúdo de conexões originadas no Brasil deve ser feita em datacenter dentro do território brasileiro;

3.1.6. Visando a disponibilidade e redundância do serviço, a CONTRATADA deverá oferecer em sua plataforma, pelo menos, 2

3.1.7. Todas as funcionalidades deverão ser ofertadas na nuvem como serviço. A nuvem deverá ser distribuída globalmente, ir

3.1.8. A solução deverá prover no mínimo 2 (dois) endereços exclusivos para TRF6 (/31) para acesso à Internet por datacente no Brasil;

3.1.9. O datacenter localizado no Brasil deverá ter conectividade redundante ao PTT (Ponto de Troca de Tráfego) no Brasil, pe Network) e provedores de nuvem pública tais como (AWS, Microsoft e Google). Desta forma, será possível garantir melhor exp

3.1.10. O datacenter do fabricante localizado no Brasil deve possuir, no mínimo, 2 (dois) links com velocidade superior a 50Gb

3.1.11. O fabricante deve possuir infraestrutura em território brasileiro, não sendo aceitas soluções como:

3.1.11.1. Virtualização de appliances em nuvens públicas;

3.1.11.2. Pontos de presença instalados em nuvens de terceiros como AWS, Azure, GCP e outros.

3.1.12. O datacenter do fabricante localizado em território nacional não deve armazenar as informações das transações em uma estrutura apartada de armazenamento de logs, que deverá ser prevista nesta contratação, através de conexões TLS seg

3.1.13. Não serão aceitos sistemas baseados em hardware ou software projetados para uso genérico, ou de código aberto *bpe*

3.1.13.1. Os elementos ofertados não podem ser customizados.

3.1.14. A solução deve oferecer uma interface de administração centralizada e intuitiva, permitindo o gerenciamento eficiente

3.1.15. O serviço deve garantir a disponibilidade mensal mínima de 99,7%, assegurando-se a máxima confiabilidade e tempo

3.1.16. É permitida a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de softwa

3.1.17. Deve consolidar múltiplos serviços de segurança para controle de acesso à Internet, como DNS, Secure Web Gateway

3.1.18. O agente instalado deve ser capaz de identificar quando estiver conectado à internet de maneira remota, ou por dentr

3.1.19. A solução não deve depender de cliente instalado na máquina do usuário. Para o acesso agentlesss, deve suportar, no

3.1.19.1. Web;

3.1.19.2. SSH;

3.1.19.3. RDP;

3.1.19.4. VNC, Team Viewer ou AnyDesk, entre outros.

3.1.20. Toda a comunicação entre o usuário e a plataforma deve ser realizada através de conexões TLS;

3.1.21. Deve ser compatível os seguintes provedores de identidade: Okta, Azure AD ou Active Directory / LDAP; SAML 2.0 Iden

3.1.22 Deve possuir base de inteligência do próprio fabricante, que inclua recursos de Inteligência Artificial (IA), estatístic ameaças e melhorar as taxas de resposta a incidentes;

3.1.23. A solução deve permitir a implementação de respostas automáticas ou guiadas a incidentes, minimizando o impacto d

3.1.24. A solução deve oferecer integração rápida com plataformas de comunicação como Slack e Microsoft Teams, facilitand

3.1.25. Deve ser compatível com plataformas de Information Event Management (SIEM) e Security Orchestration, Automatic incidentes;

3.1.26. O portal deve ser uma extensão da solução de Single Sign-On, permitindo que os usuários entrem uma única vez devendo também permitir a configuração de login único (SSO) para acesso através da integração com um provedor de ident Workspace.

3.1.27. A validação de postura para máquinas Windows deve contemplar pelo menos a validação de:

3.1.27.1. Antivírus instalado;

3.1.27.2. Certificados;

3.1.27.3. Processos em execução;

3.1.27.4. Versão de SO.

3.1.28. A validação de postura também deverá se aplicar ao acesso *agentless* (sem agentes), não apenas ao acesso com clien

3.1.29. A validação de postura para o acesso agentless deve comtemplar no mínimo as seguintes validações:

3.1.29.1. Data e hora de acesso;

3.1.29.2. IP;

3.1.29.3. Localização (País de acesso);

3.1.29.4. SO.

3.1.30. O client deve estar disponível para o seguintes Sistemas Operacionais:

3.1.30.1. Windows (exe e msi);

3.1.30.2. Linux (Ubuntu, Red Hat e Fedora);

3.1.30.3. Android / Chromebook;

3.1.30.4. iOS.

3.2. Módulo de Gerenciamento

3.2.1. Deve prover console em nuvem, para todas as funções próprias da solução sendo aceita composição de solução do mes

3.2.2. Deve permitir extrair logs a partir de soluções externas, como SIEM;

3.2.3. Deve possuir autenticação via protocolo SAML, permitindo integrar com provedores de serviços de identidade (IdP) para

3.2.4. Deve suportar APIs para gerenciamento com, no mínimo, as seguintes funcionalidades:

3.2.4.1. Autenticação;

3.2.4.2. Provisionamento;

3.2.4.3. Gestão de Políticas;

3.2.4.4. Relatórios.

3.2.5. Deve possuir ao menos três níveis de usuário: Administrador completo, Administrador de segurança e Apenas leitura;

3.2.6. Prover painel com informações sumarizadas de navegação de usuários contendo quantidade de sessões ativas e consu

3.2.6.1. A gerência centralizada e monitoração deve possibilitar a visualização dos logs de Firewall, navegação web e pre

3.2.6.2. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única inter

3.3. Segurança de Acesso - Política de Acesso

3.3.1. Deve usar o conceito de política de acesso unificada, sem políticas separadas para DNS, Secure Web Gateway (SWG);

3.3.2. Deve permitir ações de Bloqueio, Permissão, Alerta e Isolamento (Remote Browser Isolation);

3.3.3. Deve permitir a criação de páginas personalizadas de bloqueio e alerta, com opção de contato com administrador;

3.3.4. Deve permitir especificar origens a serem usadas na política de acesso internet, com base em:

3.3.4.1. Usuários/Grupos através de integração com Microsoft Active Directory ou provedores de identidade via SAML, tai

3.3.5. Deve permitir especificar destinos a serem usados na política de acesso internet, com base em:

3.3.5.1. Listas personalizadas de domínios, URLs, IPs/Redes, incluindo a capacidade de fazer o upload destas;

3.3.5.2. IP/Redes, Portas e Protocolos (Any, UDP, TCP, ICMP);

3.3.5.3. Categorias de conteúdo web ou listas personalizadas de categorias.

3.3.5.4. Aplicações ou listas personalizadas de aplicações.

3.3.6. Deve aplicar uma regra de acesso internet padrão e customizável, caso o fluxo não seja mapeado em outra regra;

3.3.7. Deve possuir contador de visitas (Hit count), indicando quantas vezes uma regra foi acionada.

3.4. Segurança de Acesso Internet - Camada DNS

3.4.1. Deve possuir infraestrutura global de resolução recursiva de DNS para proteção de acesso à internet;

3.4.2. Não deve ser uma solução para configuração, manutenção, implementação e serviço de DNS autoritativo;

3.4.3. Não deve ser uma solução para substituição de infraestrutura DNS interno, serviço DHCP;

3.4.4. Deve oferecer proteção para dispositivos de rede internos e externos;

3.4.5. Deve possuir suporte a IPv6 para DNS;

3.4.6. Deve permitir os seguintes métodos de envio de tráfego DNS:

3.4.6.1. Integração nativa com o sistema de DNS atual do ambiente de produção, substituindo as referências de servidor

3.4.7. Deve permitir visibilidade e controle de acesso a domínios, por meio de classificação por categorias;

3.4.8. Deve permitir a definição de listas personalizadas de acesso a domínios, para permissão (allow lists) e para bloqueio (bl

3.4.9. Deve ser capaz de identificar e bloquear requisições de acesso a domínios que estejam classificados, no mínimo, nas ca

3.4.9.1. Malware;

3.4.9.2. Command and Control (C&C);

3.4.9.3. Phishing;

3.4.9.4. DNS dinâmico;

3.4.9.5. Cryptomining;

3.4.9.6. Domínios novos ou vistos pela primeira vez, por, no mínimo, 24h;

3.4.9.7. DNS Tunneling;

3.4.9.8. Domínios suspeitos ou potencialmente maliciosos.

3.5. Gateway Seguro da Web - Secure Web Gateway (SWG)

3.5.1. A solução deverá identificar automaticamente tráfegos Web em portas não padrão (80 e 443) e realizar a inspeção mesmo em uma arquitetura de proxy transparente.

3.5.2. Deve permitir visibilidade e controle de acesso a URLs, por meio de classificação por categorias;

3.5.3. Deve permitir visibilidade e controle de acesso a URLs não categorizadas pelo fabricante;
3.5.4. Deve permitir a definição de listas personalizadas de acesso a domínios, URLs e IPs, para permitir (allow lists) e para bl
3.5.5. Deve suportar descriptografia TLS/HTTPS completa ou seletiva, com suporte a Certificate Authority (CA) do próprio clier
3.5.6. Deve permitir excluir categorias de conteúdo, aplicações e domínios do processo de descriptografia (descriptografia sel
3.5.7. Deve suportar descriptografia e inspeção de TLS 1.2 e 1.3;
3.5.8. Deve possuir recurso de antivírus/anti-malware para escaneamento de arquivos em trânsito;
3.5.9. Deve possuir mecanismo automático de envio de arquivos para malware sandboxing;
3.5.10. Deve permitir os seguintes métodos de envio de tráfego Secure Web Gateway(SWG):
3.5.10.1. Arquivo PAC (Proxy Auto-Configuration);
3.5.10.2. Túnel Ipsec;
3.5.10.3. Encaminhamento de tráfego com cliente para máquinas windows, macOS, linux e android;
3.5.11. Deve possuir controle granular (Upload e/ou Download) de aplicações web, suportando ao menos:
3.5.11.1. Box;
3.5.11.2. X (Twitter);
3.5.11.3. Dropbox;
3.5.11.4. Pinterest;
3.5.11.5. Messenger;
3.5.11.6. Gmail;
3.5.11.7. Facebook;
3.5.11.8. Linkedin;
3.5.11.9. Slack;
3.5.11.10. Instagram;
3.5.11.11. Google Drive;
3.5.11.12. SlideShare;
3.5.11.13. YouTube;
3.5.11.14. Vimeo;
3.5.11.15. WhatsApp;
3.5.11.16. SmartSheet;
3.5.11.17. Pastebin;
3.5.11.18. WeTransfer.
3.6. Agente de segurança de acesso à nuvem (CASB):
3.6.1. Deve ser capaz de monitorar a utilização de serviço em nuvem (Cloud Services) para identificar riscos e desenvolver ati
3.6.2. Deve possuir relatórios sobre a categoria do fornecedor, nome do aplicativo e volume de atividade para cada aplicativo
3.6.3. Deve incluir detalhes do aplicativo e informações de risco, como pontuação de reputação na Web, viabilidade financeira
3.6.4. Deve possuir capacidade de bloquear/permitir aplicativos específicos;
3.6.5. Deve possuir recurso de detecção, quarentena e/ou remoção de malware em aplicativos baseados em nuvem, via API, r
3.6.5.1. Dropbox;
3.6.5.2. Box;
3.6.5.3. Webex Teams;
3.6.5.4. Microsoft 365;
3.6.5.5. Google Drive.
3.6.6. Deve possuir opção de restrições de locatário (Tenant Controls) para permitir acesso apenas a instâncias de aplicativos
3.6.6.1. Microsoft 365;
3.6.6.2. Google G Suite;
3.6.6.3. Slack;
3.6.6.4. Dropbox.
3.7. Remote Browser Isolation (RBI)
3.7.1. Deve possuir funcionalidade de isolamento remoto de browser para proteção contra potenciais ameaças e malware, atr
3.7.2. A funcionalidade de RBI deve ser acionada como opção de ação a ser tomada nas regras para destinos e identidades se
3.7.3. A funcionalidade de RBI deve poder ser acionada para destinos considerados arriscados, como sites não categorizados
3.7.4. A funcionalidade de RBI deve poder ser acionada para qualquer destino, categoria ou aplicação suportada pelo serviço
3.7.5. O RBI deve suportar os seguintes navegadores:
3.7.5.1. Apple Safari;
3.7.5.2. Google Chrome;
3.7.5.3. Microsoft Edge;
3.7.5.4. Mozilla Firefox.
3.7.6. O RBI deve suportar autenticação de terceiros (ex. Dropbox usando Google para autenticação).
3.8. Data Loss Prevention (DLP)
3.8.1. Deve possuir camada múltipla de DLP para dados em trânsito (em tempo real) e em repouso (via API);
3.8.2. Deve permitir a classificação de dados sensíveis através de uso individual ou combinado de dicionários pré- definidos e
3.8.3. Deve permitir a classificação de dados sensíveis através de dicionários personalizados com opção de termos, frases e p

3.8.4. Deve permitir configurar diferentes níveis de severidade por regra;
3.8.5. Deve permitir inspecionar os arquivos por nome, conteúdo ou ambos;
3.8.6. O DLP deve suportar, no mínimo, os seguintes tipos de arquivos:
3.8.7.1. Word .doc e .docx;
3.8.7.2. PDF;
3.8.7.3. RTF;
3.8.7.4. Excel .xls e .xlsx;
3.8.7.5. PowerPoint .ppt e .pptx;
3.8.7.6. OpenDocument presentation .odp;
3.8.7.7. OpenDocument sheet .ods;
3.8.7.8. OpenDocument word .oth;
3.8.7.9. E-mail;
3.8.7.10. CSV;
3.8.7.11. HTML/XML;
3.8.7.12. Texto .txt;
3.8.7.13. TSV;
3.8.7.14. URL.
3.8.8. O DLP para dados em trânsito deve ter opções de alerta e bloqueio para dados expostos em arquivos, formulários web
3.8.9. O DLP para dados em trânsito de suportar os seguintes tipos de formulários (forms):
3.8.9.1. JSON;
3.8.9.2. XML;
3.8.9.3. URL encoded;
3.8.9.4. Multipart form.
3.8.10. O DLP para dados em trânsito deve ter, no mínimo, os seguintes serviços para inspeção:
3.8.10.1. Box Cloud Storage;
3.8.10.2. ChatGPT;
3.8.10.3. Concur Invoice;
3.8.10.4. Confluence;
3.8.10.5. Dropbox;
3.8.10.6. Facebook Messenger;
3.8.10.7. Gmail;
3.8.10.8. Jira;
3.8.10.9. Linkedin SlideShare;
3.8.10.10. Monday;
3.8.10.11. PasteBin;
3.8.10.12. SalesForce;
3.8.10.13. ServiceNow;
3.8.10.14. ShareFile;
3.8.10.15. Slack;
3.8.10.16. SmartSheet;
3.8.10.17. WeTransfer;
3.8.10.18. WorkDay;
3.8.10.19. Yahoo Mail.
3.8.11. Deve permitir especificar as identidades a serem usadas na política de DLP de dados em trânsito, com base em:
3.8.12. O DLP para dados em repouso deve permitir varredura de arquivos compartilhados, pelo menos, nas seguintes aplicaç
3.8.12.1. Microsoft 365 OneDrive e Sharepoint;
3.8.12.2. Microsoft Teams;
3.8.12.3. Google Drive e Meet.
3.8.13. O DLP para dados em repouso deve dar opções de ação de monitorar e revogar acesso;
3.8.14. O DLP para dados em repouso deve permitir especificar o escopo de varredura para todos os usuários ou usuários esp
3.9. Acesso à Rede Zero Trust (ZTNA)
3.9.1. Deve usar o conceito de política de acesso unificada, sem políticas separadas para ZTNA;
3.9.2. Deve permitir ações de Bloqueio e Permissão;
3.9.3. Deve permitir especificar origens a serem usadas na política de acesso privado, com base em:
3.9.3.1. Usuários/Grupos através de integração com Microsoft Active Directory ou provedores de identidade via SAML, tai
3.9.4. Deve permitir especificar destinos a serem usados na política de acesso a recursos privados, com base em:
3.9.4.1. Aplicações internas previamente configuradas, de forma individual ou global.
3.9.5. Deve permitir especificar requisitos de dispositivo de origem a serem usadas na política de acesso privado, com base e
3.9.5.1. Postura do dispositivo gerenciado ou não conforme política;
3.9.5.2. Requisitos de autenticação recorrente de usuário.
3.9.6. Deve aplicar uma regra padrão que negue acesso privado, caso o fluxo não seja mapeado em outra regra;

3.9.7. Deve possuir contador de visitas (Hit count), indicando quantas vezes uma regra foi acionada;

3.9.8. Deve permitir habilitar e desabilitar regras individualmente;

3.9.9. Suportar descriptografia para inspeção de tráfego privado.

3.10. Conector de recursos privados do ZTNA

3.10.1. A solução deve possibilitar conexões rápidas e seguras a redes e aplicações privadas, por meio de máquinas virtuai Deve ser possível instalar nos ambientes:

3.10.1.1. On-premises através de uma imagem VMWare ESXi (ova);

3.10.1.2. Nuvem AWS;

3.10.1.3. Nuvem Azure;

3.10.1.4. Nuvem Google.

3.10.2. Deve ter a capacidade de suportar conexão DTLS e TLS;

3.10.2.1. Deve regredir para a conexão TLS, caso DTLS seja bloqueado;

3.10.3. Deve ter a capacidade de calcular o número de instâncias baseado no throughput de tráfego estimado;

3.11. ZTNA com Agente

3.11.1. Deve ter a capacidade de acessar recursos privados utilizando qualquer protocolo;

3.11.2. Deve permitir a aplicação de políticas de postura do usuário, incluindo os seguintes requisitos:

3.11.2.1. Verificação do sistema operacional e a versão;

3.11.2.2. Verificação de um agente de segurança no dispositivo;

3.11.2.3. Verificação de senha no dispositivo;

3.11.2.4. Verificação do navegador utilizado e sua versão.

3.11.3. Deve rotear o tráfego baseado no IP/FQDN da aplicação destino;

3.12. ZTNA sem Agente (via browser)

3.12.1. Deve ser possível acessar aplicações privadas sem agente instalado;

3.12.2. Deve ter a capacidade de gerar um FQDN resolvível publicamente;

3.12.3. Deve ter a capacidade de autenticação via SAML;

3.12.4. Deve ter a capacidade de prover conexão a recursos privados para dispositivos não gerenciados BYOD;

3.12.5. Deve ter a capacidade de selecionar os navegadores permitidos;

3.12.6. Deve ter a capacidade de selecionar os sistemas operacionais permitidos.

3.13. Painéis e Relatórios

3.13.1. Deve possuir painel de visão geral do ambiente, incluindo informações de, pelo menos:

3.13.1.1. Gráfico com volume de tráfego (total, enviado e recebido) agregado e por método de conexão no período selec

3.13.1.2. Atividade de segurança (solicitações e bloqueios) e principais categorias de segurança visitadas por dispositivo

3.13.1.3. Conexões de rede privada ZTNA ao longo do tempo, listando usuários com maior número de solicitações no per

3.13.1.4. Número de vezes que os aplicativos internos foram acessados, número de usuários que solicitaram acesso e o

3.13.1.5. Número de vezes que cada método de acesso (ZTNA com cliente, ZTNA sem cliente) foi utilizado e recursos int

3.13.2. Deve prover, no mínimo, os seguintes relatórios:

3.13.2.1. Todas as atividades de acesso durante um determinado período de tempo ajustável, relacionadas a segurança identidade usada no acesso, destino, categoria de segurança e categoria de conteúdo;

3.13.2.2. Todas as atividades de acesso relacionadas a segurança durante um determinado período de tempo ajustá categoria de segurança;

3.13.2.3. Visão sobre aplicativos Web descobertos (Shadow IT), indicando fornecedor, categoria, nome, volume de atividade

3.13.2.4. Destinos mais acessados num período determinado de tempo ajustável, relacionados a segurança ou não, com

categoria de segurança e categoria de conteúdo;

3.13.2.5. Categorias mais acessadas num período determinado de tempo ajustável, relacionadas a segurança ou não acesso;

3.13.2.6. Atividades executadas na console da solução, indicando usuário responsável, data e hora, IP de origem, área d

tempo e IP;

3.13.2.7. Visão geral dos arquivos maliciosos identificados nas plataformas SaaS integradas ao ambiente, indicando tota detecção, com filtros, no mínimo, por plataforma, nível de exposição, status e nome do arquivo. Deve possibilitar ações

3.13.2.8. Violações de dados (DLP) detectadas em tempo real e via API, indicando data e hora do evento, regra acionada API), ação tomada, severidade, aplicação, nível de exposição, identidade e hash de arquivos. Deve indicar, nos detalhes parte mais sensível do texto.

3.13.3. Todos os dados disponíveis para a consulta e criação de relatórios deverão residir no plano de gestão por, no mínimo,

3.13.4. Deve permitir exportar relatórios para arquivos CSV, JSON, HTML ou outro formato capaz de manipulação;

3.13.5. Deve permitir agendamento e envio automático de relatórios.

3.14. Monitoramento de Experiência Digital:

3.14.1. Deve incluir, de forma unificada na console administrativa, área para monitoramento de experiência digital com med na resolução de problemas e melhoria de produtividade;

3.14.2. Deve possuir, ao menos, os seguintes recursos de monitoramento:

3.14.2.1. Disponibilidade e desempenho de dispositivos em tempo real, indicando consumo de CPU, memória, disco, sina

3.14.2.2. Análise da rota de comunicação de dados entre os dispositivos de usuários até o serviço contratado;

3.14.2.3. Mapa da infraestrutura de rede, fornecendo informações sobre a distribuição geográfica, conectividade e situaç

3.14.2.4. Disponibilidade e desempenho do principal aplicativo de colaboração cadastrado, com opção para, pelo menos,

3.14.2.5. Desempenho e a disponibilidade de acesso aos aplicativos SaaS mais comuns, tais como AWS, Microsoft 365 e

3.15. Capacitação Técnica

3.15.1. O treinamento deverá ser completo para contemplar a instalação, customização, operação e administração da solu online e ao vivo;

3.15.2. O treinamento deverá ser ministrado para turma especifica para a CONTRATANTE;

3.15.3. Serão aceitos cursos oficiais do fabricante da solução.

3.16. Instalação e Configuração

3.16.1. O serviço de instalação e configuração deverá ser executado por técnico certificado pelo fabricante;

3.16.2. O serviço de instalação compreende as atividades de planejamento, instalação física, instalação lógica e finalização da

3.16.3. O serviço de configuração consiste em ajustar todos os parâmetros necessários (físicos e lógicos) para o funcionam requisitos dessa especificação.

3.17. Operação Assistida

3.17.1. A operação assistida deverá ocorrer durante 45 (quarenta e cinco) dias corridos a partir da instalação e configuração d

3.17.2. O serviço de operação assistida é composto por um conjunto de atividades que permitem o treinamento e a capacit corretiva, transferindo todo o conhecimento e experiência necessária para a operação da solução;

3.17.3. Durante os 45 dias corridos, será prestado todo o suporte necessário para a operacionalidade da solução, minimi tecnologia envolvida em regime de treinamento enquanto trabalha, até que a CONTRATANTE possa assumir as atividades cor

3.17.4. Durante a operação assistida também será necessário realizar, pela CONTRADADA, possíveis customizações e ajustes

3.17.5. Por padrão, a prestação da operação assistida ocorrerá presencialmente nas dependências da CONTRATANTE ou remo

3.18. Suporte, Manutenção e Atualização de Versão

3.18.1. O suporte técnico compreende o diagnóstico e identificação de problemas, apoio técnico na utilização, correção de módulo disponível de forma nativa efetuada pela CONTRATANTE;

3.18.2. O atendimento a um chamado de suporte deverá ocorrer por qualquer uma das seguintes formas: contato telefônico solução, com controle de acesso por senha;

3.18.3. A CONTRATANTE poderá efetuar um número ilimitado de chamados técnicos para a CONTRATADA, por qualquer uma d

3.18.4. Caso acionado o suporte direto do fabricante, este deverá ter atendimento em português. Caso contrário, a CONTRATA

b) Plano de Sustentação

1. O plano de sustentação tem como objeto permitir o funcionamento adequado e contínuo de ambiente crítico de Infraestrutura d

2. Recursos necessários à continuidade do negócio

2.1. Recursos Materiais

Recurso	Qtde.	Disponibilidade	Ação para c
Espaço	1	Entrega da Solução	Obter espaço para guarda dos novos equipamentos até que a troca seja efe Local para armazenar os equipamentos antigos até que seja feita o desfazir Espaço disponível no galpão.

2.2. Recursos Humanos

Função	Formação	Período	
Gestor e Fiscais do Contrato	Designados por Portaria	Assinatura do Contrato	Fazer reunião inicial com a CONTRATADA para alinhamento da execução contratual, apresentação da fatores que possam impactar a execução do objeto.
Fiscais Requisitantes e Técnicos		Da assinatura até o recebimento definitivo da solução	Repassar as informações técnicas para elaboração do plano de implantação. Receber o plano de implantação, analisar e propor as correções técnicas necessárias se for o caso. Aprovar o plano de implantação, com os ajustes propostos. Acompanhar a instalação da solução. Apoiar as comissões de recebimento quanto a quesitos técnicos.
Comissão de Recebimento Provisório		Recebimento	Controlar o prazo para entrega da solução. Receber e conferir os objetos entregues se em conformidade com a proposta aprovada. Emitir documentos de não conformidade, em caso de objetos divergentes. Emitir termo de recebimento provisório, identificando os bens entregues, cumprimento dos prazos co
Comissão de Recebimento Definitivo		Instalação, Configuração e Migração	Acompanhar e controlar os prazos contratados previstos para cada etapa de execução, até a emissão Fiscalizar o processo de instalação, configuração e migração. Emitir documentos de não conformidade, em caso de divergência observada. Acompanhar os testes de compatibilidade da solução com as especificações técnicas do Edital. Conferir, validar e aprovar os produtos e serviços executados. Atestar a instalação e configuração mediante emissão de Termo de Recebimento Definitivo.
Fiscais Requisitantes e Técnicos		Recebimento definitivo até fim de vigência do contrato	Acompanhar e fiscalizar a execução dos serviços e anotar em registro próprio todas as ocorrências re fatos que exijam medidas corretivas por parte da contratada. Determinar as datas e os horários para realização das manutenções, prevendo o mínimo de impacto Abrir chamados para solicitação de suporte. Analisar e verificar se os níveis de qualidade contratados foram alcançados e aplicar as glosas estipul
Gestor do Contrato		Vigência Contratual	Autorizar a aplicação das glosas/descontos propostas pelos fiscais. Encaminhar a documentação comprobatória de penalizações ou multas administrativas para os setor

2.3. Continuidade da Solução de TIC

2.3.1. A continuidade de prestação dos serviços de rede é um dos objetivos principais da contratação proposta.

Evento

Inexecução ou má prestação nos serviços de manutenção pela CONTRATADA
Falência da empresa ou rescisão por descumprimento de obrigações contratuais (inexecução total do contrato)
Encerramento normal do Contrato

2.4. Transição Contratual

2.4.1. Avaliação de Continuidade Contratual

Ação
Avaliar mensalmente os serviços prestados no período e os resultados obtidos, efetuando os descontos, desconsiderações e multas necessárias quando for resultados não conformes.
Acompanhar os serviços e exigir a transferência de conhecimento entre as equipes de colaboradores técnicos e a CONTRATADA.

2.4.2. Ações para Encerramento Contratual

Ação
Analisar a existência de atualização de versionamentos, fixes e evoluções dos softwares e hardwares da solução e solicitar as correções finais.
Executar a transferência de conhecimento entre as equipes de colaboradores técnicos do atual fornecedor de serviços para a nova CONTRATADA, de forma a minimizar a possibilidade de interrupção ou degradação na operação e prestação desses serviços no âmbito do TRF6.
Os custos de desmobilização para encerramento do contrato correrão por conta do TRF6.
Elaborar documentos e avisos para comunicar à SECTI e à SUINF que a Contratada não possuirá mais acesso para manutenção no ambiente do SECTI.
Efetuar o descadastramento das contas de serviço da contratada, impedindo acesso às instalações e equipamentos da SECTI.
Garantir que todas as manutenções previstas no plano até a data de encerramento do contrato sejam atualizadas.
Solicitar à administração a liberação da garantia contratual.

2.5. Estratégia de Independência

2.5.1. Transferência de conhecimento

Atividade	Forma de
Documentação do projeto da solução	Documentação atualizada do projeto da solução, compartilhada entre todos os integrantes da equipe.
Encontro de alinhamento Técnico	Realização de encontros técnicos, quando necessário, com a equipe técnica do CONTRATANTE responsável pela g

Procedimento de instalação e configuração	Todas as instalações, configurações e manutenções deverão ser registradas e documentadas em procedimentos i
Descrição das entregas de serviços	Todas as construções de produtos através da prestação de serviços deverão ser entregues acompanhadas de des
Relatório de atividades	Em todo atendimento para manutenções no ambiente, deverá ser entregue um relatório com a descrição da ativi
Direitos de Propriedade Intelectual	Todos os produtos advindos da execução contratual, não se limitando aos documentos descritivos da solução, dia exclusiva do TRF6. Tais produtos deverão ter tratamento confidencial por parte da CONTRATADA, que não poderá divulgá-los a terce

VIII - Justificativas para o parcelamento ou não da contratação

( ) Não se aplica em razão da licitação ser dispensável ou inexigível.

( ) Não é possível o parcelamento, pois trata-se de apenas 1 (um) item. (ADJUDICAÇÃO: MENOR PREÇO POR ITEM).

(X) É possível a contratação da solução de forma divisível observado o §2 do art. 40 da Lei n. 14.133/2021 (ADJUDICAÇÃO: MENOR PREÇO

( ) Todos ou alguns itens da solução devem ser agrupados para o fornecimento por um único fornecedor, observado o §3º do art. 40 da Lei n

(ADJUDICAÇÃO: MENOR PREÇO GLOBAL).

Justificativa:

Justifica-se a divisão do objeto em lotes em razão da interdependência entre os equipamentos e serviços que compõem o objeto da natureza específica e o seu caráter contínuo, aliada à alta criticidade e à complexidade da infraestrutura apoiada.

As melhores práticas na implantação de uma nova solução de segurança se baseiam na integração das soluções e serviços, que são i em termos de qualidade técnica, resultando assim, no perfeito atendimento dos princípios da celeridade, economicidade e eficiência.

O fracionamento da solução em itens avulsos poderia expor a diversos riscos a qualidade e a disponibilidade do ambiente tecnológicc fornecedor dentro do processo de execução dos serviços.

A definição de um lote único, por sua vez, impede a disputa entre fabricantes e prestadores com*know-how* para os lotes da presente co

Seguem abaixo algumas considerações técnicas adicionais para o parcelamento do objeto em lotes:

- A pesquisa de mercado identificou somente um fabricante capaz de atender a todo o objeto da contratação, logo a divisão por lotes po
- Quando analisado sob os aspectos técnicos, percebe-se o inter-relacionamento e a interdependência entre os serviços e equipament tênues, de início e término das repercussões entre um e outro. Destacam-se as metas de alcance de maturidade, alta disponibilidade aspectos distintos;
- Para a adequada execução dos serviços ora contratados é fundamental que esteja assegurada a unidade conceitual de todas as etap direcionado para o resultado esperado que é a disponibilidade do ambiente de infraestrutura de TI, incluídos todos os aspectos necessa
- A indivisibilidade do lote é imprescindível, pois tecnicamente e gerencialmente é inviável que os serviços sejam fornecidos por difer custo gerencial para gestão contratual, constituindo todos estes benefícios em vantajosidade técnica e economicidade;
- No tocante à economicidade, particionar em itens poderia impactar diretamente os custos globais da contratação, uma vez que a e diluição do custo do *overhead* administrativo por um maior número de profissionais alocados para atendimento dos serviços. A ges aumentariam também os custos indiretos com recursos humanos da CONTRATANTE a serem alocados para tal atividade;
- Contratar prestadores distintos para o fornecimento de produto e a execução dos serviços de um lote poderia trazer conflitos de respo parte da CONTRATANTE;
- Por tudo exposto e considerando a interdependência entre o itens e lotes determinados, entende-se incabível a reserva de cotas para conjunto do objeto a ser contratado.

Por tudo exposto e em virtude da especificidade do objeto, pode-se afirmar que é tecnicamente inadequado o seu desmembramento p em razão da falta de concorrência. Sob o ponto de vista econômico, não há elementos nos autos que permitam concluir que a adc vantajosos para o TRF6.

IX - Demonstrativo dos resultados pretendidos em termos de economicidade e de melhor aproveitamento dos recursos huma

Busca-se com a presente contratação:

a) Atualizar o parque tecnológico do TRF6;

b) Obter serviços de alta disponibilidade;

c) Aumentar a velocidade de operação entre os equipamentos;

d) Otimizar o desempenho da rede de dados;

e) Garantir a estabilidade operacional das comunicações do TRF6 e suas subseções judiciárias;

f) Aumentar a proteção de rede do TRF6, possibilitando a inspeção de tráfego com maior granularidade que a atualmente realizada

g) Melhorar o desempenho e eficácia no controle de acesso ao perímetro de rede através de equipamentos com níveis de processa

h) Aumentar a disponibilidade das aplicações, evitando o comprometimento da capacidade do firewall em eventuais situações de a

i) Possuir viabilidade para realizar futuras expansões da capacidade e granularidade da rede do Tribunal;

j) Possibilitar a ampliação da segmentação da rede com o objetivo de reduzir os riscos de segurança;

k) Aumento da resiliência em caso de ataques;

l) Diminuir o tempo de análise e resolução de problemas.

X - Providências a serem adotadas pela Administração previamente à celebração do contrato, inclusive quanto à capacitação

Não se aplica.

XI - Contratações correlatas e/ou interdependentes

Não se aplica.

XII - Descrição de possíveis impactos ambientais e respectivas medidas mitigadoras, incluídos requisitos de baixo consumo d de bens e refugos, quando aplicável

12.1. Critérios:

12.1.1. Tenho conhecimento de que: A fabricante e/ou distribuidora, e/ou importadora, e/ou comerciante e/ou consumidora deste obje Recursos Ambientais (CTF/APP)?

a) (X) Não. ( ) Sim. Identifique a(s) categoria(s) da Ficha Técnica de Enquadramento (FTE): _____

b) ( ) a fabricante, e/ou distribuidora, e/ou importadora, e/ou comerciante, e/ou consumidora deste objeto não se enquadra nas FTE

12.1.2. Os produtos/objetos são constituídos de material (marque quantos itens forem necessários):

( ) renovável ( ) reciclado ( ) atóxico ( ) biodegradável (X) não se aplica

12.1.3. Os objetos são considerados produtos perigosos, segundo a Gestão de Resíduos Sólidos do TRF6/SJMG:

(X) Não. ( ) Sim. Quais? _____

12.1.4. Os objetos da aquisição devem estar em conformidade com os seguintes regulamentos técnico/legal: (marque quantos itens for

( ) Etiqueta Nacional de Conservação de Energia

( ) Certificado de Conformidade de Potência Sonora de Produtos Eletrodomésticos

( ) Certificado de Vistoria de Veículo

( ) Ficha de Informações de Segurança de Produtos Químicos

( ) Documento de Origem Florestal

( ) Autorização para o Exercício da Atividade de Revenda de GLP

( ) Outro(s). Especificar: _____

12.1.5. Há outros critérios de sustentabilidade, além dos relacionados acima:

(X) Não. ( ) Sim. Descreva: _____

12.2. Deverão ser consideradas as diretivas do Plano de Logística Sustentável do TRF6, normativos internos e a legislação vigente.

12.2.1. A aquisição ou contratação demandará ou resultará em (marque quantos itens forem necessários)

(X) geração de resíduo.

( ) consumo de papel.

( ) consumo de outros materiais de expediente (caneta, grampos, clips, pastas etc).

( ) consumo de café ou açúcar.

( ) consumo de água mineral envasada.

( ) gastos com correspondências.

( ) instalação de computador ou impressora.

( ) aparelho de telefone fixo ou móvel.

(X) consumo de energia elétrica.

( ) consumo de água.

( ) serviços de engenharia (instalações elétricas, hidráulicas, ponto de rede, ponto de telefone, divisórias).

( ) obras civis (reforma ou construção de edificação).

( ) serviço de limpeza - aumento da área a ser limpa no TRF6.

( ) serviço de vigilância - aumento no número de postos.

( ) quantidade de veículos na frota do TRF6.

( ) gasto com contratos de veículos (manutenção, peças, insumos, seguro, lavagem, terceirização, exceto motorista).

( ) consumo de combustível.

( ) ação de qualidade de vida.

( ) ação de capacitação socioambiental.

( ) não demandará ou resultará em nenhum dos itens acima.

XIII - Posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina

Com base nas informações levantadas ao longo deste estudo técnico, declaramos que a solução apresentada é viável de pr
pela área demandante.

Certificamos que somos responsáveis pela elaboração do presente documento que compila os Estudos Técnicos Preliminares

Na redação foram observadas as diretrizes estabelecidas no Guia de Contratações de TIC, instituídas pela Resolução CNJ nº 4

13.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria TRF6-SECOF 10/2024 (0779055).

Responsáveis pela elaboração:

Integrante Requisitante	**Integrante Técnic**
Nome: Heli Lopes Rios Diretor da Subsecretaria de Infraestrutura - SUINF / SECTI Matrícula: TR 38	Nome: Arianne Caldeira do Carmo Diretora do Núcleo de Defesa Cibernética e Tratamento Informação - NUDCI Matrícula: TR 587
O presente planejamento está em conformidade com os requisitos técnicos necessários ao cumprimento do objeto e atende adequadamente às demandas previstos são compatíveis e caracterizam a economicidade.	

Responsável pela revisão, supervisão e controle de qualidade:

Autoridade Máxima da Área de TI
Nome: Daniel Santos Rodrigues Diretor da Secretaria de Tecnologia da Informação - SECTI/TRF6 Matrícula: TR 44
O presente planejamento está em conformidade com os requis cumprimento do objeto e atende adequadamente às demandas benefícios pretendidos são adequados, os riscos envolvidos sã previstos são compatíveis e caracterizam a economicidade, **pelo encaminho para prosseguimento da contratação**.

Documento assinado eletronicamente por **Heli Lopes Rios**, **Diretor(a) de Subsecretaria**, em 06/11/2024, às 13:30, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Arianne Caldeira do Carmo**, **Diretor(a) de Núcleo**, em 06/11/2024, às 13:33, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Fernanda Marília Gonçalves Caetano**, **Assessor(a) I**, em 06/11/2024, às 14:42, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Daniel Santos Rodrigues**, **Diretor(a) de Secretaria**, em 06/11/2024, às 15:18, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.trf6.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0990939** e o código CRC **AC2700C7**.