

Termo de Referência 138/2024

Informações Básicas

Número do artefato	UASG	Editado por	Atualizado em
138/2024	110001-SECRETARIA DE ADMINISTRAÇÃO	NELSON GONCALVES REZENDE	10/09/2024 10:55 (v 11.0)
Status	ASSINADO		

Outras informações

Categoria	Número da Contratação	Processo Administrativo
VII - contratações de tecnologia da informação e de comunicação/Bens de TIC		00094.000097/2024-34

1. Definição do objeto

1.1. Aquisição de solução de equipamentos Firewall de Aplicação Web - WAF, para proteção do perímetro da rede de dados, dos ativos de hardware e software e das aplicações Web da Presidência da República, com gerência centralizada, compreendendo fornecimento de equipamentos (appliances) e suas respectivas licenças de suporte e atualização, conforme quantidades e exigências estabelecidas neste Termo de Referência, resumido na tabela abaixo:

GRUPO	ITEM	DESCRIÇÃO/ESPECIFICAÇÃO	CATMAT	UNIDADE DE MEDIDA	QTDE	VALOR UNITÁRIO (R\$)	VALOR TOTAL (R\$)
Único	1	Solução de Firewall de Aplicação Web (Web Application Firewall), com 2 unidades F5 BIG IP R4800, com licenciamento Premium Service e License BEST Bundle, com BIG-IQ VE + BIG-IQ Data Collection Device (DCD) e com suporte técnico e garantia de 60 meses	481646/27090	SOLUÇÃO	1	4.551.175,12	4.551.175,12
	2	Serviço de instalação e configuração da Solução de firewall de aplicação Web	027111	SERVIÇO	1	113.560,51	113.560,51
	3	Treinamento da solução (8 participantes)	016837	SERVIÇO	1	139.000,00	139.000,00
TOTAL						4.803.735,63	4.803.735,63

- Obs.: Os valores apurados na tabela acima se encontram consignados na Cotação-Detalhado-041/2024, anexada ao processo SUPER nº 00094.000097/2024-34.
- 1.2. Os objetos desta contratação são caracterizados como comuns, pois suas especificações são usuais no mercado.
- 1.3. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.
- 1.4. O prazo de vigência da contratação é de 12 (doze) meses contados da assinatura do contrato, na forma do artigo 105 da Lei nº 14.133, de 2021, e conforme regramentos abaixo:

"Orientação Normativa AGU Nº 51, de 25 de abril de 2014: "A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.""

"ACÓRDÃO DE RELAÇÃO 1789/2005 - PRIMEIRA CÂMARA: Acórdão 1.8. atente para o cumprimento do art. 57 c/c o art. 69, § 2º do art. 73, da Lei nº 8666/93 que trata do prazo de duração dos contratos, no qual não deve ser incluído o período de vigência da garantia, uma vez que esse direito perdura após a execução do objeto do contrato (Decisão TCU nº 202/2002 - Primeira Câmara)."

- 1.5. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.
- 1.6. Detalhamento dos Bens, Soluções e Serviços
- 1.6.1. O detalhamento das especificações e características dos bens, soluções e serviços decorrentes, se encontram consignado no anexo do presente Termo de Referência, com a denominação de Especificações Técnicas (WAF).

2. Fundamentação da contratação

- 2.1. A Fundamentação da Contratação e de seus quantitativos encontra-se pormenorizada no **Item 3. Descrição da Necessidade**, no **Item 5. Necessidades de Negócio** e no **Item 8. Estimativa da Demanda - Quantidade de Bens e Serviços**, do Estudo Técnico Preliminar nº 25/2024, apêndice deste Termo de Referência.
- 2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2024 - 110001 - Secretaria de Administração, conforme detalhamento a seguir:
- I) ID PCA no PNCP: 00394411000109-0-000006/2024;
- II) Data de publicação no PNCP: 01/04/2024, atualização em 15/04/2024;
- III) Id do item no PCA: nº 207;
- IV) Classe/Grupo: 7050 - EQUIPAMENTOS DE REDE DE TIC - LOCAL E REMOTA;
- V) Identificador da Futura Contratação: 110001-90250/2023.
- 2.3. O objeto da contratação foi priorizada pelo CGD/PR, considerando a altíssima criticidade do serviço ao negócio das unidades da PR, e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação PDTIC/PR 2021-2022, que teve sua vigência prorrogada até 31/12/2024, por intermédio da Resolução nº 38, de 18 de dezembro de 2023, do Comitê de Governança Digital e Segurança da Informação, e se encontra alinhada da seguinte forma:

OBJETIVO ESTRATÉGICO		
ID	OBJETIVO ESTRATÉGICO DE TIC	DESCRIÇÃO DO OBJETIVO
OE08	Promover a inovação e a modernização da infraestrutura e serviços de TIC	Manter os recursos de infraestrutura atualizados, a fim de garantir a continuidade dos serviços de TIC e a disponibilidade dos recursos necessários ao cumprimento das metas institucionais, evitando a obsolescência de equipamentos críticos e a estagnação tecnológica

ALINHAMENTO AO PDTIC/PR 2021/2022				
ID	Necessidade de TIC	ID	Ação	Meta
N13	Elevar o nível de segurança dos ativos de informação da PR	A40	Implantar software de auditoria e análise de vulnerabilidade	Solução adquirida e implantada

Por tratar de oferta de serviços públicos digitais, o objeto da contratação será integrado à Plataforma Gov.br, nos termos do Decreto nº 8.936, de 19 de dezembro de 2016, e suas atualizações, de acordo com as especificações deste Termo de Referência.

3. Descrição da solução

3.1. A solução de segurança cibernética a ser contratada envolve a aquisição de equipamento do tipo firewall de próxima geração para prover as seguintes funcionalidades e controles de segurança:

- a) Filtro e inspeção de pacotes;
- b) Proteção contra malwares e ameaças cibernéticas;
- c) Proteção da rede interna contra ataques de negação de serviços;
- d) Prover sistema de prevenção de intrusos;
- e) Proteção contra ameaças avançadas;
- f) Proteção de perímetro da rede contra tentativas de invasões e de ataques maliciosos.

3.2. Solução de firewall de aplicações web (WAF), balanceador de carga e publicação DNS para prover as seguintes funcionalidades e controles de segurança:

- a) Filtro e inspeção de pacotes de camada 7;
- b) Balanceamento de carga das aplicações e DNS;
- c) Proteção contra ataques de camada 7;
- d) Publicação e balanceamento de DNS;
- e) Proteção Anti-DDoS.

3.2.1. A solução de firewall de aplicação Web - WAF, publicação e proteção de DNS e balanceador de carga proverá proteção contra ataques de camada de aplicação, DNS e de negação de serviços, além de publicar as aplicações da Presidência da República na Internet de forma otimizada e balancear o tráfego das aplicações entre os ativos de infraestrutura e rede da Presidência da República.

4. Requisitos da contratação

4.1. Necessidades de Negócio

4.1.1. Prover proteção contra-ataques que exploram vulnerabilidade das aplicações da Presidência da República.

4.1.2. Prover proteção contra-ataques na borda da rede da Presidência da República, por meio da inspeção do tráfego de entrada e saída da rede.

4.1.3. Alta disponibilidade das soluções de proteção da rede.

4.1.4. Garantir o acesso balanceado e otimizado às aplicações.

4.1.5. Prover performance e acesso seguro e confiável às aplicações.

4.1.6. Garantir a publicação na internet das aplicações da Presidência da República.

4.1.7. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).

4.1.8. Manter a integridade dos dados e das informações sensíveis dos sistemas da Presidência da República.

4.1.9. Melhorar o nível de qualidade de serviço das aplicações internas da Presidência da República.

4.1.10. Melhorar a experiência do usuário ao acessar os serviços da Presidência da República fora da rede interna.

4.1.11. Prover o acesso com segurança a rede corporativa dos empregados em trabalho remoto.

4.1.12. Atender à Política de Segurança da Informação nos Órgãos e Entidades da Administração Pública Federal.

4.1.13. Garantir a qualidade, o desempenho e a alta disponibilidade das informações e dos equipamentos da Presidência da República.

4.1.14. Garantir a continuidade dos serviços aos usuários da Presidência da República.

- 4.1.15. Manter a infraestrutura de alto desempenho adequada para o tráfego de informações e sistemas críticos de TIC.
- 4.1.16. Manter o licenciamento em conformidade com o parque tecnológico.
- 4.1.17. Manter o parque tecnológico atualizado e padronizado.
- 4.1.18. Obter atualizações, correções e evoluções durante o período de vigência do contrato.
- 4.1.19. Capacidade de suportar ataques e ajustar o ambiente para fazer frente as mudanças ou restabelecimento dos serviços de forma mais célere em caso de problemas na rede.
- 4.1.20. Prover escalabilidade, redundância e resiliência para os serviços de tecnologia da informação da Presidência da República.
- 4.1.21. Prover disponibilidade, integridade, confidencialidade e autenticidade dos dados e informações.

4.2. Necessidades Tecnológicas

- 4.2.1. Proteção do perímetro da rede, inspeção dos pacotes da rede local e de entrada e saída da rede de dados da Presidência da República.
- 4.2.2. Proteção contra-ataques que exploram vulnerabilidades em nível de aplicação.
- 4.2.3. Prover proteção granular contra-ataques da camada de aplicação.
- 4.2.4. Filtrar o conteúdo WEB e controle das aplicações.
- 4.2.5. Detecção e mitigação de tentativas de intrusão.
- 4.2.6. Proteção contra malwares.
- 4.2.7. Prover IPS (Intrusion Prevention System) para prevenção de intrusão.
- 4.2.8. Provisionar acesso externo seguro via VPN - Virtual Private Network.
- 4.2.9. Proporcionar túneis de conexão entre pontos da Presidência da República com tráfego de dados de forma criptografada.
- 4.2.10. Prover balanceamento de carga e de tráfego.
- 4.2.11. Prover publicação das aplicações.
- 4.2.12. Análise de tráfego criptografado.
- 4.2.13. Determinar de forma dinâmica o melhor caminho para tráfego entre os links de dados.
- 4.2.14. Proporcionar relatórios gerenciais de monitoramento e controle para os diversos tipos de ameaças.
- 4.2.15. Gerenciar as soluções de firewall de maneira centralizada, otimizando a administração de toda a solução.
- 4.2.16. Proteção contra-ataques, balanceamento e publicação de DNS.
- 4.2.17. Firewall de Aplicação Web - WAF.
 - 4.2.17.1. O WAF é um tipo de firewall criado para combater as ameaças que estão além das capacidades dos firewalls tradicionais. Ele cria uma barreira entre o seu serviço baseado na web e todo o resto da Internet, bloqueando e protegendo sua aplicação de ações criminosas, como manipulação de conteúdo exibido, conhecida como “pixação”, injeções indevidas em banco de dados de padrão SQL (Structured Query Language) ou simplesmente “SQL Injection”, determinados tipos de fraudes em acesso administrativo e várias outras espécies de ciberataques.

4.3. Requisitos sociais, ambientais e culturais

- 4.3.1. Os profissionais da CONTRATADA deverão trajar-se de maneira adequada, quando no ambiente da Presidência da República, e usar linguagem respeitosa e formal no trato com a Gestão e/ou Fiscalização Contratual, os dirigentes da Presidência da República e usuários, em consonância com as regras e normas internas.
- 4.3.2. Os serviços prestados pela CONTRATADA deverão pautar-se sempre no uso racional de recursos e equipamentos, de modo a evitar e prevenir o desperdício de insumos e material.

4.3.3. A CONTRATADA deverá atender, no que couber, os critérios de sustentabilidade ambiental previstos na Instrução Normativa SGD nº 94, de 23 de dezembro de 2022.

4.4. Requisitos de adequação do ambiente da Presidência da República para viabilizar a execução contratual

4.4.1. Será necessário disponibilizar espaço para acomodação dos equipamentos e acessórios na Coordenação de Centro de Dados, da Diretoria de Tecnologia, Anexo I, do Palácio do Planalto, Brasília/DF.

4.4.2. Os racks de equipamentos deverão ter um espaço de 1 U por equipamento e infraestrutura elétrica e de climatização necessária.

4.5. Requisitos de Capacitação

4.5.1. A transferência de conhecimento deve garantir que toda a informação gerada durante os processos de instalação e migração seja integralmente apresentada pela equipe da contratada, por meio de métodos expositivos, realização prática das atividades, apresentação de resumos, esquemas, relatórios ou qualquer outro documento que viabilize ou facilite a absorção da tecnologia do novo ambiente pela equipe da contratante.

4.6. Requisitos Legais

4.6.1. Deverão ser cumpridos os procedimentos, normas, modelos e regulamentos vigentes na Presidência da República.

4.6.2. O presente processo de contratação deve estar aderente à Constituição da República Federativa do Brasil de 1988 e as seguintes legislações vigentes:

4.6.2.1. Lei nº 14.133, de 1º de abril de 2021 (Nova Lei de Licitações).

4.6.2.2. Lei nº 13.709/2018: Lei Geral de proteção de Dados Pessoais - LGPD, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

4.6.2.3. Decreto nº 10.024, de 20 de setembro de 2019, regulamenta os novos procedimentos para realização do pregão eletrônico nas aquisições de bens e contratações de serviços comuns, inclusive serviços comuns de engenharia, bem como dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal.

4.6.2.4. Instrução Normativa nº 40, de 22 de maio de 2020, dispõe sobre a elaboração dos Estudos Técnicos Preliminares - ETP - para a aquisição de bens e a contratação de serviços e obras, no âmbito da Administração Pública federal direta, autárquica e fundacional, e sobre o Sistema ETP digital.

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

4.6.2.6. Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, estabelece o modelo de contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISIP do Poder Executivo Federal.

4.7. Subcontratação

4.7.1 Não será admitida a subcontratação para o Item 01 - Solução de Firewall de Aplicação Web (Web Application Firewall) e nem para o Item 02 - Serviço de instalação e configuração, do objeto do presente Termo de Referência.

5. Modelo de execução do objeto

5.1 Condições de Entrega e Critérios de Aceitação do Objeto

5.1.1. Os fornecimentos serão por abertura de Ordem de Serviço/Fornecimento (OS/OF).

5.1.2. O prazo da entrega será de até **90** (noventa) dias corridos a contar da abertura da Ordem de Serviço/Fornecimento. Os demais serviços deverão ser executados a contar 45 (quarenta e cinco) dias após a abertura das Ordens de Serviço, conforme modelo anexo ao presente termo.

5.1.3. Os equipamentos, deverão ser instalados em até 30 (trinta) dias a partir da data do recebimento provisório.

5.1.4. A entrega dos equipamentos deverá ser realizada para o seguinte endereço: Almoxarifado Central da Presidência da República, situado na Avenida N-2, Palácio do Planalto, CEP 70150-900, em Brasília-DF.

5.1.5. Os bens/produtos deverão ser aceitos, mediante elaboração de documento da seguinte forma:

a) Termo de Recebimento Provisório, conforme modelo anexo ao presente termo, no ato da entrega dos produtos e dos documentos fiscais, para posterior verificação da conformidade dos bens/produtos com a especificação exigida;

b) Termo de Recebimento Definitivo, conforme modelo anexo ao presente termo, verificado o cumprimento de todos os requisitos e de acordo com os critérios de aceitação definidos, a Presidência da República dará o aceite definitivo, no prazo de até 30 (trinta) dias úteis, contados do recebimento provisório.

5.1.6. Os bens/produtos serão recebidos provisoriamente no prazo de 15 (quinze) dias, pelo (a) responsável pelo acompanhamento e fiscalização do Contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta.

5.1.7. Após o recebimento provisório, a instalação deverá ser realizada pela Contratada, em conjunto com o corpo técnico da Presidência da República, dentro do prazo do item 5.1.3 deste Termo de Referência.

5.1.8. Os bens/produtos poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 (quinze) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

5.1.9. Os bens serão recebidos definitivamente, após instalação, configuração e implantação, conforme especificações técnicas deste Termo de Referência, mediante parecer do (a) responsável pelo acompanhamento e fiscalização do Contrato, em até 15 (quinze) dias após a execução do serviço por parte da Contratada.

5.1.10. Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento definitivo no dia do esgotamento do prazo.

5.1.11. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da contratada pelos prejuízos resultantes da incorreta execução do Contrato.

5.1.12. A garantia dos bens/produtos, será de, no mínimo, 60 (sessenta) meses, a partir da assinatura do Termo de Recebimento Definitivo dos objetos contratados.

5.1.13. Local da instalação:

5.1.13.1. Coordenação de Centro de Dados, Palácio do Planalto, Ed. Anexo I-A, sala 107, Praça dos Três Poderes, Brasília-DF, Telefones: (61) 3411-2159 ou (61) 3411-3450.

5.2. Garantia, manutenção e assistência técnica

5.2.1. A CONTRATADA deverá garantir a completa interoperabilidade e compatibilidade entre os produtos a serem adquiridos, o pleno funcionamento dos produtos, prestando o serviço de garantia remoto ou on-site (quando, a critério da CONTRATANTE, for necessário), durante o período de garantia, contados a partir da data de emissão do Termo de Recebimento Definitivo.

5.2.2. A CONTRATADA deve garantir o funcionamento dos equipamentos, considerados isoladamente ou interligados aos demais, de acordo com as características descritas nos manuais e nas especificações aplicáveis.

5.2.3. A CONTRATADA, no caso da atualização de equipamento para corrigir falhas apresentadas, deve se responsabilizar pelos custos envolvidos, inclusive eventuais trocas de hardware, cabendo à CONTRATANTE a emissão de documento fiscal ou equivalente necessário ao transporte do equipamento, quando for o caso.

5.3. Mecanismos formais de comunicação

5.3.1. Conforme art. 18, inciso III da Instrução Normativa SGD/ME nº 94/2022, a comunicação entre CONTRATANTE e CONTRATADA deverá ser formal e ocorrerá através dos seguintes mecanismos:

- a) Contrato e Termos Aditivos;
- b) Ordem de Serviço ou de Fornecimento de Bens;
- c) Termos de Recebimento;
- d) Cartas e Ofícios;

- e) Atas de reuniões;
- f) Chamados registrados na central de atendimento da CONTRATADA;
- g) E-mails institucionais ou corporativos;
- h) Demais documentos previstos no instrumento convocatório.

5.4. Manutenção de Sigilo e Normas de Segurança

5.4.1. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pelo Contratante a tais documentos.

5.4.2. O Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na Presidência da República, a ser assinado pelo representante legal da Contratada, e Termo de Ciência, a ser assinado por todos os profissionais da CONTRATADA diretamente envolvidos na contratação, encontram-se no anexo do presente Termo de Referência, com a denominação de Termo de Compromisso e Manutenção de Sigilo e Termo de Ciência.

6. Modelo de gestão do contrato

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

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

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

6.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.5. A execução do contrato deverá ser acompanhada e fiscalizada por gestor e fiscais, especialmente designados para representar a Presidência da República perante o contratado, cabendo zelar pela observância dos termos constantes do contrato, do edital, do termo de referência/projeto básico ou de instrumentos hábeis a substituí-los, assim como pela adoção das providências necessárias ao fiel cumprimento das cláusulas contratuais.

6.6. As atividades de gestão e fiscalização da execução contratual deverão ser realizadas de forma preventiva, rotineira e sistemática, podendo ser exercidas por servidores, equipe de fiscalização ou único servidor, desde que, no exercício dessas atribuições, fique assegurada a distinção dessas atividades e, em razão do volume de trabalho, não comprometa o desempenho de todas as ações relacionadas à gestão do contrato.

6.7. Na gestão e fiscalização da execução contratual, a equipe de fiscalização deverá utilizar os resultados da gestão de riscos para apoio à melhoria contínua do desempenho e dos processos de controle e gestão contratual.

6.8. O prazo inicial da prestação de serviços ou da entrega de bens poderá ser objeto de alterações, em caráter excepcional, devidamente justificado e mediante autorização da autoridade competente, desde que requerido pela contratada antes da data prevista para o seu início ou das respectivas etapas, cumpridas as formalidades exigidas na legislação.

6.9. A Administração, na análise do pedido de que trata o item anterior, deverá observar se o seu acolhimento não viola as regras do ato convocatório, a isonomia, o interesse público ou a qualidade da execução do objeto, devendo ficar registrados que os pagamentos serão realizados em conformidade com o objeto.

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

6.11. O registro das ocorrências, as comunicações entre as partes e demais documentos relacionados à execução do objeto deverão ser organizados em processo específico de fiscalização.

6.12. Para as contratações de serviço sob o regime de execução indireta, bem como para as aquisições e contratações de soluções de tecnologia da informação e comunicação realizadas pela Presidência da República, deverão ser observadas, respectivamente, as instruções normativas expedidas pelos órgãos centrais do Sistema de Serviços Gerais e do Sistema de Administração dos Recursos de Tecnologia da Informação.

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

Fiscalização

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

Fiscalização Técnica

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

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

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

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

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

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

Fiscalização Administrativa

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

6.16.1. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

Gestor do Contrato

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

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

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

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

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

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

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

7. Critérios de medição e pagamento

Recebimento do Objeto

7.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo (a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

7.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 5 (cinco) dias, a contar da notificação do Contratado, às suas custas, sem pré-juízo da aplicação das penalidades.

7.3. O recebimento definitivo ocorrerá no prazo de **10** (dez) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

7.4. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021, o prazo máximo para o recebimento definitivo será de até **15** (quinze) dias úteis.

7.5. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

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

7.7. O prazo para a solução, pelo Contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

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

Liquidação

7.9. Recebida as Notas Fiscais ou documentos de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

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

7.10. Para fins de liquidação, o setor competente deverá verificar se a(s) nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente apresentado(s) expressa(ão) os elementos necessários e essenciais do documento, tais como:

7.10.1. O prazo de validade;

7.10.2. A data da emissão;

7.10.3. Os dados do contrato e do órgão Contratante;

7.10.4. O período respectivo de execução do contrato;

7.10.5. O valor a pagar; e

7.10.6. Eventual destaque do valor de retenções tributárias cabíveis.

7.11. Havendo erro na apresentação da(s) nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o Contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante;

7.12. A(s) nota(s) fiscal(is) ou instrumento(s) de cobrança equivalente deverá(ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

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

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

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

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

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

Prazo de pagamento

7.18. O pagamento será efetuado no prazo de até **10 (dez)** dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

7.19. No caso de atraso pelo Contratante, os valores devidos ao Contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice de correção monetária.

Forma de pagamento

7.20. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.

7.21. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

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

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

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

Cessão de crédito

7.24. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na Instrução Normativa SEGES/ME nº 53, de 8 de julho de 2020, conforme as regras deste presente tópico.

7.25. As cessões de crédito não fiduciárias dependerão de prévia aprovação do Contratante.

7.26. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

7.27. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do Contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme o art. 12 da Lei nº 8.429, de 1992, tudo nos termos do Parecer JL-01, de 18 de maio de 2020.

7.28. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração (Instrução Normativa nº 53, de 8 de julho de 2020 e Anexos).

7.29. A cessão de crédito não afetará a execução do objeto Contratado, que continuará sob a integral responsabilidade do Contratado.

8. Critérios de seleção do fornecedor

Forma de seleção e critério de julgamento da proposta

8.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo **menor preço global**.

8.1.1. A utilização do critério de julgamento pelo menor preço global por grupo, se justifica tendo em vista a indivisibilidade do fornecimento das Soluções, que constitui uma única solução de TI, sem prejuízo à ampla participação de licitantes e à economicidade da contratação de uma mesma empresa.

8.1.2. No critério de julgamento do tipo "menor preço total do grupo" é necessária a oferta de preço em todos os itens que compõem o grupo, sendo que os preços ofertados de cada item serão avaliados individualmente, em relação ao respectivo preço estimado, para fins de aceitabilidade da proposta final.

8.2. Os serviços a serem contratados enquadram-se nos pressupostos do Decreto nº 9.507, de 21 de setembro de 2018, não se constituindo em quaisquer das atividades previstas no art. 3º do aludido decreto, cuja execução indireta é vedada.

8.3. A prestação dos serviços não gera vínculo empregatício entre os empregados da Contratada e a Administração Contratante, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

Forma de fornecimento

8.4. O fornecimento do objeto será integral.

Exigências de habilitação

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

Habilitação jurídica

8.6. **Pessoa física:** cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional.

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

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

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

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

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

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

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

8.14. Agricultor familiar: Declaração de Aptidão ao Pronaf – DAP ou DAP-P válida, ou, ainda, outros documentos definidos pela Secretaria Especial de Agricultura Familiar e do Desenvolvimento Agrário, nos termos do art. 4º, §2º do Decreto nº 10.880, de 2 de dezembro de 2021.

8.15. Produtor Rural: matrícula no Cadastro Específico do INSS – CEI, que comprove a qualificação como produtor rural pessoa física, nos termos da Instrução Normativa RFB n. 971, de 13 de novembro de 2009 (arts. 17 a 19 e 165).

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

Habilitação fiscal, social e trabalhista

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

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

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

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

8.21. Prova de inscrição no cadastro de contribuintes estadual/distrital relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual.

8.22. Prova de regularidade com a Fazenda estadual/distrital do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre.

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

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

Qualificação Econômico-Financeira

8.25. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples.

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

8.27. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando.

8.27.1. Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um).

8.27.2. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura.

8.27.3. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.

8.27.4. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.

8.28. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação patrimônio líquido de 10% (dez por cento) do valor estimado da contratação.

8.29. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

Qualificação Técnica

8.30. Atestado(s) de capacidade técnica contendo nome completo, endereço, telefone, e-mail e CPF do emitente, data da emissão, objeto do serviço, número do contrato e a qualidade do serviço oferecido, fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) que a empresa LICITANTE tenha fornecido solução de natureza compatível com o objeto ora licitado, que permita estabelecer por comparação de características funcionais, técnicas, dimensionais e qualitativas com o objeto da presente licitação. A Presidência da República reserva-se o direito de realizar diligências para confirmar as informações prestadas nos atestados apresentados.

8.30.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito ao fornecimento de Solução WAF, com gerencia centralizada.

8.30.2. Os atestados deverão referir-se a serviços prestados no âmbito de sua atividade econômica principal ou secundária especificados no contrato social vigente.

8.30.3. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 do Anexo VII-A da IN SEGES/MP n. 5, de 2017.

8.30.4. O licitante disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados apresentados, apresentando, dentre outros documentos, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foram prestados os serviços, consoante o disposto no item 10.10 do Anexo VII-A da IN SEGES/MP n. 5/2017.

8.31. A justificativa para se exigir atestado(s) de capacidade técnica, prende-se a necessidade de salvaguardar a Administração Pública quanto ao futuro contratado possuir aptidão suficiente para desempenhar a atividade objeto desta licitação, ou seja, que a entrega da Solução de Equipamentos Firewall de Aplicação Web (WAF) para a Presidência da República seja de qualidade e de acordo com as especificações técnicas desejadas (hardware, software, instalação, configuração e suporte)), conforme julgado do Superior Tribunal de Justiça (STJ):

“É de vital importância, no trato da coisa pública, a permanente perseguição ao binômio qualidade e eficiência, objetivando não só a garantir a segurança jurídica do contrato, mas também a consideração de certos fatores que integram a finalidade das licitações, máxime em se tratando daquelas de grande complexidade e de vulto financeiro tamanho que imponha ao administrador a elaboração de dispositivos, sempre em atenção à pedra de toque do ato administrativo - a lei - mas com dispositivos que busquem resguardar a Administração de aventureiros ou de licitantes de competência estrutural, administrativa e organizacional duvidosa.” - Recurso provido (Resp. nº 44.750-SP, rel. Ministro Francisco Falcão, 1ª T., unânime, DJ de 25.9.00)”

8.32. Poderia até ser considerada desídia da Diretoria de Tecnologia deixar de exigir a comprovação da capacitação técnica da empresa, face à complexidade do objeto envolvido, sob pena de, não raro, restar prejudicada a execução do objeto a contento, em prejuízo ao interesse público, do qual não se pode descuidar.

8,33, Não é razoável licitar o fornecimento de Solução de Equipamentos Firewall de Aplicação Web (WAF) sem ter experiência específica suficiente ao atendimento do fim desejado pela Administração, sob pena da licitante vencedora causar sérios danos ao Poder Público.

8.34. Portanto, a exigência de comprovação da execução de fornecimento similar ao da presente licitação, se faz necessário para demonstrar que o licitante tem aptidão para o desempenho da atividade objeto desta licitação, razão pela qual, ratificamos a inclusão do Item (Qualificação Técnica) e seus subitens, contendo as exigências mencionadas nos subitens acima.

9. Estimativas do Valor da Contratação

Valor (R\$): 4.803.735,63

9.1. O custo estimado total da contratação é de **R\$ 4.803.735,63** (quatro milhões, oitocentos e três mil setecentos e trinta e cinco reais e sessenta e três centavos), conforme custos unitários consignados na Cotação-Detalhado-041/2024, anexada ao processo SUPER nº **00094.000097/2024-34**.

9.2. Nos valores acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

10. Adequação orçamentária

10.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

10.2. A contratação será atendida pela seguinte dotação:

I) Gestão/Unidade: **110001/0001**;

II) Fonte de Recursos: **0100**;

III) Elemento de Despesa: **339040 - Serviços de Terceiros Pessoa Jurídica – TIC**;

10.3. Após aprovação deste Termo de Referência, será indicada disponibilidade orçamentária, através de Pré-Empenho, indicando os recursos necessários ou de outro documento comprobatório.

11. Obrigações da Contratante

11.1. Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos.

11.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência.

11.3. Notificar o Contratado, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas.

11.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado.

11.5. Comunicar a empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021.

11.6. Efetuar o pagamento ao Contratado do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência.

11.7. Aplicar ao Contratado as sanções previstas na lei e neste Contrato.

11.8. Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado.

11.9. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

11.9.1. A Administração terá o prazo de 10 (dez), a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

11.10. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 (trinta) dias.

11.11. Comunicar o Contratado na hipótese de posterior alteração do projeto pelo Contratante, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.

11.12. A Administração não responderá por quaisquer compromissos assumidos pelo Contratado com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato do Contratado, de seus empregados, prepostos ou subordinados.

12. Obrigações da Contratada

12.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas:

12.1.1. A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.

12.2. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II) e prestar todo esclarecimento ou informação por eles solicitados.

12.3. Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência.

12.4. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

12.5. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos.

12.6. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021.

12.7. Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT.

12.8. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao Contratante.

12.9. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

- 12.10. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.
- 12.11. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.
- 12.12. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.
- 12.13. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.
- 12.14. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.
- 12.15. Não permitir a utilização de qualquer trabalho do menor de dezesesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.
- 12.16. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para qualificação na contratação direta.
- 12.17. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116).
- 12.18. Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único).
- 12.19. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.
- 12.20. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021.
- 12.21. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante.

13. Infrações e Sanções Administrativas

13.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado que:

- a) der causa à inexecução parcial do contrato;
- b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) der causa à inexecução total do contrato;
- d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

13.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:

13.2.1. Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

13.2.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima deste Termo de Referência, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021).

13.2.3. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima deste Termo de Referência, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

13.2.4. Multa:

13.2.4.1. Moratória de 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, limitada a incidência de 15 (quinze) dias corridos. O atraso superior a 15 (quinze) dias corridos autorizará a Administração a promover o rescisão do Contrato por inexecução total do objeto;

13.2.4.2. Compensatória de 5% (cinco por cento) sobre o valor adjudicado do contrato, no caso de inexecução parcial da obrigação assumida, prevista no do Termo de Referência;

13.2.4.3. Compensatória de 10% (dez por cento) sobre o valor adjudicado, por qualquer das infrações administrativas previstas no Termo de Referência;

13.2.4.4. Compensatória de 15% (quinze por cento) sobre o valor adjudicado, no caso de inexecução total do contrato, prevista no Termo de Referência. Em caso de inexecução parcial, a multa compensatória, no mesmo percentual das alíneas acima, serão aplicadas de forma proporcional à obrigação inadimplida.

13.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021).

13.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

13.4.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021);

13.4.2. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 20 (vinte) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

13.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

13.6. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

- a) A natureza e a gravidade da infração cometida;
- b) As peculiaridades do caso concreto;
- c) As circunstâncias agravantes ou atenuantes;
- d) Os danos que dela provierem para o Contratante;
- e) A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

13.7. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

13.8. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021).

13.9. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021).

13.10. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

13.11. Os débitos do contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

14. Obrigações Pertinentes à LGPD

14.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

14.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

14.3. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

14.4. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

14.5. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

14.5.1. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

14.6. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

14.7. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

15. Do Reajuste

15.1. Os preços inicialmente contratados são fixos e irredutíveis no prazo de um ano contado da data da assinatura do contrato.

15.2. Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

15.3. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

15.4. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).

15.5. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).

15.6. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.

15.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.

15.8. O reajuste será realizado por apostilamento.

16. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

NELSON GONCALVES REZENDE

Integrante Requisitante



Assinou eletronicamente em 05/09/2024 às 16:32:48.

JAN CARLOS RODRIGUES TELES

Integrante Técnico



Assinou eletronicamente em 09/09/2024 às 08:53:06.

ROBSON MARTINS GUIMARAES DA SILVA

Integrante Técnico



Assinou eletronicamente em 09/09/2024 às 09:31:05.

FABRICIO DA SILVA GAMA

Integrante Administrativo



Assinou eletronicamente em 09/09/2024 às 14:43:55.

BRUNO PEREIRA PONTES

Autoridade competente



Assinou eletronicamente em 10/09/2024 às 10:55:31.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Termo de Recebimento Provisorio.pdf (458.06 KB)
- Anexo II - Termo de Recebimento Definitivo.pdf (465.51 KB)
- Anexo III - Termo de Ciencia.pdf (331.15 KB)
- Anexo IV - Termo de Compromisso e Manutencao de Sigilo.pdf (444.8 KB)
- Anexo V - Termo de Ordem de Servico ou Fornecimento de Bens.pdf (459.16 KB)
- Anexo VI - Especificacoes Tecnicas - WAF, vSegunda.pdf (678.66 KB)
- Anexo VII - Cotacao-Detalhado-41-2024, vDecimaPrimeira.pdf (1.66 MB)
- Anexo VIII - ETP25_2024, vAssinado.pdf (823.94 KB)

Anexo I - Termo de Recebimento Provisorio.pdf



PRESIDÊNCIA DA REPÚBLICA
Casa Civil
Secretaria-Executiva da Casa Civil
Secretaria de Administração
Diretoria de Tecnologia
Coordenação-Geral de Infraestrutura Tecnológica

ANEXO I
TERMO DE RECEBIMENTO PROVISÓRIO

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
dd/mm/aaaa	1.0	Primeira versão do documento	XXXXXXXXXXXXXXXXXX

ATENÇÃO!

< Os trechos marcados em vermelho neste documento são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessidade>.

< Conforme ACÓRDÃO 172/2021 – TCU -PLENÁRIO, os órgãos e entidades federais têm o dever legal de realizar o planejamento prévio de cada contratação de TIC, inclusive daquelas viabilizadas mediante adesão a ARPs, que vai além do mero preenchimento formal dos artefatos previstos na legislação>.

< Nas contratações de licenciamento de softwares, é imprescindível verificar se toda a documentação entregue pela contratada está completa e corresponde exatamente ao que foi especificado no TR. É fundamental certificar-se de que todas as licenças, suporte e/ou garantia entregues estejam de acordo com os part numbers especificados no TR>.

INTRODUÇÃO

O Termo de Recebimento Provisório declarará, de forma sumária, que as compras foram entregues, para verificação posterior da conformidade do material com as exigências contratuais, baseada nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato.

Referência: Inciso XXI, art. 2º, e alínea “i”, inciso II, art. 33 da IN SGD/ME Nº 94/2022.

1 – IDENTIFICAÇÃO			
CONTRATO/NOTA DE EMPENHO N°	xx/aaaa		
CONTRATADA	<Nome da Contratada>	CNPJ	xxxxxxxxxxxxx
N° DA OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		
2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S) E VOLUMES DE EXECUÇÃO			
SOLUÇÃO DE TIC			
<Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>			
ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	MÉTRICA	QUANTIDADE
1	<Descrição igual ao da OFB de abertura>	<Ex.: UNID.>	<n>
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...
...	...	...	...
TOTAL DE ITENS			

3 – RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea “i”, da IN SGD/ME nº 94/2022, por este instrumento ATESTO que os <bem (s) /produto(s)> correspondentes à <OFB> acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram entregues, estando sujeitos à avaliação específica para verificação do atendimento às demais exigências contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato.

Ressaltamos que o recebimento definitivo destes <bem (s)/produto(s)> ocorrerá somente após a verificação desses requisitos e das demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da **CONTRATADA**. Por fim, reitera-se que o objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

4 – ASSINATURA
FISCAL TÉCNICO
<Nome do Fiscal Técnico do Contrato> Matrícula: xxxxxx <Local>, <dia> de <mês> de <ano>.
PREPOSTO
<Nome do Preposto do Contrato> Matrícula: xxxxxx <Local>, <dia> de <mês> de <ano>.

Anexo II - Termo de Recebimento Definitivo.pdf



PRESIDÊNCIA DA REPÚBLICA
Casa Civil
Secretaria-Executiva da Casa Civil
Secretaria de Administração
Diretoria de Tecnologia
Coordenação-Geral de Infraestrutura Tecnológica

ANEXO II
TERMO DE RECEBIMENTO DEFINITIVO

HISTÓRICO DE REVISÕES

Data	Versão	Descrição	Autor
dd/mm/aaaa	1.0	Primeira versão do documento	XXXXXXXXXXXXXXXXXX

ATENÇÃO!

< Os trechos marcados em vermelho neste documento são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessidade>.

<Conforme ACÓRDÃO 172/2021 – TCU -PLENÁRIO, os órgãos e entidades federais têm o dever legal de realizar o planejamento prévio de cada contratação de TIC, inclusive daquelas viabilizadas mediante adesão a ARPs, que vai além do mero preen-chimento formal dos artefatos previstos na legislação>.

<Nas contratações de licenciamento de softwares, é imprescindível verificar se toda a documentação entregue pela contratada está completa e corresponde exatamente ao que foi especificado no TR. É fundamental certificar-se de que todas as licenças, suporte e/ou garantia entregues estejam de acordo com os part numbers especifica-dos no TR>.

INTRODUÇÃO

O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente avaliados e atendem às exigências contratuais, de acordo com os requisitos e critérios de aceitação estabelecidos.

Referência: Inciso XXII, Art. 2º e alínea “h” inciso I do art. 33, da IN SGD/ME Nº 94/2022.

1 – IDENTIFICAÇÃO

CONTRATO/NOTA DE EMPENHO N°	xx/aaaa		
CONTRATADA	<Nome da Contratada>	CNPJ	XXXXXXXXXXXX
N° DA OS/OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S) E VOLUMES DE EXECUÇÃO**SOLUÇÃO DE TIC**

<Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>

ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	MÉTRICA	QUANTIDADE
1	<Descrição igual ao da OFB de abertura>	<Ex.: UNID.>	<n>
...	...	...	...
...	...	...	...
TOTAL DE ITENS			

3 – ATESTE DE RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea “h”, da IN SGD/ME nº 94/2022, por este instrumento ATESTO/ATESTAMOS que o(s) <serviço(s)/ bem(s)> correspondentes à <OS/OFB> acima identificada foram <prestados/entregues> pela CONTRATADA e ATENDEM às exigências contratuais, discriminadas abaixo, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Contrato acima indicado.

ITEM	EXIGÊNCIA CONTRATUAL	ATENDIMENTO	OBSERVAÇÃO
1	<exigência contratual estabelecida no TR >		

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR
5 – ASSINATURA
GESTOR DO CONTRATO
<Nome do Gestor do Contrato> Matrícula: xxxxxxxx <Local>, <dia> de <mês> de <ano>.

<As seções seguintes podem constar em documento diverso, pois dizem respeito à autorização para o faturamento, a cargo do Gestor do Contrato, e a respectiva ciência do preposto quanto a esta autorização>.

6 – AUTORIZAÇÃO PARA FATURAMENTO
GESTOR DO CONTRATO
Nos termos da alínea “n”, inciso I, art. 33, da IN SGD/ME nº 94/2022, AUTORIZA-SE a CONTRATADA a <faturar os serviços executados / apresentar as notas fiscais dos bens entregues> relativos à supracitada <OS/OFB>, no valor discriminado no item 4, acima. <Nome do Gestor do Contrato> Matrícula: xxxxxxxx <Local>, <dia> de <mês> de <ano>
7 – CIÊNCIA
PREPOSTO
<Nome do Preposto do Contrato> Matrícula: xxxxxxxx <Local>, <dia> de <mês> de <ano>

Anexo III - Termo de Ciencia.pdf



PRESIDÊNCIA DA REPÚBLICA
Casa Civil
Secretaria-Executiva da Casa Civil
Secretaria de Administração
Diretoria de Tecnologia
Coordenação-Geral de Infraestrutura Tecnológica

ANEXO III
TERMO DE CIÊNCIA

IDENTIFICAÇÃO DO CONTRATO	
Contrato nº:	
Objeto (resumido):	
Contratada: CNPJ:	
Gestor do Contrato: Matrícula:	
Preposto da Contratada: CPF:	
DECLARAÇÃO	
Pelo presente instrumento, o(s) funcionário(s) abaixo qualificado(s) e assinado(s) DECLARA(M) ter plena ciência e conhecimento do Termo de Compromisso e Manutenção de Sigilo firmado pela CONTRATADA, e da Política de Segurança da Informação e normas de segurança da Presidência da República – PR, bem como de sua(s) responsabilidade(s) no que concerne ao sigilo que deve ser mantido sobre as atividades desenvolvidas ou as ações realizadas no âmbito do Contrato Administrativo em epígrafe, bem como sobre todas as informações que eventualmente ou por força de sua(s) função(ões) venha(m) a tomar conhecimento, comprometendo-se a guardar o sigilo necessário nos termos da legislação aplicável e a prestar total obediência às normas de segurança da informação vigentes no ambiente da PR ou que venham a ser implantadas a qualquer tempo por este.	
LOCAL E DATA	
Local/UF, _____ de _____ de 20__.	
IDENTIFICAÇÃO E ASSINATURA DO(S) DECLARANTE(S)	
Nome: Identidade: CPF: Função/Cargo:	Assinatura:
Nome: Identidade: CPF: Função/Cargo:	Assinatura:
Observação: Este Termo deve ser impresso em papel timbrado da CONTRATADA.	

Anexo IV - Termo de Compromisso e Manutencao de Sigilo.pdf



PRESIDÊNCIA DA REPÚBLICA
Casa Civil
Secretaria-Executiva da Casa Civil
Secretaria de Administração
Diretoria de Tecnologia
Coordenação-Geral de Infraestrutura Tecnológica

ANEXO IV
TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

O NOME DO ÓRGÃO, sediado em ENDEREÇO, CNPJ nº CNPJ, doravante denominado CONTRATANTE, e, de outro lado, a NOME DA EMPRESA, sediada em ENDEREÇO, CNPJ nº CNPJ, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão do CONTRATO N.º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas do CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de

computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes;

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto – A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 156 da Lei nº 14.133, de 1º de abril de 2021.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

A CONTRATANTE elege o foro da CIDADE DA CONTRATANTE, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

DE ACORDO

CONTRATANTE	CONTRATADA
Nome: _____ Matrícula: _____	Nome: _____ Qualificação: _____

TESTEMUNHAS	
Testemunha 1	Testemunha 2
Nome: _____ Qualificação: _____	Nome: _____ Qualificação: _____

Local/UF, _____ de _____ de 20__.

**Anexo V - Termo de Ordem de Serviço ou
Fornecimento de Bens.pdf**



PRESIDÊNCIA DA REPÚBLICA
Casa Civil
Secretaria-Executiva da Casa Civil
Secretaria de Administração
Diretoria de Tecnologia
Coordenação-Geral de Infraestrutura Tecnológica

ANEXO V
TERMO DE ORDEM DE SERVIÇO
OU DE FORNECIMENTO DE BENS

ATENÇÃO!

< Os trechos marcados em vermelho neste documento são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessidade>.

< Conforme **ACÓRDÃO 172/2021 – TCU -PLENÁRIO**, os órgãos e entidades federais têm o dever legal de realizar o planejamento prévio de cada contratação de TIC, inclusive daquelas viabilizadas mediante adesão a ARPs, que vai além do mero preenchimento formal dos artefatos previstos na legislação>.

INTRODUÇÃO

Por intermédio da Ordem de Serviço (OS) ou Ordem de Fornecimento de Bens (OFB) será solicitado formalmente à Contratada a prestação de serviço ou o fornecimento de bens relativos ao objeto do contrato.

O encaminhamento das demandas deverá ser planejado visando a garantir que os prazos para entrega final de todos os bens e serviços estejam compreendidos dentro do prazo de vigência contratual.

(Referência: Art. 32 IN SGD Nº 94/2022)

1 – IDENTIFICAÇÃO

Nº da OS/OFB	xxxx/aaaa	Data de emissão	<dd/mm/aaaa>
CONTRATO/NOTA DE EMPENHO Nº	xx/aaaa		
Objeto do Contrato	<Descrição do objeto do contrato>		
Contratada	<Nome da contratada>	CNPJ	99.999.999/9999-99
Preposto	<Nome do preposto>		
Início vigência	<dd/mm/aaaa>	Fim vigência	<dd/mm/aaaa>

ÁREA REQUISITANTE

Unidade	< Sigla – Nome da unidade>		
Solicitante	<Nome do solicitante>	E-mail	xxxxxxxxxxxxxx

2 – ESPECIFICAÇÃO DOS BENS/SERVIÇOS E VOLUMES ESTIMADOS

Item	Descrição do bem ou serviço	Métrica	Valor unitário (R\$)	Qtde/Vol.	Valor Total (R\$)
1					
Valor total estimado da OS/OFB					
3 – <INSTRUÇÕES/ESPECIFICAÇÕES> COMPLEMENTARES					
<Incluir instruções complementares à execução da OS/OFB> <Ex.: Contatar a área solicitante para agendamento do horário de entrega> <Ex.: Conforme consta no Termo de Referência, o recebimento provisório está condicionado à entrega do código no ambiente de homologação, e a documentação do software no repositório oficial de gestão de projetos>					

4 – DATAS E PRAZOS PREVISTOS			
Data de Início:	<dd/mm/aaaa>	Data do Fim:	<dd/mm/aaaa>
CRONOGRAMA DE EXECUÇÃO/ENTREGA			
Item	Tarefa/entrega	Início	Fim
1		<dd/mm/aaaa>	<dd/mm/aaaa>
...		<dd/mm/aaaa>	<dd/mm/aaaa>

5 – ARTEFATOS / PRODUTOS	
Fornecidos	A serem gerados e/ou atualizados

5 – ASSINATURA E ENCAMINHAMENTO DA DEMANDA

Autoriza-se a <execução dos serviços / entrega dos bens> correspondentes à presente <OS/OFB>, no período e nos quantitativos acima identificados.

<Responsável pela Demanda/Fiscal Requisitante>

Matrícula: xxxxxx

<Local>, <dia> de <mês> de <ano>.

<Nome do Gestor do Contrato>

Matrícula: xxxxxx

<Local>, <dia> de <mês> de <ano>.

**Anexo VI - Especificacoes Tecnicas - WAF, vSegunda.
pdf**

Especificações Técnicas

1. ESPECIFICAÇÕES TÉCNICAS

1.1. Para comprovação dos itens das especificações técnicas da solução, serão aceitos datasheets, documentos e cartas do fabricante dos produtos ou ainda registros da CLI (Command Line Interface) dos produtos que asseverem o atendimento aos requisitos.

1.2. A solução é composta por um cluster contendo 2 (dois) equipamentos do tipo Web Application Firewall (WAF), gerência centralizada, incluindo o fornecimento de licenças, o fornecimento de transceivers, serviços de instalação, configuração, transferência de conhecimento, garantia e suporte técnico.

1.3. Há uma grande variedade de fabricantes de Web Application Firewall. Entretanto, é importante reforçar que há um alto grau de complexidade na administração e gerenciamento destas ferramentas, e a portabilidade entre elas não é uma tarefa fácil nem rápida. A Presidência da República dispõe atualmente de equipamentos da fabricante F5 Networks, e esta equipe de planejamento da contratação considera que se deve manter o fabricante para o melhor benefício de todos os usuários que acessam os serviços da Presidência da República.

1.4. Tendo em vista que o esforço realizado numa eventual migração de equipamento para um novo fabricante acarretará em um risco de total indisponibilidade de todos os portais e serviços hospedados no Centro de Dados da Presidência da República.

1.5. Não há qualquer tipo de cerceamento da competitividade na definição do fabricante F5 para a garantia do melhor interesse da Presidência da República e para a lisura e competitividade de um procedimento licitatório idôneo, uma vez que existem ao menos 11 representantes autorizados pela fabricante para oferecerem os equipamentos solicitados, conforme pode ser observado no site do próprio fabricante: <https://www.f5.com/partners/find-a-partner?partnerLocation=Brazil&partnerPage=1>, acessado em 31 de outubro de 2023.

2. CARACTERÍSTICAS DO HARDWARE QUE CONTEMPLAM AS SEGUINTE FUNCIONALIDADES

2.1.1. Os appliances físicos devem ser novos e de primeiro uso;

2.1.2. Os equipamentos devem ser fornecidos em modo appliance, com conjunto de hardware e software dedicados, não podendo ser servidor de uso genérico, e que atendam todas as funcionalidades descritas nas Especificações técnicas mínimas;

2.1.3. Devem ser novos, sem uso prévio e entregues em perfeito estado de funcionamento. Não devem ser remanufaturados, recondicionados ou possuir reparos de qualquer espécie;

2.1.4. Não serão aceitos equipamentos ou softwares que constem em anúncio ou lista do tipo end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, produtos que serão descontinuados, perderão suporte e garantia oficiais do fabricante;

2.1.5. As funcionalidades da solução (balanceador de carga, global server load balancing, proteção para aplicação, proteção para a rede, proteção contra-ataque DDoS, DNS Application Firewall, inspeção SSL, etc) deverão ser licenciadas pelo período de 60 (sessenta) meses;

2.1.6. Deverão ser fornecidos no mínimo 2 appliances para o uso em alta disponibilidade, cada um contemplando as seguintes características/funcionalidades:

2.1.2. Distribuição de carga e otimização das aplicações.

2.1.3. Proteção contra-ataques de aplicação.

2.2. O equipamento deverá ser novo, de primeiro uso e acondicionado adequadamente em caixa lacrada de fábrica, de forma a propiciar completa segurança durante o transporte.

2.3. Equipamento do tipo appliance, possuir altura de, no máximo, 2U, deve ser instalado em rack de 19" e vem acompanhado do kit de instalação.

2.4. Processador mínimo octa core.

2.5. Possuir quantidade total de memória (RAM) de, no mínimo, 64 GB (sessenta e quatro Gigabytes).

2.6. Possuir placa dedicada a tratar tráfego SSL (hardware).

2.7. Possuir, no mínimo, um disco com 480GB de espaço de armazenamento do tipo SSD.

2.8. Possuir no mínimo 2 fontes hot swappable.

2.9. Mínimo de 01 (uma) porta console para configuração através de CLI (Command Line Interface) para cada appliance.

2.10. Possuir 1 (uma) interface Gigabit Ethernet para gerenciamento out-of-band.

2.11. Possuir, no mínimo, 4 (quatro) interfaces 1 (um) Gigabit em cobre, seja através de portas nativas ou de slots SFP com os devidos transceivers 1000BASE-T.

2.12. Deve possuir no mínimo, por appliance, 4 portas 25/10/1 GbE SPF+/SFP28/SPF ou no mínimo 6 portas 1/10 GbE SFP/SFP+ que permita fazer agregação das interfaces para comunicação com switches, em ambos os casos incluindo todos os respectivos transceivers.

2.13. Todas as portas de fibras referenciadas no item anterior devem vir em cada appliance acompanhadas dos respectivos transceivers e de 04 (quatro) cordões ópticos padrão lc/lc de no mínimo 5 metros multimodo e 04 (quatro) cordões ópticos padrão lc/lc de no mínimo 10 metros multimodo.

2.14. Desempenho por appliance:

- 2.14.1. Possuir capacidade para operar, no mínimo, 50/40 Gbps de tráfego na camada L4/L7;
- 2.14.2. Possuir capacidade de operar, no mínimo, 45.000 TPS de tráfego SSL com chaves de 2048 bits;
- 2.14.3. Possuir capacidade de operar, no mínimo, 20.000 TPS de tráfego SSL com chaves ECDSA P-256;
- 2.14.4. Possuir capacidade de operar, no mínimo, 25 Gbps de tráfego SSL;
- 2.14.5. Possuir capacidade de operar, no mínimo, 1.8 milhão de requisições por segundo na camada 7;
- 2.14.6. Possuir capacidade de operar, no mínimo, 750 mil conexões por segundo na camada 4;
- 2.14.7. Possuir capacidade de operar, até 38 milhões de conexões concorrentes L4;
- 2.14.8. Possuir painel de LCD frontal com funções básicas;
- 2.14.9. Possuir Compressão de Hardware de no mínimo 30 Gbps em tráfego HTTP/HTTPS;
- 2.14.10. Recursos de agregação de portas baseado no protocolo LACP em seus modos ativo e passivo;
- 2.14.11. Deve suportar, até 3.500.000 (três milhões e quinhentos mil) requisições HTTP por segundo na camada 4 do modelo OSI;
- 2.14.12. Deve suportar, no mínimo, 80.000.000 (oitenta milhões) de pacotes SYN/segundo, sob ataque de SYN Flood.

3. CARACTERÍSTICAS GERAIS PARA A SOLUÇÃO

- 3.1. Suportar e garantir a instalação em ambiente de alta disponibilidade.
- 3.2. Assegurar que o equipamento deverá ser capaz de trabalhar no modo Ativo/Standby, com equipamento da mesma marca e modelo.
- 3.3. A solução deve operar no modo Ativo/Ativo, mantendo o status das conexões. Aceita-se como Ativo/Ativo a utilização de dois endereços Virtuais, onde cada endereço fica ativo em um elemento e standby no outro.
- 3.4. Assegurar que a operação da solução de 2 ou mais equipamentos, quando implementada em ambiente redundante suporte sincronismo de sessão entre os dois membros. A falha do equipamento principal não deverá causar a interrupção das sessões balanceadas.
- 3.5. A solução deve fornecer todos os recursos possíveis de redundância sem nenhuma despesa com licenças adicionais.

- 3.6. A solução deve possuir escalabilidade, podendo crescer na forma de cluster adicionando novos appliances inclusive de modelos diferentes.
- 3.7. O equipamento deverá possuir sistema operacional certificado ICSA Labs podendo assim ser instalado na borda antes de qualquer equipamento de segurança.
- 3.8. A solução deve fornecer recurso de agregação de portas baseado no protocolo LACP.
- 3.9. Deve possuir suporte a LACP em modo passivo e ativo.
- 3.10. A solução deve fornecer recurso para suportar até 32 portas em um mesmo conjunto agregado.
- 3.11. Deve possuir suporte a Spanning-Tree (802.1D), Fast Spanning-Tree (802.1w, 802.1t) e Multi Spanning-Tree (802.1s).
- 3.12. Deve fornecer recurso para o transporte de múltiplas VLAN por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q.
- 3.13. Possuir suporte a IPv6.
- 3.14. A solução deve suportar múltiplas tabelas de rotas independentes.
- 3.15. O equipamento, quando habilitado para mais de uma função deverá permitir a definição da importância da função, determinando quanta CPU e memória será alocada para cada tipo de funcionalidade.
- 3.16. Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos.
- 3.17. A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6.
- 3.18. Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado da solução e informações preventivas.
- 3.19. Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software Defined Network).
- 3.20. Serviço de suporte técnico na modalidade de 24x7 (24 horas/dia e 7 dias/semana) durante 60 meses.
- 3.21. Na data da proposta e durante a vigência do contrato, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale.

3.22. Deve se integrar com sistemas de gerenciamento de containers (ex.:Kubernetes/Openshift), de modo a permitir que mudanças dinâmicas na infraestrutura de microsserviços sejam refletidas automaticamente no balanceamento de entrada, aumentando ou diminuindo a quantidade de pods, e ainda, inserindo ou removendo serviços do Big-IP.

3.23. Deve ser integrado nativamente ao Kubernetes/Openshift para realizar obalanceamento entre pods.

3.24. Deve criar os serviços de Balanceamento de Carga dinamicamente ao mesmo tempo em que uma nova aplicação é provisionada pelo Kubernetes/Openshift.

4. FUNCIONALIDADE DE GERENCIAMENTO

4.1. Implementar uma configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento.

4.2. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol).

4.3. Permitir acesso in-band via SSH.

4.4. Manter internamente múltiplos arquivos de configurações do sistema.

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

4.6. Possuir auto-complementação de comandos na CLI.

4.7. Possuir ajuda contextual.

4.8. Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos.

4.9. Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura.

4.10. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados.

4.11. Deverá ser possível receber da base RADIUS, LDAP e TACACS+ o nível de acesso (Grupo ou Permissões).

4.12. Possuir Interface Gráfica via Web.

4.13. A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando.

- 4.14. A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot.
- 4.15. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps).
- 4.16. Suportar o rollback de configuração e imagem.
- 4.17. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema.
- 4.18. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog.
- 4.19. Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento.
- 4.20. A interface Gráfica deverá permitir a reinicialização do equipamento.
- 4.21. Reinicialização do equipamento por comando na CLI.
- 4.22. Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3.
- 4.23. Possuir traps SNMP.
- 4.24. Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events.
- 4.25. Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo.
- 4.26. Implementar Debugging: CLI via console e SSH.
- 4.27. Deve possuir suporte a Link Layer Discovery Protocol (LLDP).
- 4.28. Deve ser possível enviar, pelo menos, as seguintes informações via LLDP: Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size.
- 4.29. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas.
- 4.30. A Solução deve ter suporte a sFlow.

5. DISTRIBUIÇÃO DE CARGA E OTIMIZAÇÃO DAS APLICAÇÕES

- 5.1. Suportar todas as aplicações comuns de um Switch Layer 7, como:
 - 5.1.1. Server Load-Balancing;

5.1.2. Firewall Load-Balancing;

5.1.3. Proxy Load-Balancing.

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

5.3. A solução de Load Balance deve possuir, no mínimo, capacidade de resposta aos clientes por roteamento direto (os servidores balanceados respondem diretamente aos clientes), tunelamento (a solução é capaz de utilizar servidores de redes diferentes da que está inserida) ou fullproxy (todas as transações entre clientes e servidores são intermediadas pela solução).

5.4. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente.

5.5. Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede.

5.6. Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação.

5.7. A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.

5.8. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.

5.9. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.

5.10. Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço.

5.11. Suportar os seguintes métodos de balanceamento:

5.11.1. Round Robin;

5.11.2. Least Connections;

5.11.3. Weighted Percentage (por peso);

- 5.11.4. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;
- 5.11.5. Weighted Percentage dinâmico (baseado no número de conexões);
- 5.11.6. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI.
- 5.12. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web.
- 5.13. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:
 - 5.13.1. Por cookie: inserção de um novo cookie na sessão;
 - 5.13.2. Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;
 - 5.13.3. Por endereço IP destino;
 - 5.13.4. Por endereço IP origem;
 - 5.13.5. Por sessão SSL;
 - 5.13.6. Através da análise da URL acessada;
 - 5.13.7. Através da análise de qualquer parâmetro no header HTTP;
 - 5.13.8. Através da análise do MS Terminal Services Session (MSRDP);
 - 5.13.9. Através da análise do SIP Call ID ou Source IP;
 - 5.13.10. Através da análise de qualquer informação da porção de dados (camada 7).
- 5.14. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH.
- 5.15. O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:
 - 5.15.1. Layer 3 – ICMP;
 - 5.15.2. Conexões TCP e UDP pela respectiva porta no servidor;
 - 5.15.3. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP (em especial Microsoft AD), IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI.

- 5.16. Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY).
- 5.17. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real.
- 5.18. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual.
- 5.19. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores.
- 5.20. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico:
- 5.20.1. Realizar Network Address Translation (NAT);
 - 5.20.2. Realizar Proteção contra Denial of Service (DoS);
 - 5.20.3. Realizar Proteção contra Syn flood;
 - 5.20.4. Realizar Limpeza de cabeçalho HTTP.
- 5.21. A solução deve permitir o controle da resposta ICMP por servidor virtual.
- 5.22. Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração.
- 5.23. Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares.
- 5.24. Permitir a criação de Virtual Servers com endereço IPv4 e os servidores reais com endereços IPv6.
- 5.25. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente.
- 5.26. Deve permitir compressão tipo GZIP e Deflate.
- 5.27. Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate).
- 5.28. Possuir capacidade para definir compressão especificamente para certos tipos de objetos.
- 5.29. Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições HTTP são enviadas aos servidores sem criptografia.
- 5.30. Permitir a definição de quais tipos de objeto serão armazenados ou não em cache.
- 5.31. Permitir a reescrita de requisições HTTP baseado no conteúdo da URL, possibilitando o redirecionamento de requisições HTTP para HTTPS.

- 5.32. Permitir a reescrita de respostas HTTP, possibilitando a inclusão de cabeçalho (header) customizado.
- 5.33. Suportar multiplexação TCP e Reuso de Sessão para reaproveitamento e uso eficiente de conexões entre a solução de balanceamento de aplicações e os servidores balanceados.
- 5.34. Garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados sejam realizadas com aceleração em hardware, para não onerar o sistema, este item somente é válido para solução em appliance.
- 5.35. Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo “man in the middle”, ou seja, descriptografar, otimizar e re-criptografar o tráfego SSL em comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor. Caso haja falha na leitura da conexão SSL, esta deverá, se assim definido, prosseguir em regime de passthrough.
- 5.36. A solução deve possuir a funcionalidade de espelhamento de conexões SSL.
- 5.37. A solução deve possuir a capacidade de redirecionar o SSL Offload (troca de chaves) de determinado serviço para outro appliance físico que tenha mais capacidade para tratamento SSL. Dessa forma deve ser possível otimizar recursos executando tarefas que exigem muito desempenho para serem tratadas em hardware especializado.
- 5.38. Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado.
- 5.39. Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste edital devem estar disponíveis quando a conexão segura for estabelecida usando:
- 5.39.1. Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS.
- 5.39.2. Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;
- 5.39.3. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea.
- 5.40. Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS, a solução deverá ser capaz de:
- 5.40.1. Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;

5.40.2. Encaminhar ao servidor real via cabeçalho HTTP campos específicos do certificado digital utilizado pelo cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS.

5.41. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web.

5.42. Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições POP3, IMAP e SMTP são enviadas aos servidores sem criptografia.

5.43. A solução deve possuir diversos recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto na performance das aplicações. Dentre eles deve ser possível configurar parâmetros como:

5.43.1. SSL session cache Timeout;

5.43.2. Session Ticket;

5.43.3. OCSP (Online Certificate Status Protocol) Stapling;

5.43.4. Dynamic Record Sizing;

5.43.5. ALPN (Application Layer Protocol Negotiation);

5.43.6. Perfect Forward Secrecy.

5.44. Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores.

5.45. Possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados.

5.46. Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos.

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

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

5.49. Deve ser capaz de realizar DHCP relay.

5.50. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:

5.50.1. Tempo de resposta da aplicação;

5.50.2. Latência;

5.50.3. Conexões para conjunto de servidores, servidores individuais;

5.50.4. Por URL.

5.51. A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:

5.51.1. Servidores virtuais;

5.51.2. Servidores balanceados;

5.51.3. URLs;

5.51.4. Países de origem, baseados em geolocalização (GEOIP);

5.51.5. Dispositivos de origem do cliente (user agent).

5.52. Deve possuir framework unificado para configuração da aplicação.

5.53. Deve possuir criptografia IPSEC para comunicação entre os balanceadores.

5.54. Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS.

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

5.56. A Solução deve ter suporte a sFlow.

5.57. A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6.

5.58. A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6.

5.59. A solução deve suportar Equal Cost Multipath (ECMP).

5.60. A solução deve realizar Bidirectional Forward Detection (BFD).

5.61. A solução deve ter suporte a Stream Control Transmission Protocol (SCTP).

5.62. Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI).

5.63. A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação.

- 5.64. Suportar diversas cifras e protocolos SSL/TLS, incluindo TLS 1, 1.1, 1.2, 1.3, Forward Secrecy/Perfect Forward Secrecy, RSA, ECDSA, DHE, ECDHE, AES-128, AES-256, CBC/GCM, Camellia128, Camellia256, SHA, SHA2(SHA256/384) e Chacha20-Poly1305;
- 5.65. A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA.
- 5.66. A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. O balanceador não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores:
- 5.66.1. Deve ser possível configurar o tamanho máximo da fila;
 - 5.66.2. Deve ser possível configurar o tempo máximo de permanência na fila.
- 5.67. A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede.
- 5.68. A solução deve realizar Controle de Banda Dinâmico por aplicação e usuário.
- 5.69. A solução deve realizar Controle de Banda baseado em domínio de roteamento.
- 5.70. Permitir tráfego por parâmetros de QoS (Quality of Service) ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação. Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes. A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações.
- 5.71. A solução deve permitir a criação de túneis IP por domínio de roteamento utilizando GRE, IPIP, EtherIP, PPP.
- 5.72. A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP.
- 5.73. Deve fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server.
- 5.74. Possuir suporte ao protocolo SPDY e HTTP 2.0.
- 5.75. O equipamento deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL.
- 5.76. O equipamento deverá permitir a sincronização das configurações:
- 5.76.1. De forma automática;
 - 5.76.2. Manualmente, forçando a sincronização apenas no momento desejado.
- 5.77. Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:

5.77.1. Compartilhar a rede de heartbeat com a rede de dados; e

5.77.2. Utilizar uma rede exclusiva para o heartbeat.

5.78. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra-ataques.

5.79. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.

5.80. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.

5.81. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:

5.81.1. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-setcookie, http-status, http-uri e http-version.

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

5.82.1. Bloqueio de tráfego;

5.82.2. Reescrita e manipulação de URL;

5.82.3. Registro de tráfego (log);

5.82.4. Adição de informação no cabeçalho HTTP;

5.82.5. Redirecionamento do tráfego para um membro específico;

5.82.6. Selecionar uma política específica para Aplicação Web.

5.83. A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:

5.83.1. Endereço IP de origem.

5.84. A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:

5.84.1. Endereço IP de origem;

5.84.2. Porta TCP ou UDP de origem;

5.84.3. Endereço IP de destino;

5.84.4. Porta TCP ou UDP de destino;

5.84.5. Protocolo de camada 4 (TCP ou UDP);

5.84.6. Data e hora da mensagem;

5.84.7. URL acessada.

5.85. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory.

5.86. A solução deve suportar controle de versão da política de configuração de forma a permitir fazer roll back de políticas aplicadas.

5.87. A solução deve ser capaz de analisar a performance de aplicações web.

5.88. A solução deve possuir relatórios das aplicações.

5.89. Deve prover métricas de aplicações como: Transações por Segundo; Tempo de latência do cliente e servidor; Throughput de requisição e resposta; Sessões.

5.90. A solução deverá gerar informações para permitir análises históricas e auxiliar nos processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações.

5.91. As informações coletadas deverão permitir a análise dos dados por aplicações, por URL's, por clientes e por servidores, permitindo assim a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução.

5.92. A solução deverá gerar informações estatísticas de acesso identificando para cada aplicação os métodos de acesso HTTP (GET e Post), o tipo de sistema operacional utilizado pelos clientes, e os browsers utilizados.

5.93. A geração de informações históricas deverá permitir:

5.93.1. O detalhamento do tempo de resposta total de carregamento de uma URL e ou Página;

5.94. Permitir a correlação de métricas de uso de rede com o comportamento das aplicações.

6. PROTEÇÃO CONTRA-ATAQUES DE APLICAÇÃO

6.1. A solução deve operar nos modos ativo-ativo e ativo-standby.

6.2. O equipamento oferecido deverá proteger a infra-estrutura web de ataques contra a camada de aplicação (Camada 7).

- 6.3. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado.
- 6.4. Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS, pois esses valores devem ser auto-ajustáveis e adaptativos de acordo com mudanças.
- 6.5. A solução deve possuir a capacidade de automaticamente capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador.
- 6.6. A solução deve suportar o uso de firewall camada 3-4 junto com firewall camada 7 no mesmo equipamento/appliance para evitar problemas com o aumento da latência.
- 6.7. O equipamento oferecido deverá possuir a certificação ICSA para Firewall de Aplicação (Web Application Firewall).
- 6.8. Permitir a utilização de um modelo positivo de segurança para proteger contra-ataques conhecidos aos protocolos HTTP e HTTPS e às aplicações web acessíveis através destes.
- 6.9. Possuir política de segurança de aplicações web pré-configurada na solução.
- 6.10. Permitir a criação de novas regras com parâmetros e expressões regulares definidos pelo administrador.
- 6.11. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes.
- 6.12. Permitir a criação de políticas diferenciadas por aplicação.
- 6.13. Permite configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies.
- 6.14. A solução WAF deve, no mínimo, funcionar como proxy reverso de aplicações.
- 6.15. A solução WAF deve, no mínimo, permitir o mapeamento de diversas aplicações em um mesmo IP virtual, enviando informações para conjuntos de servidores diferentes de acordo com a URL requisitada.
- 6.16. A solução WAF deve, no mínimo, permitir o mapeamento em um mesmo IP virtual, de acordo com a URL requisitada, que exija certificado digital de cliente para algumas aplicações e não exija para outras.
- 6.17. A solução WAF deve, no mínimo, permitir a inclusão de parâmetros customizados nos cabeçalhos (headers) HTTP, além da alteração dos existentes, para envio à aplicação de destino.

- 6.18. A solução deverá se integrar a soluções de análise (Scanner) de vulnerabilidade do site. O resultado desta análise deve ser utilizado para configurar as políticas do equipamento.
- 6.19. A solução deve permitir a integração com soluções de análise de vulnerabilidades (Scanner) de terceiros.
- 6.20. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação. Essa inspeção pode ser feita via integração ICAP. Deve ser possível integrar com diferentes softwares de Antivírus.
- 6.21. Deve se integrar com o software de Antivírus existente no ambiente da CONTRATANTE.
- 6.22. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar e aumentar a proteção contra-ataques recentes.
- 6.23. Permitir a integração com Firewall de Database de outros fabricantes.
- 6.24. A solução deve se integrar com outras soluções de segurança e análise de logs de outros fabricantes.
- 6.25. Deve possuir tecnologia de detecção de anomalias baseado nos IDs dos dispositivos, permitindo a detecção de DoS, ataques de força bruta e ataques de sequestro de sessão. Deve ser possível filtrar relatórios por IDs de dispositivos.
- 6.26. A solução deve permitir incluir em blacklist os endereços IPs que repetidamente falharem a desafios no browser. Portanto o sistema não precisa usar recursos para mitigar tráfego enviado por esses endereços Ips. Ao entrar em Blacklist o sistema automaticamente bloqueia os pacotes enviados por esse endereço por um período de tempo.
- 6.27. A solução deve suportar e fazer a proteção do tráfego em cima de protocolo WebSocket.
- 6.28. A solução deve possibilitar o uso de múltiplas formas de logging remoto ao mesmo tempo para a mesma aplicação. Portanto dever ser possível por exemplo logar os requests válidos num servidor de SIEM e os requests inválidos em outro servidor de SIEM de outra marca e modelo.
- 6.29. A solução deverá possuir funcionalidade de proteção positiva e segura contra-ataques, como:
- 6.29.1. Acesso por Força Bruta;
 - 6.29.2. Ameaças Web AJAX/JSON;
 - 6.29.3. DoS e DDoS camada 7;
 - 6.29.4. Buffer Overflow;
 - 6.29.5. Cross Site Request Forgery (CSRF);
 - 6.29.6. Cross-Site Scripting (XSS);

- 6.29.7. SQL Injection;
- 6.29.8. Cookie e Command Injection;
- 6.29.9. Code Injection.
- 6.29.10. Parameter tampering;
- 6.29.11. Cookie poisoning;
- 6.29.12. HTTP Request Smuggling;
- 6.29.13. Manipulação de campos escondidos;
- 6.29.14. Manipulação de cookies;
- 6.29.15. Roubo de sessão através de manipulação de cookies;
- 6.29.16. Sequestro de sessão;
- 6.29.17. Força bruta no browser;
- 6.29.18. XML bombs/DoS;
- 6.29.19. Checagem de consistência de formulários;
- 6.29.20. Checagem do cabeçalho do “user-agent” para identificar clientes inválidos.
- 6.30. A solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automática.
- 6.31. Deverá ser capaz de identificar e bloquear ataques através de:
 - 6.31.1. Regras de verificação personalizadas – política de segurança configurada;
 - 6.31.2. Assinaturas, com atualização periódica da base pelo fabricante;
 - 6.31.3. As assinaturas devem ser atualizadas durante o período do contrato sem que seja necessário nenhum custo a mais por parte da CONTRATANTE na aquisição de novas licenças ou subscrições. Deve fazer parte da solução de WAF ofertada;
 - 6.31.4. Ausência de tratamento de erros pela aplicação.
- 6.32. Prevenir contra vazamento de dados sensíveis (mensagens de erro HTTP, códigos das aplicações, entre outros) dos servidores de aplicação, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários.

- 6.33. Permitir a customização da resposta de bloqueio.
- 6.34. Permitir a liberação temporária ou definitiva (white-list) de endereços IP bloqueados por terem originados ataques detectados pela solução.
- 6.35. Deve permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual.
- 6.36. Deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem o limite estabelecido, por um período de tempo determinado através de configuração.
- 6.37. Deve permitir criar lista de exceção (white list) por endereço IP específico ou faixa de sub-rede.
- 6.38. A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10.
- 6.39. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle.
- 6.40. Deverá implantar, no mínimo, as seguintes funcionalidades:
- 6.40.1. Proteção contra Buffer Overflow;
 - 6.40.2. Checagem de URL;
 - 6.40.3. Checagem de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT);
 - 6.40.4. Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);
 - 6.40.5. Proteção contra Cross-site Scripting;
 - 6.40.6. Funcionalidade de Cookie Encryption;
 - 6.40.7. Checagem de consistência de formulários;
 - 6.41.8. Checagem do cabeçalho “user-agent” para identificar clientes inválido.
- 6.41. Implementar as seguintes funcionalidades:
- 6.41.1. Cloaking – Proteção contra exposição de informações do ambiente e servidores internos como:
 - 6.41.1.1. Sistema operacional e servidor web com impressão digital.

- 6.41.2. Esconder qualquer mensagem de erro HTTP dos usuários;
- 6.41.3. Remover as mensagens de erro às páginas que serão enviadas aos usuários;
- 6.41.4. Permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios.
- 6.42. Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro Xforwarded-for (XFF).
- 6.43. Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado (s) País/Países seja (m) bloqueado (s).
- 6.44. Possuir mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres), cookies, arquivos XML e elementos XML.
- 6.45. O equipamento oferecido deverá possuir uma funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação.
- 6.46. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado.
- 6.47. O equipamento oferecido deverá possuir proteção baseada em assinaturas para prover proteção contra-ataques conhecidos. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção à regra geral.
- 6.48. A atualizações de assinaturas deverão passar por um período configurável de testes, onde nenhuma requisição que viole a assinatura será bloqueada, apenas informada no relatório. Este processo deve ser automatizado, não sendo necessário criar regras específicas a cada atualização de assinatura.
- 6.49. O equipamento oferecido deverá permitir o bloqueio de ataques DoS na camada 7, possuindo também a opção de apenas registrar o ataque, sem tomar nenhuma ação de bloqueio.
- 6.50.1. O equipamento oferecido deverá possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:
- 6.50.1.1. Número de requisições por segundo enviados a uma URL específica;
- 6.50.1.2. Número de requisições por segundo enviados de um IP específico;
- 6.50.1.3. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);
- 6.50.1.4. Número máximo de transações por segundo (TPS) de um determinado IP;

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

6.50.1.6. Aumento do stress do servidor de aplicação.

6.51. O equipamento oferecido deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas. Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável.

6.52. O equipamento oferecido deverá permitir o bloqueio de determinados endereços IPs que ultrapassem um número máximo de violações por minuto. O período de bloqueio deverá ser configurável e durante este período todas as requisições do cliente serão bloqueadas automaticamente.

6.53. O equipamento oferecido deverá permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais. Robôs conhecidos do mercado, como Google, Yahoo e Microsoft Bing deverão ser liberados por padrão.

6.54. O equipamento oferecido deverá permitir o cadastro de robôs que podem acessar a aplicação.

6.55. Possuir política de segurança de aplicações pré-configuradas no equipamento para pelo menos as seguintes aplicações:

6.55.1. Microsoft ActiveSync v1.0, v2.0;

6.55.2. Microsoft OWA in Exchange 2003, 2007, 2010 e as versões mais recentes;

6.55.3. Microsoft SharePoint 2010 e as versões mais recentes;

6.55.4. Oracle 10g Portal;

6.55.5. Oracle Application 11i;

6.55.6. Oracle PeopleSoft Portal.

6.56. O equipamento oferecido deverá implementar proteção ao JSON (JavaScript Object Notation).

6.57. Possuir firewall XML integrado – suporte a filtro e validação de funções XML específicas da aplicação.

6.58. Implementar a segurança de web services, através dos seguintes métodos:

6.58.1. Criptografar/Decriptografar partes das mensagens SOAP;

- 6.58.2. Assinar digitalmente partes das mensagens SOAP;
- 6.58.3. Verificação de partes das mensagens SOAP.
- 6.59. Prevenir o vazamento de informações, permitindo o bloqueio ou a remoção dos dados confidenciais.
- 6.60. Prevenir que erros de aplicação ou infra-estrutura sejam mostrados ao usuário.
- 6.61. Deverá ter integração, via ICAP, com servidor de anti-vírus para verificação dos arquivos a serem carregados nos servidores.
- 6.62. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle.
- 6.63. Deverá proteger o protocolo FTP com pelo menos os seguintes métodos:
 - 6.63.1. Determinar os comandos FTP permitidos;
 - 6.63.2. Requests FTP anônimos;
 - 6.63.3. Checar compliance com o protocolo FTP;
 - 6.63.4. Proteger contra-ataques de força bruta nos logins.
- 6.64. Deverá proteger o protocolo SMTP com pelo menos os seguintes métodos:
 - 6.64.1. A comunicação deve ser aderente a RFC 2821;
 - 6.64.2. Limitar o número de mensagens;
 - 6.64.3. Validar registro SPF do DNS;
 - 6.64.4. Determinar quais métodos SMTP podem ser utilizados.
- 6.65. Deverá armazenar os logs localmente ou exportar para Syslog server.
- 6.66. Deverá proteger contra ataques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs serão examinadas.
- 6.67. Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determinado site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal.
- 6.68. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados: Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade e PCI Compliance.

- 6.69. Deverá permitir o agendamento de relatórios a serem entregues por email.
- 6.70. Fornecer os seguintes Gráficos de alertas por:
- 6.70.1. Política de segurança;
 - 6.70.2. Tipos de ataques;
 - 6.70.3. Violações;
 - 6.70.4. URL;
 - 6.70.5. Endereços IP;
 - 6.70.6. Países;
 - 6.70.7. Severidade;
 - 6.70.8. Código de resposta;
 - 6.70.9. Métodos;
 - 6.70.10. Protocolos;
 - 6.70.11. Vírus;
 - 6.70.12. Usuário;
 - 6.70.13. Sessão.
- 6.71. Deverá exportar as requisições que contém os ataques, pelo menos nos formatos PDF e binário.
- 6.72. Deve possuir relatório em tempo real sobre ataques DoS L7, atualizado automaticamente.
- 6.73. A solução deve mostrar o impacto de ataques DoS L7 na performance e memória do servidor.
- 6.74. Os logs devem indicar o momento de início e final de um ataque DoS L7.
- 6.75. Possuir método de mitigação de DoS L7 baseado em: CAPTCHA; Descarte de todas as requisições de um determinado IP e/ou país suspeito; Geolocalização, incluindo a prevenção com CAPTCHA para países suspeitos que ultrapassem os thresholds; Defesa proativa contra Bot, através da injeção de um desafio JavaScript para detectar se é um usuário legítimo ou robô.
- 6.76. A solução deve permitir que ao detectar um falso positivo, o administrador aceite a requisição e atualize a política automaticamente.

- 6.77. A solução ao se integrar com um Scanner de vulnerabilidade deve mostrar quais a vulnerabilidades podem ser resolvidas automaticamente (pela própria solução de WAF) e quais podem ser resolvidas manualmente, pelo próprio administrador. No caso de resolução manual, deve ainda mostrar um guia com os passos necessários para resolver aquela vulnerabilidade, inclusive com a avisos de possíveis consequências na aplicação Web.
- 6.78. A solução deve classificar o nível de violação de uma requisição, possuindo pelo menos 5 níveis, onde o nível 5 é referente a violação mais grave e, portanto, deve ter prioridade.
- 6.79. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual.
- 6.80. Suportar os protocolos HTTP/1.0, HTTP/1.1 e HTTP/2.0.
- 6.81. Suportar codificação HTML "application/x-www-form-urlencoded".
- 6.82. Suportar Cookies v0 e v1.
- 6.83. Suportar codificação fragmentada (chunked encoding) em requisições e respostas.
- 6.84. Suportar compressão de requisições e respostas.
- 6.85. Suportar validação de protocolo, como:
- 6.85.1. Possibilidade de restringir uso de métodos;
 - 6.85.2. Possibilidade de restringir protocolos e versões de protocolos;
 - 6.85.3. Strict (per-RFC) Request Validation;
 - 6.85.4. Validar caracteres URL-encoded; e
 - 6.85.5. Validação de codificação fora de padrão %uXXYY.
- 6.86. Suportar restrições de HTML, como:
- 6.86.1. Tamanho do nome de parâmetros;
 - 6.86.2. Tamanho dos valores de parâmetros; e
 - 6.86.3. Combinação de tamanho de parâmetros (nome e valores).
- 6.87. Suportar POST no upload de arquivo.
- 6.88. Permitir configurar ou oferecer restrições para tamanho individual de arquivo.

- 6.89. Permitir customizar a lógica na inspeção de upload de arquivos.
- 6.90. Suporte para os métodos Basic, Digest e NTLM para autenticação.
- 6.91. Suporte para autenticação por back end tipo LDAP e Microsoft Active Directory.
- 6.92. Capacidade de filtrar cabeçalhos, corpo e status de respostas.
- 6.93. Suportar as seguintes técnicas de detecção:
 - 6.93.1. URL-decoding;
 - 6.93.2. Terminação Null Byte String;
 - 6.93.3. Paths auto-referenciados;
 - 6.93.4. Case de caracteres misturados;
 - 6.93.5. Uso excessivo de espaços em branco;
 - 6.93.6. Remoção de comentários;
 - 6.93.7. Decodificação de entidades HTML; e
 - 6.93.8. Caracteres de escape.
- 6.94. Possuir registro de logs com as seguintes características:
 - 6.94.1. Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo par requisição/resposta;
 - 6.94.2. Os registros de log de acesso e eventos devem ser armazenados em arquivo ou em banco de dados que permita a exportação ou em outro formato aberto como CSV ou TXT, podendo ainda serem armazenados localmente ou carregados (upload) em servidor de log via FTP ou SCP ou armazenados em servidor externo de banco de dados;
 - 6.94.3. Permitir configurar a retenção dos logs por tempo e volume; e
 - 6.94.4. Ter capacidade para detecção, remoção ou codificação de dados sensíveis do log.
- 6.95. A solução deverá gerar relatórios com as seguintes características:
 - 6.95.1. Permitir a filtragem por data ou hora, endereço IP e tipo de incidente;
 - 6.95.2. Permitir a geração de relatórios sob demanda ou pré-programados periodicamente (diário e semanal); e
 - 6.95.3. Permitir a geração de relatórios em formatos PDF/A (versão aberta) e HTML.

6.96. Possuir as seguintes características de gerenciamento:

6.96.1. Facilidade para liberação de regras aprendidas automaticamente que estejam gerando grande quantidade de falso positivo;

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

6.96.3. Facilidade para aplicar diferentes regras para diversas aplicações;

6.96.4. Capacidade para customizar regras de negação de serviço;

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

6.96.6. Capacidade para desfazer a aplicação de uma regra.

6.97. Possuir mecanismos que garantam a capacidade de gerenciamento do equipamento sob condições de alto tráfego.

6.98. A solução deve apresentar perfil de aprendizagem automática com:

6.98.1. Capacidade de aprendizagem automática sem intervenção humana; e

6.98.2. Capacidade de inspeção das regras criadas automaticamente.

6.99. Permitir o gerenciamento da configuração com as seguintes características:

6.99.1. Gerenciamento por autenticação dos usuários e as autorizações baseadas em perfis (roles); e

6.99.2. Capacidade de gerenciamento remoto dos equipamentos.

6.100. Apresentar logs e relatórios administrativos com as seguintes características:

6.100.1. Capacidade para identificar e notificar falhas do sistema ou perda de performance;

6.100.2. Capacidade de agregação de informações para simplificar a revisão das atividades do dispositivo; e

6.100.3. Capacidade para gerar estatísticas de serviço e sistema.

6.101. Possuir suporte a XML:

6.101.1. Para proteção de WebServices;

6.101.2. Em conformidade com a especificação WS-I básico; e

6.101.3. Com capacidade de restringir métodos do Webservice via definição em WSDL.

6.102. Suportar funções de camuflagem (cloaking), como:

6.102.1. Esconder qualquer mensagem de erro http dos usuários; e

6.102.2. Remover as mensagens de erro das páginas que serão enviadas aos usuários.

6.103. Proteger a aplicação Web contra robôs sofisticados através da combinação de desafios enviados ao browser do usuário e técnicas avançadas de análise comportamental.

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

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

6.106. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego com o stress do servidor de aplicação para determinar uma condição de DDoS.

6.107. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação.

6.108. Deve possuir uma proteção proativa contra-ataques automatizados por robôs e outras ferramentas de ataque.

6.109. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário.

6.110. Deve proteger esses dados criptografados de malwares e keyloggers.

6.111. Deve suportar a criptografia de sessões HTTP desde o browser do usuário, provendo proteção contra interceptação por terceiros e evitando ataques do tipo Man in the Browser e Keyloggers.

6.112. Deve possuir proteção contra-ataques DDoS, através da análise de comportamento de tráfego usando técnicas de análise de dados e Machine Learning.

6.113. Através da análise contínua de carga e monitoração de saúde de servidores, deve ser possível identificar anomalias e mitigá-las.

6.114. Deve ajudar a prevenir contra-ataques de Credential Stuffing, onde bases de credenciais expostas na Internet são usados para tentativa de acesso de outras aplicações Web.

6.115. A solução deve possuir lista dinâmica de endereços IP globais com atividades maliciosas:

6.116. Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro Xforwarded-for (XFF).

6.117. Deve possuir, pelo menos, as seguintes categorias de endereços IP: Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing Proxy, Anonymous Proxy.

6.118. Possuir linguagem de script que possibilite a interação com o payload das requisições e inclusive alterações.

7. DNS

7.1. A solução deve operar em, no mínimo, a seguintes formas:

7.1.1. DNS autoritativo;

7.1.2. DNS secundário;

7.1.3. DNS resolver;

7.1.4. DNS cache;

7.1.5. Balanceamento de DNS servers.

7.1.6. DNSSEC;

7.1.7. A solução deve ser capaz de realizar transferência de zonas para múltiplos servidores DNS Primários responsáveis por diferentes zonas;

7.1.8. Capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;

7.1.9. A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;

7.1.10. A solução deve servir as respostas as requisições onde o DNS é o autoritativo a partir da memória RAM;

7.1.11. A solução deve possuir certificação ICASA.

7.2. A solução deve possuir proteções contra-ataques DNS, no mínimo:

7.2.1. Inspeção de protocolo;

7.2.2. Validação de protocolo.

7.2.3. UDP flood;

7.2.4. Pacotes mal formados;

7.2.5. Ataque Teardrop;

7.2.6. Ataque ICMP;

7.2.7. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra-ataques.

7.3. A solução deve ser capaz de realizar balanceamento dos servidores DNS.

7.4. A solução deve ser capaz de realizar filtragem de pacotes.

7.5. A solução deve prover segurança do protocolo DNS, protegendo contra-ataques de negação de serviço, NXDOMAIN e reflexão e amplificação de DNS.

7.6. A solução deve prover segurança do protocolo DNS, protegendo contra-ataques de Cache Poisoning.

7.7. A solução deve realizar stateful inspection.

7.8. A solução deve possuir base de Geolocalização IP.

7.9. A solução deve implementar DNS64.

7.10. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT.

7.11. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente.

7.12. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura.

7.13. Deve prover as respostas a queries DNS da própria RAM CACHE.

7.14. A solução deve ser capaz de realizar IP Anycast.

7.15. A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso.

7.16. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento.

7.17. A solução de alta disponibilidade será realizada baseada em respostas a requisições DNS. A resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas.

7.18. A solução deverá aceitar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição.

7.19. Deve ser possível ajustar quantos endereços são enviados em uma única resposta.

7.20. Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido.

7.21. Suportar pelo menos os seguintes algoritmos de balanceamento:

7.21.1. Round Robin;

7.21.2. Global Availability;

7.21.3. Ratio;

7.21.4. LDNS Persist;

7.21.5. Geografia;

7.21.6. Disponibilidade da Aplicação;

7.21.7. Capacidade do Virtual Server;

7.21.8. Least Connections;

7.21.9. Pacotes por segundo;

7.21.10. Round trip time;

7.21.11. Hops;

7.21.12. Packet Completion Rate;

7.21.13. QoS definido pelo usuário;

7.21.14. Kilobytes per Second.

7.22. Implementar persistência da conexão do usuário entre aplicações ou data centers.

7.23. A solução deverá suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo.

- 7.24. A solução deverá permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada.
- 7.25. A solução deverá permitir que a contingência seja automática, mas que o retorno seja manual.
- 7.26. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6).
- 7.27. Possuir suporte a IPv6 no balanceamento global entre datacenters.
- 7.28. Ter capacidade de tratar informações das camadas L4-L7 (FTP, SMTP, URL, HTTP Header, TCP e UDP) para a tomada de decisão de encaminhamento a servidor real, em IPv4 e IPv6.
- 7.29. Deverá possuir a funcionalidade de resposta rápida a queries DNS, permitindo respostas mais rápidas para zonas que seja autoritativo.
- 7.30. A solução deve possuir suporte a Response Policy Zones (RPZ), mecanismo de firewall usado por DNS recursivo para permitir o tratamento customizado da resolução de nomes. Portanto a solução deve ser capaz de filtrar queries DNS para domínios considerados maliciosos e retornar respostas customizadas.
- 7.31. A solução deve suportar edns-client-subnet (ECS) para tanto responder requisições de clientes (Balanceamento de Carga Global de Servidores) ou encaminhar requisições de clientes (screening).
- 7.32. Baseado no ECS DNS deve ser possível preservar o endereço IP da subnet do cliente ao invés do LDNS para tomar decisões.
- 7.33. A solução deve funcionar pelo menos das seguintes formas:
- 7.33.1. Usar o ECS para tomar decisões de Balanceamento de Carga Global de Servidores baseado em topologia (Subnets);
- 7.33.2. Injetar o ECS (proxy requests) para outros servidores DNS.
- 7.34. A solução deve fazer persistência baseado no endereço IP do cliente (ECS), significando que se o cliente mudar de LDNS resolver (suporte ECS), o Balanceamento de Carga Global de Servidores deve usar a persistência existente para manter o cliente no mesmo Datacenter.
- 7.35. O serviço deverá ser implementado sobre uma infraestrutura de hardware e software dedicada ou em conjunto com equipamento Anti-DDoS. O hardware empregado deverá ser do tipo appliance, específico para operar softwares de DNS Firewall. O software e o hardware empregados deverão corresponder a uma solução de notória eficácia já em uso no mercado nacional. O serviço deve ter suporte a IPv6, registros AAAA e zonas reversas IPv6.
- 7.36. Infraestrutura de hardware e software destinada à função de resolução de nomes DNS de uso exclusivo da CONTRATANTE.

7.37. O serviço deve ter a habilidade de detectar, monitorar, controlar e mitigar ataques baseados em DNS sem gerar nenhum impacto ao tráfego válido de DNS.

7.38. A solução deverá ter serviço de resolução de nomes destinado a armazenar, de forma “autoritativa”, as zonas do CONTRATANTE e o IP reverso do bloco CIDR do CONTRATANTE.

7.39. Os equipamentos que atenderão ao serviço deverão ser estruturados de forma redundante, permitindo o failover completo na ocorrência de falhas, suportando, no mínimo, o modo de operação ativo-ativo. Um nó deverá suportar sozinho todos os requisitos de performance solicitados neste projeto.

7.40. Para o devido dimensionamento do serviço cada equipamento isolado deve possuir desempenho DNS de pelo menos 50.000 QPS (50 mil Queries Per Second – Consultas Por Segundo).

7.41. O serviço deverá possuir capacidade para resolver consultas para as quais não tem autoridade (ou seja, da zona “.”, tipo “hint”), com a finalidade de atender somente às consultas DNS oriundas da rede interna do CONTRATANTE, bem como dos demais Serviços Gerenciados de Segurança e servidores instalados no Data Center.

7.42. O serviço deve ter, pelo menos, as seguintes características de segurança:

7.43. Deve permitir o uso de lista negra para bloquear domínios DNS.

7.44. Deve possuir capacidade de criação de ACLs para bloqueio de domínios e redes maliciosas.

7.45. Prover uma linha de defesa para bloquear tentativas de acesso a sites maliciosos impedindo a resolução de nomes de domínio que hospedem tais conteúdos maliciosos minimizando possíveis infecções de Malware, Trojan, Spyware, Ransomware e softwares de comando e controle (BotNet).

7.46. Registrar todas as tentativas de comunicação com os nomes de domínio que hospedem conteúdo malicioso. Estes registros devem conter: IP de origem, destino, data e hora do acesso.

7.47. Deve suportar no mínimo os seguintes métodos de controle: apenas logar, bloquear o dado ou substituir o nome do domínio.

7.48. A solução deverá suportar mecanismo de “assinaturas”, ou técnicas semelhantes, que permitam ao fabricante disponibilizar regras de bloqueios contra novos ataques conforme surgimento.

7.49. O serviço deverá permitir que o administrador crie regras customizadas de bloqueio, da seguinte maneira:

7.49.1. Bloqueio de nomes de domínio totalmente qualificados em consultas de DNS feitas via TCP ou UDP;

7.49.2. Bloqueio de endereços de origem IPv4 ou IPv6 em consultas realizadas via TCP ou UDP. Esta regra deverá permitir a configuração de endereços de hosts ou de redes.

7.50. Configuração de limites de quantidades de consultas de DNS (rate limit) realizadas via TCP ou UDP por nome de domínio totalmente qualificado.

7.51. De acordo com o IP de origem, configurar limite (rate limit) para consultas realizadas via TCP ou UDP.

7.52. Criar “Listas brancas” que permitam a realização de qualquer número de consultas de DNS por segundo, para determinado endereço IP de origem.

7.53. O serviço deverá proteger no mínimo contra os seguintes ataques de DNS:

7.53.1. Reflexão;

7.53.2. Anomalias de Protocolo;

7.53.3. Negação de Serviço;

7.53.4. Negação de Serviços Distribuídos;

7.53.5. Amplificação;

7.53.6. Tunelamento;

7.53.7. Reconhecimento;

7.53.8. Explorações (Exploit);

7.53.9. Envenenamento do cache;

7.53.10. Excessos (Floods).

7.54. O serviço deve permitir que os administradores efetuem busca de endereços de rede, subrede e endereços IP através de filtros.

7.55. A administração do serviço deve permitir definir diferentes níveis de grupos e usuários para administração.

7.56. O serviço deve possuir capacidade de reverter configurações sem a necessidade de restauração de backup.

7.57. O serviço deverá fornecer pelo menos os seguintes relatórios:

7.57.1. Tendência de latência de resposta de DNS;

- 7.57.2. Nomes de domínios de DNS mais requisitados;
- 7.57.3. Tendência de uso do cache de DNS;
- 7.57.4. Top clientes de DNS;
- 7.57.5. Taxa de consultas de DNS por tipo de registro;
- 7.57.6. Tendências de respostas de DNS;
- 7.57.7. Taxa de consultas de DNS diária por servidor;
- 7.57.8. Pico de consultas diárias de DNS por servidor;
- 7.57.9. Top DNS NXDOMAIN/No error;
- 7.57.10. Top SERVFAIL enviados e recebidos;
- 7.57.11. Top clientes por domínio de DNS;
- 7.57.12. Nomes de domínios com conteúdo malicioso;
- 7.57.13. Principais domínios maliciosos;
- 7.57.14. Principais acessos ao DNS Firewall;
- 7.57.15. Quantidade de eventos registrados por horário;
- 7.57.16. Quantidade de eventos por severidade;
- 7.57.17. Quantidade de eventos por regra;
- 7.57.18. Quantidade de eventos por tendência;
- 7.57.19. Quantidade de eventos por categoria.
- 7.58. Deve permitir a criação visões (“views”) para tratamento diferenciado de consultas conforme origem das requisições.
- 7.59. Deve implementar DNSSEC com suporte a NSEC3 (RFC 5155).

8. ANTI-DDOS L4-L7

- 8.1. Deve suportar as funcionalidades de segurança para proteção DDoS.
- 8.2. Deve suportar proteção contra todos os tipos de ataques Denial of Service (DoS e DDoS).
- 8.3. A solução deve proteger de ataques DDoS que utilizem SSL.

8.4. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego com o stress do servidor de aplicação para determinar uma condição de DDoS.

8.5. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação.

8.6. Deve permitir proteção contra-ataques DDoS, através da análise de comportamento de tráfego usando técnicas de análise de dados e Machine Learning.

8.7. Deve permitir proteger contra-ataques de DNS DDoS utilizando mecanismo que bloqueie somente as requisições maliciosas e permita requisições legítimas aos domínios existentes.

8.8. Deve suportar Network Address Translation (NAT).

8.9. Deve limitar o número de conexões.

8.10. Deve suportar Listas de Controle de Acesso (ACL).

8.11. Deve permitir o log de ataques do tipo DoS.

8.12. A solução deve possuir ferramenta flexível baseado em linguagem de programação open-source para customizar e aumentar o nível de segurança contra-ataques DDoS, incluindo a possibilidade de interação com base de reputação de endereços IP e estatísticas de tráfego.

8.13. A solução deve suportar relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DDoS.

8.14. Deve possuir suporte ao envio de SNMP traps para cada ataque DDoS detectado.

8.15. A solução deve possuir uma ferramenta de teste de pacotes, através da qual deve ser possível realizar testes de pacotes com atributos específicos através da solução anti -DoS.

9. SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO

9.1. A Licitante vencedora será inteiramente responsável pela migração da solução atual para a nova solução, de forma a não comprometer o funcionamento dos sistemas, recursos ou equipamentos atualmente em operação.

9.2. Serão contemplados todos os serviços de instalação física de todos os componentes adquiridos, desde a montagem até a energização dos equipamentos.

9.3. Deverá ser fornecido documentação de toda a implementação e configuração dos produtos adquiridos.

9.4. Após no máximo 5 (cinco) dias úteis da assinatura do contrato, deverá ser realizada uma reunião presencial no Contratante, com a participação de no mínimo 1 (um) preposto da

Contratada e os representantes da equipe do Contratante, com o objetivo de elaborar o plano de migração.

9.5. A Contratada deverá apresentar, em até 15 (quinze) dias úteis da assinatura do contrato, para aprovação do Contratante, o projeto executivo contendo o plano detalhado de instalação, configuração e migração, especificando os procedimentos e cronograma a serem adotados.

9.6. O Contratante fará análise e validação do projeto executivo contendo o plano detalhado de instalação, configuração e migração, em até 5 (cinco) dias úteis, apontado as devidas correções no documento, ficando a Contratada responsável por ajustar o plano em até 7 (sete) dias úteis, conforme as alterações apontadas pela Contratante.

9.7. Fica a critério do Contratante, definir o horário de instalação e configuração dos equipamentos, podendo tais procedimentos serem executados em feriados ou finais de semana e em horário noturno.

9.8. A Contratada não poderá realizar terceirização dos serviços objeto deste termo de referência, sendo responsável pela execução do serviço objeto desta contratação.

9.9. Os serviços de instalação e configuração, para cada um dos itens, devem ser executados por técnicos da futura contratada, certificados pelo fabricante dos equipamentos fornecidos, sendo necessária a apresentação de documentação original que comprove a validade desta (s) certificação (ões) enquanto durar o contrato, que pode ser solicitada a qualquer momento.

9.10. A futura CONTRATADA deverá apresentar um Projeto Executivo que deve conter, no mínimo, as seguintes informações:

9.10.1. Objetivo dos serviços;

9.10.2. Plano de gerenciamento de mudanças, detalhando passo a passo o escopo da migração;

9.10.3. Cronograma das atividades que serão realizadas, com os prazos estimados e as diretrizes para cada atividade;

9.10.4. Projeto lógico de configuração e diagrama de interconexão dos equipamentos;

9.10.5. Nome (s) do (s) gerente (s) de projetos responsável (is) e do (s) técnico (s) responsável (is) pela execução dos serviços;

9.10.6. Lista de todos os elementos instalados contendo:

- a) Nome e endereço IP do equipamento.
- b) Equipamento e porta na qual o equipamento foi conectado.
- c) Local de instalação (prédio, andar, sala).
- d) Número de série do equipamento.

9.11. O Projeto Executivo deverá ser entregue pela futura CONTRATADA em até 15 (quinze) dias úteis após a assinatura do contrato, o qual deverá ser aprovado pela CONTRATANTE. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes.

9.12. A instalação e configuração da solução compreenderá dentre outros atendimentos, no mínimo, os seguintes requisitos:

9.12.1. Acondicionamento dos equipamentos nos locais de instalação, incluindo a desembalagem, a montagem de todos os componentes que integram a solução, a instalação dos conjuntos montados nos rack padrão 19" da CONTRATANTE, a energização do equipamento, incluindo o fornecimento de eventuais réguas, caso necessário, devendo seguir obrigatoriamente os manuais técnicos do fabricante;

9.12.2. Instalação dos transceivers e outros acessórios em seus respectivos slots;

9.12.3. Ligações de rede dos equipamentos a infraestrutura da CONTRATANTE, incluindo o fornecimento, quando necessário, de:

9.12.3.1. Cordões ópticos OM4 com, no mínimo, 2 (dois) metros de comprimento para ligações em fibra;

9.12.3.1. Patch-cords UTP CAT6A com, no mínimo, 2 (dois) metros de comprimento para ligações em par metálico.

9.12.4. Os cabos/cordões necessários para a interligação de servidores, usuários e outras conexões que não as estritamente fornecidas são de responsabilidade da CONTRATANTE, ou seja, cabe a CONTRATADA interligar os equipamentos fornecidos;

9.12.5. Upgrade ou Downgrade do firmware;

9.12.6. A realização dos ajustes de hardware e software necessários ao funcionamento do ambiente e a instalação da solução de gerenciamento;

9.12.7. Conexão das interfaces de gerenciamento a nova rede out-of-band e testes de acesso a ferramenta de gerência para administração;

9.12.8. Configuração e teste de envio de Traps SNMP. Verificações dos recursos e o seu perfeito funcionamento e integração com os demais, conforme as melhores práticas indicadas pelo fabricante;

9.12.9. A identificação dos equipamentos e de todas as suas conexões.

9.13. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, podendo estas ser realizadas presencialmente, por telefone ou via conferência web, devendo a futura CONTRATADA sugerir as configurações de acordo com

normas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas.

9.14. A Contratada deverá configurar todas as funcionalidades do produto licenciadas e solicitadas pela Contratante.

9.15. As configurações deverão seguir fielmente a padronização previamente estabelecida pela CONTRATANTE.

9.16. Durante o processo de instalação e configuração deverá ser realizada transferência de conhecimento para a equipe da Contratante.

9.17. A futura CONTRATADA deverá fazer análise do ambiente tecnológico atual, devendo a CONTRATANTE fornecer todas as informações necessárias sobre a infraestrutura instalada, de modo que se possa garantir a continuidade dos serviços prestados pelo órgão durante a migração, mantendo a disponibilidade dos serviços básicos de rede (resolução de nomes, endereçamento dinâmico, autenticação dos usuários, etc.) e dos demais serviços de retaguarda (aplicativos, correio eletrônico, banco de dados, Internet, etc.).

9.18. A substituição da infraestrutura atual deve ser planejada e executada de modo que não cause interrupções e paralisações não programadas, ou qualquer outro tipo de transtorno ao correto funcionamento do ambiente operacional da CONTRATANTE; caso não seja possível manter a disponibilidade dos serviços básicos no momento da instalação, as manobras de implantação deverão ser realizadas durante janela de manutenção agendada previamente, em horários que não comprometam o funcionamento das atividades do órgão, inclusive aos sábados, domingos e feriados.

9.19. Ao término do serviço deve ser fornecido um relatório detalhado (as-built) contendo todas as configurações realizadas, com comentários sobre os principais comandos e as justificativas das opções de parametrização de modo a facilitar a posterior administração da solução e a continuidade de seu funcionamento.

9.20. O relatório deve conter, no mínimo, as seguintes informações:

9.20.1. Diagrama de arquitetura da solução;

9.20.2. Procedimento operacional detalhado com as etapas de instalação e configuração;

9.20.3. Informações de monitoramento da solução;

9.20.4. Informações pertinentes a posterior continuidade e manutenção da solução;

9.20.5. Referências da documentação oficial do produto.

9.21. A critério da CONTRATANTE, poderá ser elaborado um único as-built contendo todas as informações de todos os equipamentos e softwares instalados/configurados.

9.22. O serviço de instalação e configuração somente será concluído após a apresentação pela contratada do projeto executivo, as-built e o recebimento definitivo do serviço pela contratante.

9.23. A contratada deverá monitorar o ambiente da contratante por ao menos 15 dias após o final e aprovação da instalação e configuração pela contratante e atuar imediatamente no caso de evento ou falha das configurações ou equipamentos.

10. GERENCIAMENTO CENTRALIZADO

10.1. A solução de gerenciamento deve fornecer um ponto de controle unificado para todo o cluster de equipamentos da solução.

10.2. A solução de gerenciamento centralizada deve ser capaz de armazenar logs, eventos.

10.3. Seja capaz de realizar operações de backup;

10.4. Deve ser capaz de realizar o licenciamento dos componentes do cluster;

10.5. Deve ser capaz de realizar monitoramento e gerenciamento do cluster;

10.6. Ser capaz de gerenciar usuários, limitando os acessos dos usuários de acordo com seus níveis de acesso;

10.7. Deve realizar coleta de dados do cluster com objetivo de armazenar e gerenciar os dados;

10.8. Deve ser capaz de armazenar backups de eventos, alertas e dados estatísticos para requisitos de recuperação de desastres do cluster;

10.9. Realizar backups automático de imagens e configurações;

10.10. Monitoramento por meio de painéis, relatórios e alertas;

10.11. Deve ser capaz de permitir realização de análises detalhadas por aplicativo;

10.12. Gerenciar licenças do cluster;

10.13. Garantir políticas consistentes de segurança e gerenciamento de tráfego em toda a sua infraestrutura;

10.14. Criar, provisionar e implantar novos dispositivos e serviços de aplicativos;

10.15. Caso a solução de gerenciamento centralizado ofertada seja virtualizado, a solução deve ser compatível com as plataformas vmware;

10.16. Deve fornecer controle de acesso baseado em função (RBAC);

10.17. Ser capaz de associar funções a usuários e grupos locais ou a outros usuários e grupos de servidores remotos do Active Directory (AD), TACACS+, RADIUS ou LDAP;

- 10.18. Deve permitir o gerenciamento de solicitações de certificados Let's Encrypt;
- 10.19. Deve ser capaz de gerar relatórios de alertas de segurança;
- 10.20. Permitir geração de relatórios de segurança por tipo de dispositivo, aplicativo, anomalias, DDoS, atividade de bot, políticas de segurança diferenciais e políticas não utilizadas;
- 10.21. Deve ser capaz de agendar e gerar automaticamente relatórios;

11. SUPORTE TÉCNICO

11.1. O serviço de suporte técnico deve ser prestado conforme especificação a seguir:

11.1.1. O licitante vencedor deverá fornecer serviço de suporte técnico on-site e remotamente, sempre que for necessário à Presidência da República para solucionar problemas, instalar, configurar e reconfigurar o software ou dirimir dúvidas técnicas relacionadas as soluções ofertadas.

11.1.2. A escolha entre o suporte técnico on-site ou remoto será realizada pela contratante e ocorrerá na ocasião da abertura de cada ordem de serviços.

11.1.3. O licitante vencedor deverá iniciar o atendimento de acordo com os prazos definidos no Instrumento de Medição de Resultado, a contar da abertura da Ordem de Serviço e esse prazo para o início do atendimento para ambos os tipos de suporte On-site, e remoto é o mesmo.

11.1.4. O suporte técnico será realizado 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, incluindo feriados, conforme Instrumento de Medição de Resultado.

11.1.5. O término do atendimento não poderá ultrapassar o prazo estipulado no Instrumento de Medição de Resultado.

11.1.6. Os serviços de suporte técnico, a serem prestados, abrangem atividades que não são cobertas pela garantia ou pelo suporte técnico do fornecedor/fabricante, que garante a resolução de problemas referentes a falhas e defeitos.

11.1.7. O serviço será remunerado mensalmente.

11.1.8. A Ordem de Serviço poderá ser aberta por e-mail e telefone, e na ocasião da assinatura do contrato, o licitante vencedor deverá fornecer as informações para a abertura de Ordens de Serviço.

11.1.9. A empresa deverá possuir no mínimo 2 (dois) técnicos certificados pelo fabricante da solução.

11.1.10. O suporte técnico iniciará a partir da data de recebimento definitivo da solução.

11.2. Instrumento de Medição de Resultado:

11.2.1. As soluções ofertadas devem estar cobertas por garantia total fornecida pelo fabricante.

11.2.2. Durante o período de suporte, o licitante vencedor deverá atender às solicitações da PR, feitas por meio da Coordenação-Geral de Infraestrutura Tecnológica, em qualquer horário, respeitando as condições e níveis de serviço especificados a seguir.

11.2.3. O Instrumento de Medição de Resultado (IMR) será contado a partir da abertura de ordem de serviço e será classificado conforme as severidades especificadas a seguir.

11.2.4. Severidade ALTA: Esse nível de severidade é aplicado quando há indisponibilidade de componentes da solução ou as aplicações que são acessadas por meio da solução estão indisponíveis:

Dias Úteis		Sábados, Domingos e Feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
04 horas	04 horas	04 horas	04 horas

11.2.5. Severidade MÉDIA: Esse nível de severidade é aplicado quando há falha no uso da solução, estando ainda disponível, porém apresentando problemas ou instabilidade:

Dias Úteis		Sábados, Domingos e Feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
08 horas	24 horas	08 horas	24 horas

11.2.6. Severidade BAIXA: Esse nível de severidade é aplicado para a instalação, configuração, manutenções preventivas, aplicações de firmwares e esclarecimento técnico relativo ao uso da solução. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados:

Dias Úteis		Sábados, Domingos e Feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
24 horas	72 horas	Não se aplica	Não se aplica

11.2.7. Haverá multa em caso de atraso na prestação dos serviços de acordo com a seguinte tabela:

Multa	Classificação IMR	Limite da Incidência
Para infração descrita na alínea “b” do subitem 13.1 do Termo de Referência, a multa será de 5% (cinco por cento) a 10% (dez por cento), do valor do Contrato	Severidade Crítica	180 dias

Compensatória, para a inexecução total do contrato prevista na alínea “c” do subitem 13.1 do Termo de Referência, a multa será de 1% (um por cento) a 5% (cinco por cento), do valor do Contrato	Severidade Alta	180 dias
Para infração descrita na alínea “d” do subitem 13.1 do Termo de Referência, a multa será de 0,5% (cinco décimos por cento) a 1% (um por cento), do valor do Contrato	Severidade Média	90 dias
Moratória de 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida	Severidade Baixa	15 dias
Referência: Item “13. Infrações e Sanções Administrativas” do Termo de Referência.		

11.2.8. Serão considerados para efeitos dos níveis exigidos:

11.2.8.1. Prazo de Atendimento: Tempo decorrido entre a solicitação efetuada pela Equipe Técnica da PR à Prestadora de Serviço e o efetivo início dos trabalhos de manutenção;

11.2.8.2. Prazo de Solução Definitiva: Tempo decorrido entre a solicitação efetuada pela Equipe Técnica do PR à Prestadora de Serviço e a efetiva colocação dos equipamentos em seu pleno estado de funcionamento e operação normais.

11.2.9. A contagem do prazo de atendimento e solução definitiva de cada solicitação será a partir da notificação ao licitante vencedor, até o momento da comunicação da solução definitiva do problema e aceite pela equipe técnica da PR.

11.2.10. O atendimento às solicitações de severidade ALTA deverá ser realizado nas instalações da PR (on-site) e não poderá ser interrompido até o completo restabelecimento do serviço, mesmo que se estenda para períodos noturnos, sábados, domingos e feriados. Nesse caso, não poderá implicar em custos adicionais à PR. A interrupção do suporte técnico de uma solicitação desse tipo de severidade por parte do licitante vencedor e que não tenha sido previamente autorizado pela PR, poderá ensejar em aplicação de glosas previstas.

11.2.11. As ordens de serviços classificadas com severidade MÉDIA, quando não solucionados no prazo definido, poderão ser automaticamente escaladas para a severidade ALTA, sendo que os prazos de atendimento e solução definitiva do problema, bem como glosas previstas, serão automaticamente ajustados para o novo nível. A interrupção do suporte técnico de uma solicitação desse tipo de severidade por parte do licitante vencedor e que não tenha sido previamente autorizado pela PR, poderá ensejar em aplicação de glosas previstas.

11.2.12. Depois de concluído o suporte técnico, o licitante vencedor comunicará o fato à Equipe Técnica da PR e solicitará autorização para o fechamento do chamado. Caso a PR não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pelo licitante vencedor. Nesse caso, a PR fornecerá as pendências relativas à solicitação em aberto.

11.2.13. A PR encaminhará ao licitante vencedor, quando da reunião de apresentação inicial, relação nominal da equipe técnica autorizada a abrir e fechar solicitações de suporte técnico.

11.2.14. Por necessidade excepcional de serviço, a PR também poderá solicitar a escalção de chamado para níveis superiores de severidade. Nesse caso, a escalção deverá ser justificada e os prazos dos chamados passarão a contar do início novamente.

11.2.15. O pagamento das faturas estará sujeito à glosa quando não houver cumprimento dos níveis de serviço exigidos ou quaisquer outras que impliquem em glosas previstas.

12. CAPACITAÇÃO

12.1. A capacitação deverá ser realizada no idioma português do Brasil.

12.2. O material didático utilizado na capacitação deve estar no idioma inglês ou português do Brasil.

12.3. O instrutor que ministrará a capacitação da solução deve possuir certificação do fabricante da solução ofertada.

12.4. A documentação exigida em relação ao instrutor deverá ser apresentada na assinatura do contrato.

12.5. A capacitação deverá possuir uma carga horária mínima de 40 horas.

12.6. A capacitação deverá abordar no mínimo sobre a instalação, configuração, administração e resolução de problemas da solução ofertada.

12.7. Deve ser emitido um certificado para cada servidor que participar da capacitação e tiver frequência mínima de 70% (setenta por cento).

12.8. A capacitação será realizada DE FORMA ON-LINE OU PRESENCIAL em Brasília em local definido pelo licitante vencedor.

12.9. O licitante vencedor irá capacitar 8 (oito) servidores da PR.

12.10. A capacitação deve ser realizada em até 90 (noventa) dias corridos, contados a partir da solicitação oficial deste serviço.

12.11. É permitida a subcontratação desse item.

**Anexo VII - Cotacao-Detalhado-41-2024,
vDecimaPrimeira.pdf**

Relatório de pesquisa de preço

Relatório Detalhado

Informações básicas

Número da Pesquisa	UASG	Status	Editado por
41/2024	110001	Concluída	NELSON GONCALVES REZENDE
Título: Aquisição de solução de equipamentos Firewall de Aplicação Web (WAF)			
Observações: Solução de equipamentos Firewall de Aplicação Web (WAF), com suporte técnico e garantia de 60 meses. (Processo SUPER nº 00094.000097/2024-34)			
Total de itens cotados: 3		Valor total da pesquisa de preços: R\$ 5.533.756,8400	

Itens cotados

Item: 1

Descrição do item	Unidade de Fornecimento	Quantidade
481646 - Equipamento Segurança Rede Tipo: Amppliance , Aplicação: Firewall	Unidade	1
Consolidação dos preços cotados		
Menor Preço	Média	Mediana
R\$ 2.849.077,0000	R\$ 4.551.175,1233	R\$ 5.219.848,3700
Método de cálculo adotado: Mediana		
Coeficiente de Variação: 26,6468% Desvio Padrão: 1.212.741,9220 Maior Preço: R\$ 5.584.600,0000		

Filtro Aplicado
Período: 12 Meses

Nº	Inciso	Nome	Quantidade	Unidade	Preço unitário	Data	Compõe
1	IV	ISH TECNOLOGIA S/A - Fornecedor	1		R\$ 5.219.848,3700	01/04/2024	Sim

Identificação do Fornecedor	Marca/modelo	Endereço Eletrônico
01.707.536/0001-04	Hardware, licenças de softwares e de serviços de suporte técnico da F5 Networks	http://www.ish.com.br
Data da Cotação	Hora da Cotação	Validade da Cotação
01/04/2024	15:12	01/05/2024
Contato	Informações Adicionais	
Daniel Duarte (E-mail: daniel.duarte@ish.com.br)	-	
Anexos		
PT 2024040100 - Presidencia - BIG IP.pdf		

Nº	Inciso	Nome	Quantidade	Unidade	Preço unitário	Data	Compõe
2	IV	Global Sec. Tecnologia & Informação Ltda. - Fornecedor	1		R\$ 5.584.600,0000	05/04/2024	Sim

Identificação do Fornecedor	Marca/modelo	Endereço Eletrônico
31.862.002/0001-13	-	www.globalsectecnologia.com.br

Data da Cotação	Hora da Cotação	Validade da Cotação
05/04/2024	14:49	05/07/2024

Contato	Informações Adicionais
Gustavo Miranda ((61) 99810-7773; E-mail: comercial@globalsectecnologia.com.br)	-

Anexos
PC 2024 - 073 - Presidencia da Republica.pdf

Nº	Inciso	Nome	Quantidade	Unidade	Preço unitário	Data	Compõe
3	II	SUPERIOR TRIBUNAL DE JUSTICA/DF - Contratações Similares pela Administração Pública	1		R\$ 2.849.077,0000	29/11/2023	Sim

Data da Cotação	Marca/Modelo	Informações Adicionais
29/11/2023	Solução de Web Application Firewall (WAF), F5	Fornecedor: TELTEC SOLUTIONS LTDA, CNPJ/CPF nº 004.892.991/0001-15.
Hora da Cotação	Endereço Eletrônico	Anexos
18:58	paineldepregos.planejamento.gov.br	-

Legenda:  Compra Anulada ou Revogada.

Item: 2

Descrição do item	Unidade de Fornecimento	Quantidade
27111 - Serviços de Instalação de Computadores e seus Periféricos	UNIDADE	1
Consolidação dos preços cotados		
Menor Preço	Média	Mediana
R\$ 60.000,0000	R\$ 113.560,5100	R\$ 89.071,0200
Método de cálculo adotado: Mediana		
Coeficiente de Variação: 55,0691% Desvio Padrão: 62.536,7917 Maior Preço: R\$ 216.100,0000		

Filtro Aplicado
Período: 12 Meses

Nº	Inciso	Nome	Quantidade	Unidade	Preço unitário	Data	Compõe
1	I	COMANDO DO EXERCITO - Compras.gov.br	1	UNIDADE	R\$ 60.000,0000	09/02/2024	Sim

Id da Compra	Comprado em	Nº do Item	Objeto da Compra
16052805000112023	09/02/2024	25	Objeto: Pregão Eletrônico - Contratação de Empresa Especializada em Serviços de Atualização de Equipamentos de Conectividade com e sem Fio, Implementação de Firewall, Manutenção e Atualização do Sistema de Gerenciamento de Backup(DTI)
Esfera	UASG	Forma	Modalidade
Federal	160528	SISRP	Pregão

Fornecedor
SERVIX INFORMATICA LTDA

Índice e Valor	Ata	Edital	Compra
-	Acesse a Ata	Acesse o Edital	Acesse a compra

Descrição Detalhada
Serviços de Instalação de Computadores e seus Periféricos

Nº	Inciso	Nome	Quantidade	Unidade	Preço unitário	Data	Compõe
2	I	JUSTICA FEDERAL - Compras.gov.br	3	UNIDADE	R\$ 66.040,0000	17/01/2024	Sim

Id da Compra	Comprado em	Nº do Item	Objeto da Compra
9002605000182023	17/01/2024	3	Objeto: Pregão Eletrônico - PREGÃO ELETRÔNICO, do tipo MENOR PREÇO POR LOTE E ITEM, para ampliação da solução de armazenamento principal NETAPP FAS9000 do Conselho da Justiça Federal - CJF e aquisição de solução de armazenamento de contingência do CJF e ambiente principal e de contingência do Superior Tribunal de Justiça STJ, do fabricante NETAPP, através do Sistema de Registro de Preços, contemplando o fornecimentode equipamento(s), discos e gavetas, serviços de instalação e configuração.
Esfera	UASG	Forma	Modalidade
Federal	90026	SISRP	Pregão

Fornecedor
SERVIX INFORMATICA LTDA

Índice e Valor	Ata	Edital	Compra
-	Acesse a Ata	Acesse o Edital	Acesse a compra

Descrição Detalhada
Serviços de Instalação de Computadores e seus Periféricos

Nº	Inciso	Nome	Quantidade	Unidade	Preço unitário	Data	Compõe
3	IV	ISH TECNOLOGIA S/A - Fornecedor	1		R\$ 112.102,0400	01/04/2024	Sim

Identificação do Fornecedor

01.707.536/0001-04

Endereço Eletrônico

<http://www.ish.com.br>

Data da Cotação

01/04/2024

Hora da Cotação

16:24

Validade da Cotação

01/05/2024

Contato

Daniel Duarte (E-mail: daniel.duarte@ish.com.br)

Informações Adicionais

-

Anexos

PT 2024040100 - Presidencia - BIG IP.pdf

Nº	Inciso	Nome	Quantidade	Unidade	Preço unitário	Data	Compõe
4	IV	Global Sec. Tecnologia & Informação Ltda. - Fornecedor	1		R\$ 216.100,0000	05/04/2024	Sim

Identificação do Fornecedor

31.862.002/0001-13

Endereço Eletrônico

www.globalsectecnologia.com.br

Data da Cotação

05/04/2024

Hora da Cotação

15:16

Validade da Cotação

05/07/2024

Contato

Gustaco Miranda ((61) 99810-7773; E-mail: comercial@globalsectecnologia.com.br)

Informações Adicionais

-

Anexos

PC 2024 - 073 - Presidencia da Republica.pdf

Legenda:  Compra Anulada ou Revogada.

Item: 3

Descrição do item	Unidade de Fornecimento	Quantidade
16837 - Treinamento Informática - Equipamento / Hardware	UNIDADE	1
Consolidação dos preços cotados		
Menor Preço	Média	● Mediana
R\$ 139.000,0000	R\$ 220.493,7250	R\$ 224.837,4500
Método de cálculo adotado: Mediana		
Coeficiente de Variação: 24,9046%		
Desvio Padrão: 54.913,1761		
Maior Preço: R\$ 293.300,0000		

Filtro Aplicado

Período: 12 Meses

Nº	Inciso	Nome	Quantidade	Unidade	Preço unitário	Data	Compõe
1	I	ESTADO DO PARA - Compras.gov.br	1	UNIDADE	R\$ 218.430,0000	15/01/2024	Sim

Id da Compra	Comprado em	Nº do Item	Objeto da Compra
98059505000302023	15/01/2024	4	Objeto: Pregão Eletrônico - Prestação de serviços continuados de implantação e licença/locação de software BPM, integrador de processos públicos municipais, 100% web, com criação, controle e tramitação de doc. digitais com base em consultas internas ou externas, autentic. e validação de doc. por chave de segurança e assin. eletrônica em arquivos, base de dados base de dados digitalizados e cadastro único, aplicativo mobile integrado ao ao Sistema, além de serviçosde infraestrutura de data centers SEMAD
Esfera	UASG	Forma	Modalidade
Estadual	980595	SISPP	Pregão
Fornecedor	CENTRODATA TELECOMUNICACOES ECO TECHNOLOGY LTDA		
Índice e Valor	Ata	Editais	Compra
-	-	Acesse o Edital	Acesse a compra
Descrição Detalhada			
Treinamento			

Nº	Inciso	Nome	Quantidade	Unidade	Preço unitário	Data	Compõe
2	I	MINISTERIO PUBLICO DA UNIAO - Compras.gov.br	4	UNIDADE	R\$ 135.000,0000	30/12/2023	Não

Id da Compra	Comprado em	Nº do Item	Objeto da Compra
20023405000092023	30/12/2023	3	Objeto: Pregão Eletrônico - O objeto da presente licitação é o registro de preços para a contratação de empresas especializadas no fornecimento de equipamentos para Data Center com garantia e suporte técnico por 60 (sessenta) meses, conforme especificações técnicas e quantitativos contidos neste documento, para atendimento daEscola Superior do Ministério Público ESMPU e do Conselho Nacional do Ministério Público - CNMP.. conforme condições, quantidades e exigências estabelecidas neste Edital
Esfera	UASG	Forma	Modalidade
Federal	200234	SISRP	Pregão
Fornecedor	WISEIT - SISTEMAS E INFORMATICA LTDA		
Índice e Valor	Ata	Editais	Compra
-	Acesse a Ata	Acesse o Edital	Acesse a compra
Descrição Detalhada			
Switch SAN			

Nº	Inciso	Nome	Quantidade	Unidade	Preço unitário	Data	Compõe
3	I	MINISTERIO PUBLICO DA UNIAO - Compras.gov.br	12	UNIDADE	R\$ 100.000,0000	30/12/2023	Não

Id da Compra	Comprado em	Nº do Item	Objeto da Compra
20023405000092023	30/12/2023	2	Objeto: Pregão Eletrônico - O objeto da presente licitação é o registro de preços para a contratação de empresas especializadas no fornecimento de equipamentos para Data Center com garantia e suporte técnico por 60 (sessenta) meses, conforme especificações técnicas e quantitativos contidos neste documento, para atendimento da Escola Superior do Ministério Público ESMPU e do Conselho Nacional do Ministério Público - CNMP.. conforme condições, quantidades e exigências estabelecidas neste Edital
Esfera	UASG	Forma	Modalidade
Federal	200234	SISRP	Pregão
Fornecedor			
CALC INFORMATICA COMERCIO E SERVICOS LTDA			
Índice e Valor	Ata	Edital	Compra
-	Acesse a Ata	Acesse o Edital	Acesse a compra
Descrição Detalhada			
Expansão de armazenamento			

Nº	Inciso	Nome	Quantidade	Unidade	Preço unitário	Data	Compõe
4	I	MINISTERIO PUBLICO DA UNIAO - Compras.gov.br	2	UNIDADE	R\$ 163.632,0000	30/12/2023	Não

Id da Compra	Comprado em	Nº do Item	Objeto da Compra
20023405000092023	30/12/2023	6	Objeto: Pregão Eletrônico - O objeto da presente licitação é o registro de preços para a contratação de empresas especializadas no fornecimento de equipamentos para Data Center com garantia e suporte técnico por 60 (sessenta) meses, conforme especificações técnicas e quantitativos contidos neste documento, para atendimento da Escola Superior do Ministério Público ESMPU e do Conselho Nacional do Ministério Público - CNMP.. conforme condições, quantidades e exigências estabelecidas neste Edital
Esfera	UASG	Forma	Modalidade
Federal	200234	SISRP	Pregão
Fornecedor			
CALC INFORMATICA COMERCIO E SERVICOS LTDA			
Índice e Valor	Ata	Edital	Compra
-	Acesse a Ata	Acesse o Edital	Acesse a compra
Descrição Detalhada			
Servidor de Rede - Backup			

Nº	Inciso	Nome	Quantidade	Unidade	Preço unitário	Data	Compõe
5	I	MINISTERIO DA CULTURA - MINC - Compras.gov.br	1	UNIDADE	R\$ 139.000,0000	28/12/2023	Sim

Id da Compra	Comprado em	Nº do Item	Objeto da Compra
42000105000142023	28/12/2023	11	Objeto: Pregão Eletrônico - AQUISIÇÃO SOLUÇÃOOSDLAN COMPOSTA DE SWITCHES CORE; SWITCHES DE DISTRIBUIÇÃO, SWITCHES DE ACESSO, ACCES POINT E SOLUÇÃO DE GERENCIAMENTO DE REDE, com garantia de assistência técnica 24hx7d por 60 (sessenta)meses, conforme condições e exigências estabelecidas no Termo de Referência e seus anexos
Esfera	UASG	Forma	Modalidade
Federal	420001	SISRP	Pregão
Fornecedor	LETTTEL DISTRIBUIDORA DE TELEFONIA LTDA		
Índice e Valor	Ata	Edital	Compra
-	Acesse a Ata	Acesse o Edital	Acesse a compra

Descrição Detalhada
REPASSE DE CONHECIMENTO (HANDS ON)

Nº	Inciso	Nome	Quantidade	Unidade	Preço unitário	Data	Compõe
6	IV	ISH TECNOLOGIA S/A - Fornecedor	1		R\$ 231.244,9000	01/04/2024	Sim

Identificação do Fornecedor		Endereço Eletrônico
01707.536/0001-04		http://www.ish.com.br
Data da Cotação	Hora da Cotação	Validade da Cotação
01/04/2024	16:55	01/05/2024
Contato	Informações Adicionais	
Daniel Duarte (E-mail: daniel.duarte@ish.com.br)	-	
Anexos		
PT 2024040100 - Presidencia - BIG IP.pdf		

Nº	Inciso	Nome	Quantidade	Unidade	Preço unitário	Data	Compõe
7	IV	Global Sec. Tecnologia & Informação Ltda - Fornecedor	1		R\$ 293.300,0000	05/04/2024	Sim

Identificação do Fornecedor		Endereço Eletrônico
31.862.002/0001-13		www.globalsectecnologia.com.br
Data da Cotação	Hora da Cotação	Validade da Cotação
05/04/2024	15:20	05/07/2024
Contato	Informações Adicionais	
Gustavo Miranda ((61) 99810-7773; E-mail: comercial@globalsectecnologia.com.br)	-	
Anexos		
PC 2024 - 073 - Presidencia da Republica.pdf		

Legenda:  Compra Anulada ou Revogada.



PRESIDÊNCIA DA REPÚBLICA
Diretoria de Tecnologia

INTRODUÇÃO

A Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, dispõe “sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional”. Os requisitos mínimos que uma pesquisa será materializada em documento que conterà, no mínimo, os seguintes argumentos consignados no Art. 3º:

“CAPÍTULO II

ELABORAÇÃO DA PESQUISA DE PREÇO

Formalização

Art. 3º A pesquisa de preços será materializada em documento que conterà, no mínimo:

I - Descrição do objeto a ser contratado;

II - Identificação do (s) agente (s) responsável (is) pela pesquisa ou, se for o caso, da equipe de planejamento;

III - caracterização das fontes consultadas;

IV - Série de preços coletados;

V - Método estatístico aplicado para a definição do valor estimado;

VI - Justificativas para a metodologia utilizada, em especial para a desconsideração de valores inconsistentes, inexequíveis ou excessivamente elevados, se aplicável;

VII - memória de cálculo do valor estimado e documentos que lhe dão suporte; e

VIII - justificativa da escolha dos fornecedores, no caso da pesquisa direta de que dispõe o inciso IV do art. 5º.”

CONTEXTO

Tem-se que o objeto a aquisição de solução de equipamentos firewall de próxima geração e firewall de aplicação web, balanceador de carga e publicador de DNS, para proteção do perímetro da rede de dados, dos ativos de hardware e software e das aplicações web da Presidência da Republica, compreendendo gerência centralizada, instalação e configuração da solução, com garantia e suporte técnico pelo período de 60 (sessenta) meses, conforme consignado no Documento de Formalização da Demanda 1 (SUPER nº 4413692), de 14 de julho de 2023. Abaixo tem-se um resumo dos principais campos da demanda necessários para subsidiar a presente pesquisa de preços:

1. Identificação da Demanda	Aquisição de soluções de segurança de redes compostas de firewall de aplicação (camada de aplicação) do tipo Web Application Firewalls (WAFs), para prover segurança de proteção da rede e dos sistemas e aplicações web, contemplando gerência unificada, serviço de instalação, configuração, repasse de conhecimento (treinamento), suporte e garantia de funcionamento pelo período de 60 (sessenta) meses
2. Justificativa da	Necessidade de atualização tecnológica das soluções de segurança de redes, sistemas e aplicações web atuais, garantindo a redução de ataques e

necessidade da contratação, considerando o Planejamento Estratégico, se for o caso	vulnerabilidades dos serviços da rede de computadores, sistemas e aplicações web, com controles de segurança abrangentes e política uniforme, motivada principalmente pelo vencimento da garantia dos equipamentos existentes em 29/12/2023
3. Quantidade a ser contratada	01 (uma) Solução separado em 03 (três) itens

Dentre os possíveis códigos CATMAT ativos existentes no Catálogo de Materiais e Serviços, aqueles que melhor se enquadram ao objeto da aquisição referente ao Itens consignados, são os Códigos **nº 481646**, **nº 27090**, **nº 027111** e **nº 016837**.

1. Identificação da Demanda	Grupo	Item	Código CATMAT/CATSER	Descrição do Código CATMAT/CATSER
Aquisição de solução de equipamentos firewall de Aplicação (WAF)	Único	nº 1	481646	Equipamento Segurança Rede Tipo: Amppliance, Aplicação: Firewall
			27090	Outros Serviços para a Infraestrutura de Tecnologia da Informação e Comunicação (TIC)
		nº 2	027111	Serviços de Instalação de Computadores e seus Periféricos
		nº 3	016837	Treinamento Informática - Equipamento / Hardware

Considerando as informações acima, os códigos CATMAT/CATSER e a quantidade a ser contratada, utilizou-se o módulo Pesquisa de Preços, do sistema Compras.gov.br, conforme preceitua o Art. 23, §1º, incisos I e II da Lei nº 14.133, de 1º de abril de 2021:

"Art. 23. O valor previamente estimado da contratação deverá ser compatível com os valores praticados pelo mercado, considerados os preços constantes de bancos de dados públicos e as quantidades a serem contratadas, observadas a potencial economia de escala e as peculiaridades do local de execução do objeto.

§ 1º No processo licitatório para aquisição de bens e contratação de serviços em geral, conforme regulamento, o valor estimado será definido com base no melhor preço aferido por meio da utilização dos seguintes parâmetros, adotados de forma combinada ou não:

I - Composição de custos unitários menores ou iguais à mediana do item correspondente no painel para consulta de preços ou no banco de preços em saúde disponíveis no Portal Nacional de Contratações Públicas (PNCP);

II - Contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;"

O Art. 5º, Inciso I, da Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, também traz dispositivo no mesmo sentido:

"Art. 5º A pesquisa de preços para fins de determinação do preço estimado em processo licitatório para a aquisição de bens e contratação de serviços em geral será realizada mediante a utilização dos seguintes parâmetros, empregados de forma combinada ou não:

I - Composição de custos unitários menores ou iguais à mediana do item correspondente nos sistemas oficiais de governo, como Painel de Preços ou banco de preços em saúde, observado o índice de atualização de preços correspondente;

II - Contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços,

observado o índice de atualização de preços correspondente;

III - dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que atualizados no momento da pesquisa e compreendidos no intervalo de até 6 (seis) meses de antecedência da data de divulgação do edital, contendo a data e a hora de acesso;

IV - Pesquisa direta com, no mínimo, 3 (três) fornecedores, mediante solicitação formal de cotação, por meio de ofício ou e-mail, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital; ou

V - Pesquisa na base nacional de notas fiscais eletrônicas, desde que a data das notas fiscais esteja compreendida no período de até 1 (um) ano anterior à data de divulgação do edital, conforme disposto no Caderno de Logística, elaborado pela Secretaria de Gestão da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia.

§ 1º Deverão ser priorizados os parâmetros estabelecidos nos incisos I e II, devendo, em caso de impossibilidade, apresentar justificativa nos autos.

§ 2º Quando a pesquisa de preços for realizada com fornecedores, nos termos do inciso IV, deverá ser observado:

I - Prazo de resposta conferido ao fornecedor compatível com a complexidade do objeto a ser licitado;

II - Obtenção de propostas formais, contendo, no mínimo:

a) descrição do objeto, valor unitário e total;

b) número do Cadastro de Pessoa Física - CPF ou do Cadastro Nacional de Pessoa Jurídica - CNPJ do proponente;

c) endereços físico e eletrônico e telefone de contato;

d) data de emissão; e

e) nome completo e identificação do responsável.

III - informação aos fornecedores das características da contratação contidas no art. 4º, com vistas à melhor caracterização das condições comerciais praticadas para o objeto a ser contratado; e

IV - Registro, nos autos do processo da contratação correspondente, da relação de fornecedores que foram consultados e não enviaram propostas como resposta à solicitação de que trata o inciso IV do caput.

§ 3º Excepcionalmente, será admitido o preço estimado com base em orçamento fora do prazo estipulado no inciso II do caput, desde que devidamente justificado nos autos pelo agente responsável e observado o índice de atualização de preços correspondente."

PESQUISA DE PREÇOS

Considerando o disposto no Art. 5º, § 1º da Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, foi priorizado os valores obtidos a partir do módulo Painel de Preços do sistema Compras.gov.br e das propostas comerciais similares, via solicitação de cotação de preços, em conformidade com o inciso IV do art. 5º da Instrução Normativa SEGES/ME nº 65. Por conseguinte, não foi realizada consultas em sítios eletrônicos especializados.

Foram solicitadas propostas de cotação de preços para as seguintes empresas:

a) **ISH** Tecnologia S/A, CNPJ nº 01.707.536/0001-04; (encaminhou proposta comercial)

b) **GLOBAL SEC.** Tecnologia & Informação Ltda., CNPJ nº 31.862.002/0001-13); (encaminhou proposta comercial)

c) **NIVA** Tecnologia da Informação Ltda., CNPJ nº 09.053.350/0001-90; (encaminhou proposta comercial)

d) **EVERY TI** Tecnologia & Inovação Ltda., CNPJ nº 08.925.028/0001-41. (encaminhou proposta comercial)

A cotação encaminhada pela empresa **NIVA** Tecnologia da Informação Ltda., CNPJ nº 09.053.350/0001-90, no valor de **R\$ 7.661.025,00** (sete milhões, seiscentos e sessenta e um mil vinte e cinco reais), foi descartada por apresentar valores excessivamente elevados.

A cotação encaminhada pela empresa **EVERY TI** Tecnologia & Inovação Ltda., CNPJ nº 08.925.028/0001-41, no valor de **R\$ 7.250.075,00** (sete milhões, duzentos e cinquenta mil setenta e cinco reais), foi descartada por apresentar valores excessivamente elevados.

Na Lista de cotações realizadas para os itens desejados, foram adotados os seguintes critérios:

a) Foram identificadas **3** (três) cotações para o Item nº 01, **6** (seis) cotações para o Item nº 02 e **7** (sete) cotações para o Item nº 03, todas com especificações similares as necessidades da Presidência da República;

a.1) Das **3** (três) cotações do Item nº 01, **2** (duas) cotações foram obtidas por intermédio das cotações encaminhadas pelas empresas **ISH** e **GLOBAL SEC**.

a.2) Das **6** (seis) cotações do Item nº 02, **2** (duas) cotações foram obtidas por intermédio das cotações encaminhadas pelas empresas **ISH** e **GLOBAL SEC**.

a.3) Das **7** (sete) cotações do Item nº 03, **2** (duas) cotações foram obtidas por intermédio das cotações encaminhadas pelas empresas **ISH** e **GLOBAL SEC**.

b) As cotações que apresentaram valores inexequíveis, inconsistentes, excessivamente elevados e com especificações técnicas inferiores (capacidade de armazenamento) as necessidades da Presidência da República, foram descartados os termos do caput do Art. 6º da Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021:

“Art. 6º Serão utilizados, como métodos para obtenção do preço estimado, a média, a mediana ou o menor dos valores obtidos na pesquisa de preços, desde que o cálculo incida sobre um conjunto de três ou mais preços, oriundos de um ou mais dos parâmetros de que trata o art. 5º, desconsiderados os valores inexequíveis, inconsistentes e os excessivamente elevados.

§ 1º Poderão ser utilizados outros critérios ou métodos, desde que devidamente justificados nos autos pelo gestor responsável e aprovados pela autoridade competente.

§ 2º Com base no tratamento de que trata o caput, o preço estimado da contratação poderá ser obtido, ainda, acrescentando ou subtraindo determinado percentual, de forma a aliar a atratividade do mercado e mitigar o risco de sobrepreço.

§ 3º Para desconsideração dos valores inexequíveis, inconsistentes ou excessivamente elevados, deverão ser adotados critérios fundamentados e descritos no processo administrativo.

§ 4º Os preços coletados devem ser analisados de forma crítica, em especial, quando houver grande variação entre os valores apresentados.

§ 5º Excepcionalmente, será admitida a determinação de preço estimado com base em menos de três preços, desde que devidamente justificada nos autos pelo gestor responsável e aprovada pela autoridade competente.

§ 6º Quando o preço estimado for obtido com base única no inciso I do art. 5º, o valor não poderá ser superior à mediana do item nos sistemas consultados. ”

Das **3** (três) cotações para o Item nº 01, **6** (seis) cotações para o Item nº 02 e **7** (sete) cotações para o Item nº 03, obteve-se os seguintes valores unitários:

MAPA COMPARATIVO DE PESQUISA DE PREÇOS (COMPLEMENTAR)

Descrição: Solução de Firewall de Aplicação Web (Web Application Firewall)

NOME DO PRODUTO/ÓRGÃO/FORNECEDOR				ISH TECNOLOGIA S/A		GLOBAL SEC TECNOLOGIA LTDA		SUPERIOR TRIBUNAL DE JUSTICA/DF		MÉDIA	MEDIANA	MENOR PREÇO	PREÇO UNITÁRIO REFERÊNCIA (R\$)	VALOR TOTAL DOS ITENS (R\$)
Item	Descrição do Material	Unidade	QTDE	Preço Unitário (R\$)	Valor Total (R\$)	Preço Unitário (R\$)	Valor Total (R\$)	Preço Unitário (R\$)	Valor Total (R\$)	(R\$)	(R\$)	(R\$)		
1	Solução de Firewall de Aplicação Web (Web Application Firewall), com 2 unidades FS BIG IP R4800, com licenciamento Premium Service e License BEST Bundle, com BIG-IP VE + BIG-IP Data Collection Device (DCD) e com suporte técnico e garantia de 60 meses	Solução	1	5.219.848,37	5.219.848,37	5.584.600,00	5.584.600,00	2.849.077,00	2.849.077,00	4.551.175,12	5.219.848,37	2.849.077,00	4.551.175,12	4.551.175,12
Total (R\$)														4.551.175,12

NOME DO PRODUTO/ÓRGÃO/FORNECEDOR				COMANDO DO EXERCITO (UASG 160528, ITEM 25)		JUSTICA ELEITORAL (UASG 90026)		ISH TECNOLOGIA S/A		GLOBAL SEC TECNOLOGIA LTDA		MÉDIA	MEDIANA	MENOR PREÇO	PREÇO UNITÁRIO REFERÊNCIA (R\$)	VALOR TOTAL DOS ITENS (R\$)
Item	Descrição do Material	Unidade	QTDE	Preço Unitário (R\$)	Valor Total (R\$)	Preço Unitário (R\$)	Valor Total (R\$)	Preço Unitário (R\$)	Valor Total (R\$)	Preço Unitário (R\$)	Valor Total (R\$)	(R\$)	(R\$)	(R\$)		
2	Serviço de instalação e configuração da Solução de firewall de aplicação Web	Serviço	1	60.000,00	60.000,00	66.040,00	66.040,00	112.102,04	112.102,04	216.100,00	216.100,00	113.560,51	89.071,02	60.000,00	113.560,51	113.560,51
Total (R\$)																113.560,51

NOME DO PRODUTO/ÓRGÃO/FORNECEDOR				ESTADO DO PARA (UASG 980595)		MINISTERIO DA CULTURA (UASG 420001)		ISH TECNOLOGIA S/A		GLOBAL SEC TECNOLOGIA LTDA		MÉDIA	MEDIANA	MENOR PREÇO	PREÇO UNITÁRIO REFERÊNCIA (R\$)	VALOR TOTAL DOS ITENS (R\$)
Item	Descrição do Material	Unidade	QTDE	Preço Unitário (R\$)	Valor Total (R\$)	Preço Unitário (R\$)	Valor Total (R\$)	Preço Unitário (R\$)	Valor Total (R\$)	Preço Unitário (R\$)	Valor Total (R\$)	(R\$)	(R\$)	(R\$)		
3	Treinamento da solução (8 participantes)	Serviço	1	218.430,00	218.430,00	139.000,00	139.000,00	231.244,90	231.244,90	293.300,00	293.300,00	220.493,73	224.837,45	139.000,00	139.000,00	139.000,00
Total (R\$)																139.000,00
Total do Grupo Único														R\$ 4.803.735,63		

Fonte: Relatório de Pesquisa de Preço - Relatório Detalhado - Cotação-Detalhado-41-2024, v10

Consolidação dos preços cotados - em R\$

Grupo	Item	Código CATMAT	Menor preço	Média	Mediana	Maior preço
Único	nº 1	481646/27090	R\$ 2.849.077,00	R\$ 4.551.175,12	R\$ 5.219.848,37	R\$ 5.584.600,00
	nº 2	027111	R\$ 60.000,00	R\$ 113.560,51	R\$ 89.071,02	R\$ 216.100,00
	nº 3	016837	R\$ 139.000,00	R\$ 220.493,72	R\$ 224.837,45	R\$ 293.300,00
Total			R\$ 3.048.077,00	R\$ 4.885.229,35	R\$ 5.533.756,84	R\$ 6.094.000,00
Valor Total de Referência			R\$ 4.803.735,63			

Tem-se que o valor total unitário de referência será o somatório das **MÉDIAS** dos Itens nº **01** e nº **02** e do **MENOR PREÇO** do Item nº **03**, totalizando o valor de **R\$ 4.803.735,63** (quatro milhões, oitocentos e três mil setecentos e trinta e cinco reais e sessenta e três centavos).

A estratégia utilizada visa mitigar o prejuízo de aquisição com valores superiores ao praticado no mercado, bem como evitar que a futura licitação tenha resultado fracassado por impor preços abaixo do praticado, fato ocorrido no Pregão Eletrônico nº 67/2023 (Grupo 2), além de estar em inerente consonância com as recomendações proferidas pela Governança da Diretoria de Tecnologia da Presidência da República.

Relativamente ao tema, de acordo com o Acórdão 4925/2012 - Plenário, a definição da metodologia de referência para estabelecer preços é **discricionária da Administração**.

ESCLARECIMENTOS COMPLEMENTARES

Convém deixar registrado que o **Grupo 2** (Aquisição de Solução de Equipamentos Firewall WAF), do Pregão Eletrônico nº 67/2023), processo SEI nº 00094.000392/2023-18, foi fracassado e homologado, em 15/01/2024, em virtude dos valores disputados e ofertados pelos participantes ficarem acima do valor de referência de **R\$ 1.585.302,00** (um milhão, quinhentos e oitenta e cinco mil trezentos e dois reais), ocasionando assim a desclassificação de todas as propostas lançadas no citado certame.

Sobre o fracassado do **Grupo 2**, a equipe de planejamento da contratação revisou todos os artefatos, em especial, o encarte das **Especificações Técnicas**, onde foi possível identificar alguns dos prováveis motivos que

levaram apurar a diferença de preços entre a estimativa da licitação fracassada (R\$ 1.585.302,00) e a estimativa do presente processo de **R\$ 4.803.735,63** (quatro milhões, oitocentos e três mil setecentos e trinta e cinco reais e sessenta e três centavos). Exemplificando, um dos prováveis motivos foi a utilização de cotações de preços incompatíveis com o objeto do processo SEI nº 00094.000097/2024-34 (novo), apesar da compatibilidade das descrições dos CATMAT e CATSER utilizados no processo fracassado.

Detalhando melhor a revisão promovida pela equipe de planejamento da contratação, foram incluídos dois novos item ao encarde das Especificações Técnicas: **Item 11 - Suporte Técnico**, com destaque para o Instrumento de Medição de Resultado (IMR), com sua classificação de severidades (Alta, Média e Baixa), bem como as multas em caso de atraso na prestação dos serviços e o **Item 12 - Capacitação**, com destaque para obrigatoriedade de que o instrutor que ministrará a capacitação da solução possua certificação oficial do fabricante da solução ofertada.

CONCLUSÃO

Por fim, considerando os quantitativos unitários dos Itens nº 01, nº 02 e nº 03 que compõem o Grupo Único, tem-se que o valor máximo total estimado para a contratação será a multiplicação desse quantitativo pelo valor unitário de referência. Logo, o valor máximo total estimado para a futura contratação será de **R\$ 4.803.735,63** (quatro milhões, oitocentos e três mil setecentos e trinta e cinco reais e sessenta e três centavos).

Brasília, 03 de julho de 2024.

NELSON GONCALVES REZENDE
Integrante Técnico
Matrícula SIAPE nº 8686325

Relatório emitido em 03/07/2024 17:14

Memória de cálculo (Art.3º, inciso VII – IN SEGES/ME nº 65, de 7 de julho de 2021):

- Média: corresponde à soma dos valores das amostras que compõem a pesquisa, dividida pelo número de amostras que compõem a pesquisa.
- Mediana: medida de tendência central das amostras que compõem a pesquisa que corresponde ao valor central do conjunto de valores extraídos.
- Desvio Padrão: É a raiz quadrada da variância de X ou também conhecido como a raiz quadrada do valor médio entre $(X-\mu)^2$, onde μ representa a média aritmética dos valores que compõem a pesquisa.

$$D = \sqrt{\frac{\sum_{i=1}^n (x - \mu)^2}{n}}$$

- Coeficiente de variação: É uma medida de dispersão calculada entre a divisão do desvio padrão e a média aritmética dos valores que compõem a pesquisa.

$$CV = \frac{D}{\mu}$$

Anexo VIII - ETP25_2024, vAssinado.pdf

Estudo Técnico Preliminar 25/2024

1. Informações Básicas

Número do processo: 00094.000097/2024-34

2. Introdução

2.1. Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no DFD-Doc de Formalização da Demanda TIC-L14133/21 14 (SUPER nº 4907637), 29 de janeiro de 2024, e Documento de Formalização da Demanda nº 248/2023 - Aquisição de Solução de Firewall de Rede, atualizado (SUPER nº 5718054), bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

3. Descrição da necessidade

3.1. Aquisição de solução de equipamento firewall de aplicação web, para proteção do perímetro da rede de dados, dos ativos de hardware e software e das aplicações web da Presidência da República, compreendendo gerência centralizada, instalação e configuração da solução, com garantia e suporte técnico pelo período de 60 (sessenta) meses, conforme condições, quantidades e exigências estabelecidas neste Estudo Técnico e seus anexos.

3.2. Contextualização

3.2.1. Em 2015, a Presidência da República contratou a solução de firewall de aplicação web, por intermédio do processo nº 00094.001125/2015-40, Contrato Administrativo nº 206/2015, com garantia e suporte de software e hardware do fabricante por 48 meses.

3.2.2. Em 13/06/2019, o suporte do fabricante ao software e ao hardware encerrou, gerando a necessidade da instrução de um novo processo licitatório, sob nº 00094.000279/2019-48, para a contratação de serviço para garantir as atualizações corretivas e evolutivas desta solução, bem como garantir a manutenção do hardware utilizado pela solução durante o novo período de vigência contratual. Essa necessidade originou o Contrato Administrativo nº 58/2020, firmado entre a Presidência da República e a empresa ISH Tecnologia S/A, com vigência de 29/12/2020 a 29/12/2023, ou seja, por 36 meses. Portanto, em 29 de dezembro de 2023, se encerrou o suporte de software e hardware do equipamento do fabricante f5.

3.2.3. A aquisição de Solução de Equipamento Firewall de Aplicação Web (WAF), foi objeto do Pregão Eletrônico nº 67/2023, promovida pela Diretoria de Tecnologia, com sessão pública realizada em 21/12/2023, às 09:30h (horário de Brasília). Todavia, somente o **Grupo 1** - Aquisição de Solução de Equipamentos Firewall de Próxima Geração (NGFW) foi homologada e adjudicada pela autoridade competente. O **Grupo 2** - Aquisição de Solução de Equipamentos Firewall de Aplicação Web (WAF) restou fracassado e homologado pela autoridade competente, já que os interessados não preenchem os requisitos estipulados pelo edital do Pregão Eletrônico nº 67/2023.

3.2.4. Cabe aqui um esclarecimento quanto ao valor apurado na cotação de preços, consignado na Cotação-Detalhada-381/2023, onde o valor do somatório das medianas dos item nº 01, nº 02 e nº 3, ficou muito aquém dos valores ofertados no Pregão Eletrônico nº 67/2023, fato que resultou no fracasso da licitação.

3.3. Tendo em vista o encerramento do suporte e garantia da solução de firewall de aplicação web e o fracasso do **Grupo 2** - Aquisição de Solução de Equipamentos Firewall de Aplicação Web (WAF) do edital do Pregão Eletrônico nº 67/2023, se faz necessária a instrução de processo licitatório para a contratação de aquisição da citada solução que visa proteger o perímetro interno e externo da Presidência da República, sendo capaz de gerir o controle do tráfego de dados e proteger contra malwares e outras ameaças de forma pró ativa e eficiente.

3.4. A referida solução é essencial para a análise e bloqueio dos ataques cibernéticos, direcionados aos portais e sistemas hospedados na infraestrutura tecnológica desta Presidência da República.

4. Área requisitante

Área Requisitante	Responsável
Diretoria de Tecnologia, da Secretaria de Administração, da Secretaria-Executiva da Casa Civil	Bruno Pereira Pontes
Coordenação-Geral de Infraestrutura Tecnológica, da Diretoria de Tecnologia	Walter Lopes Neto

5. Necessidades de Negócio

- 5.1. Aquisição de solução de firewall de aplicação web (WAF), provendo visibilidade detalhada e controle do tráfego e proteção da rede.
- 5.2. Prover proteção contra-ataques que explorem vulnerabilidade das aplicações da Presidência da República.
- 5.3. Prover proteção contra-ataques na borda da rede da Presidência da República, por meio da inspeção do tráfego de entrada e saída da rede.
- 5.4. Alta disponibilidade das soluções de proteção da rede.
- 5.5. Garantir o acesso balanceado e otimizado às aplicações.
- 5.6. Prover performance e acesso seguro e confiável às aplicações.
- 5.7. Garantir a publicação na internet das aplicações da Presidência da República.
- 5.8. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).
- 5.9. Manter a integridade dos dados e das informações sensíveis dos sistemas da Presidência da República.
- 5.10. Melhorar o nível de qualidade do serviço das aplicações internas da Presidência da República.
- 5.11. Melhorar a experiência do usuário ao acessar os serviços da Presidência da República fora da rede interna.
- 5.12. Prover o acesso com segurança a rede corporativa dos empregados em trabalho remoto.
- 5.13. Atender à Política de Segurança da Informação nos Órgãos e Entidades da Administração Pública Federal.
- 5.14. Garantir a qualidade, o desempenho e a alta disponibilidade das informações e dos equipamentos da Presidência da República.
- 5.15. Garantir a continuidade dos serviços aos usuários da Presidência da República.
- 5.16. Manter a infraestrutura de alto desempenho adequada para o tráfego de informações e sistemas críticos de TIC.
- 5.17. Manter o licenciamento em conformidade com o parque tecnológico.
- 5.18. Manter o parque tecnológico atualizado e padronizado.
- 5.19. Obter atualizações, correções e evoluções durante o período de vigência do contrato.

5.20. Capacidade de suportar ataques e ajustar o ambiente para fazer frente as mudanças ou restabelecimento dos serviços de forma mais célere em caso de problemas na rede.

5.21. Prover escalabilidade, redundância e resiliência para os serviços de tecnologia da informação da Presidência da República.

5.22. Prover disponibilidade, integridade, confidencialidade e autenticidade dos dados e informações.

5.23. Detalhamento dos Bens, Soluções e Serviços.

5.23.1. O detalhamento das especificações e características dos bens, solução e serviços decorrentes, se encontram consignados no Anexo I, do presente Estudo.

6. Necessidades Tecnológicas

6.1. Firewall de Aplicação Web - WAF

6.1.1. O WAF é um tipo de firewall criado para combater as ameaças que estão além das capacidades dos firewalls tradicionais. Ele cria uma barreira entre o seu serviço baseado na web e todo o resto da Internet, bloqueando e protegendo sua aplicação de ações criminosas, como manipulação de conteúdo exibido, conhecida como “pixação”, injeções indevidas em banco de dados de padrão SQL (Structured Query Language) ou simplesmente “SQL Injection”, determinados tipos de fraudes em acesso administrativo e várias outras espécies de ciberataques.

7. Demais requisitos necessários e suficientes à escolha da solução de TIC

7.1. Melhorar substancialmente o nível de segurança da informação da Presidência da República.

7.2. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7.3. Prover gestão e visibilidade relacionado as vulnerabilidades dos dispositivos.

7.4. Melhorar a experiência do usuário no acesso externo ao ambiente da Presidência da República.

7.5. Gerenciar as aplicações com políticas e controles baseado nas normativas de segurança e na LGPD.

7.6. Garantia e suporte técnico por 60 meses.

7.7. Equipamentos devem manter-se funcional após vencimento de licenças.

7.8. Manter base local de assinaturas de segurança após o vencimento das licenças.

7.9. Requisitos sociais, ambientais e culturais.

7.9.1. Os profissionais da CONTRATADA deverão trajar-se de maneira adequada, quando no ambiente da Presidência da República, e usar linguagem respeitosa e formal no trato com a Gestão e/ou Fiscalização Contratual, os dirigentes da Presidência da República e usuários, em consonância com as regras e normas internas.

7.9.2. Os serviços prestados pela CONTRATADA deverão pautar-se sempre no uso racional de recursos e equipamentos, de modo a evitar e prevenir o desperdício de insumos e material.

7.9.3. A CONTRATADA deverá atender, no que couber, os critérios de sustentabilidade ambiental previstos na Instrução Normativa SGD nº 94, de 23 de dezembro de 2022.

7.10. Requisitos de adequação do ambiente da Presidência da República para viabilizar a execução contratual

7.10.1. Será necessário disponibilizar espaço para acomodação dos equipamentos e acessórios na Coordenação de Centro de Dados, da Diretoria de Tecnologia, Anexo I, do Palácio do Planalto, Brasília/DF.

7.10.2. Os racks de equipamentos deverão ter um espaço de 1 U por equipamento e infraestrutura elétrica e de climatização necessária.

7.11. Requisitos de Capacitação

7.11.1. A transferência de conhecimento deve garantir que toda a informação gerada durante os processos de instalação e migração seja integralmente apresentada pela equipe da contratada, por meio de métodos expositivos, realização prática das atividades, apresentação de resumos, esquemas, relatórios ou qualquer outro documento que viabilize ou facilite a absorção da tecnologia do novo ambiente pela equipe da contratante.

7.12. Requisitos Legais

7.12.1. Deverão ser cumpridos os procedimentos, normas, modelos e regulamentos vigentes na Presidência da República.

7.12.2. O presente processo de contratação deve estar aderente à Constituição da República Federativa do Brasil de 1988 e as seguintes legislações vigentes:

7.12.2.1. Lei nº 14.133, de 1º de abril de 2021 (Nova Lei de Licitações);

7.12.2.2. Lei nº 13.709/2018: Lei Geral de proteção de Dados Pessoais - LGPD, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

7.12.2.3. Decreto nº 10.024, de 20 de setembro de 2019, regulamenta os novos procedimentos para realização do pregão eletrônico nas aquisições de bens e contratações de serviços comuns, inclusive serviços comuns de engenharia, bem como dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal;

7.12.2.4. Instrução Normativa nº 40, de 22 de maio de 2020, dispõe sobre a elaboração dos Estudos Técnicos Preliminares - ETP - para a aquisição de bens e a contratação de serviços e obras, no âmbito da Administração Pública federal direta, autárquica e fundacional, e sobre o Sistema ETP digital;

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

7.12.2.6. Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, estabelece o modelo de contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

7.13. Requisitos de Garantia, Suporte e Manutenção

7.13.1. O prazo de execução da garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, 60 meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data da assinatura do termo de recebimento definitivo do objeto.

7.13.2. O prazo de execução contratual do suporte e manutenção, é de, no mínimo, 60 meses, contado a partir do primeiro dia útil subsequente à data da assinatura do termo de recebimento definitivo do objeto.

7.13.3. A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

7.13.4. A garantia abrange a realização da manutenção corretiva dos bens pela própria Contratada, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

7.13.5. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

7.13.6. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

7.13.7. A Contratada realizará a reparação ou substituição dos bens que apresentarem vício ou defeito.

7.13.8. Durante a execução contratual será possível a troca dos equipamentos por versão superiores as estabelecidas neste Termo de Referência, sem qualquer ônus adicional a CONTRATANTE, caso os produtos apresentem defeito no período de vigência contratual. Entretanto, é necessária aceitação prévia e formal da equipe de gestão e fiscalização contratual.

7.13.9. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da Contratada.

7.13.10. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

7.13.11. Os requisitos e procedimentos referentes a garantia e suporte da solução, encontram-se pormenorizados no Termo de Referência.

7.13.12. O detalhamento dos requisitos de garantia e suporte encontram-se pormenorizados no Termo de Referência.

7.13.13. Duração da garantia e suporte

7.13.13.1. Nos processos de aquisições de bens de Tecnologia da Informação - TI, devido às suas características técnicas e por serem investimentos de alto custo, será sempre necessário que esses bens sejam acompanhados de uma garantia e de suporte para fins de assegurar o perfeito funcionamento da solução.

7.13.13.2. Em orientações anteriores de “BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC”, a antiga Secretaria de Tecnologia da informação do Ministério do Planejamento (Portaria MP/STI nº 20 /2016) padronizou que, nas elaborações das especificações técnicas de ativos de TI, deveriam ser observados:

“1.2.1 Os ativos de TI devem ser adquiridos com garantia de funcionamento provida pelo fornecedor durante sua vida útil, salvo quando justificado o contrário e com relação ao ativo em específico.

1.2.2. Tal procedimento se justifica pelo fato de que, de forma geral a contratação, a posteriori, de serviços de manutenção para ativos fora de garantia, usualmente é mais onerosa para a Administração do que quando o bem é adquirido com garantia para toda sua vida útil. Ainda, os contratos de manutenção têm seus custos elevados na medida em que os bens mantidos se tornam obsoletos. Ou seja, quanto mais antigo for o ativo de TI, menor seu valor comercial e maior será seu custo de manutenção, devido à dificuldade de provimento de peças de reposição e do maior risco do fornecedor descumprir os níveis de serviço exigidos para reparo desses equipamentos.

1.2.3. Tem-se, portanto, que um dos fatores que para definição do posicionamento adequado da tecnologia (item 1.1) é o tempo de vida útil previsto para utilização do ativo e, por conseguinte, o tempo de garantia de funcionamento a ser contratado.”

7.13.13.3. Se estabeleceu também a vida útil dos Ativos de Rede, tais como servidores de rede, aplicação, equipamentos de backup, armazenamento, segurança, entre outros:

“1.4.5.1 Para aquisição de servidores de rede, aplicação, equipamentos de backup, armazenamento, segurança, entre outros, deve-se considerar o tempo de vida útil mínimo de 5 (cinco) anos para fins de posicionamento da tecnologia e de garantia de funcionamento.”

7.13.13.4. Ressalta-se que os equipamentos a serem adquiridos nessa contratação, firewalls de próxima geração e de aplicações Web, são equipamentos de rede, de segurança e de aplicação, e, portanto, considera-se o tempo de vida útil desses equipamentos de no mínimo 5 anos (60 meses), devendo ser adquiridos com garantia de funcionamento (suporte e garantia) provida pelo fornecedor durante sua vida útil.

8. Estimativa da demanda - quantidade de bens e serviços

8.1. Atualmente a Presidência da República conta com 2 (dois) firewall de aplicação Web do fabricante F5, modelo BIG-IP 7055 SERIES, 01 BIG-IP Virtual Edition, instalados no Centro de Dados, Anexo I, do Palácio do Planalto.

8.2. Quantidade de bens e serviços

8.2.1. Para atendimento às necessidades, será necessária 01 Solução de firewalls de aplicações web. Segue abaixo o quadro com a estimativa e demanda de soluções necessárias para o completo atendimento da necessidade da Presidência da República:

GRUPO	ITEM	DESCRIÇÃO	UNIDADE	QTDE	JUSTIFICATIVA/MEMÓRIA DE CÁLCULO
Único	1	Solução de Firewall de Aplicação Web (Web Application Firewall), com 2 unidades F5 BIG IP R4800, com licenciamento Premium Service e License BEST Bundle, com BIG-IQ VE + BIG-IQ Data Collection Device (DCD) e com suporte técnico e garantia de 60 meses	Solução	1	Quantitativo referente a 1 Solução que funcionará no Centro de Dados, Anexo I, do Palácio do Planalto, baseado na descrição e nos requisitos tecnológicos
	2	Serviço de instalação e configuração da Solução de firewall de aplicação Web	Serviço	1	Quantitativo referente a instalação e configuração da solução baseada nas melhores práticas: Solução de firewall de aplicação Web (Web Application Firewall) e seus componentes de segurança
	3	Treinamento da solução (8 participantes)	Serviço	1	1 Turma com 8 participantes

9. Levantamento de soluções

9.1. Solução 01: Aquisição de conjunto de equipamentos de forma separada.

9.1.1. Solução composta por um conjunto de equipamentos, appliances, que tratam, cada um, de uma funcionalidade específica. Neste caso a solução nunca será composta apenas por um equipamento e, portanto, apresentará maiores dificuldades de gerenciamento das funcionalidades, pois cada equipamento terá sua plataforma de gerência.

9.1.2. Pontos positivos desta solução:

- a) Estrutura da solução mais robusta possível;
- b) Apresenta a possibilidade de aquisição de appliance dedicado para apenas uma funcionalidade considerada essencial para estruturar ou adicionar a infraestrutura de rede existente, e que necessite maior robustez;
- c) Podem ser contratadas separadamente conforme a necessidade da Presidência da República.

9.1.3. Pontos negativos desta solução:

- a) Exige gerenciamento descentralizado das soluções, pois cada appliance apresenta sua plataforma própria de gerência;
- b) Necessita de equipe técnica maior e mais capacitada para operacionalização dos equipamentos;
- c) O custo de soluções segregadas geralmente é maior que as integradas;

d) Dificuldade para correlacionar e analisar eventos em plataformas distintas o que impacta no poder e na tempestividade da reação do órgão diante de incidentes de segurança;

e) Ocupam mais espaço no Data Center e apresentam maior consumo de energia.

9.1.4. A aquisição de equipamentos específicos para cada funcionalidade (balanceamento, filtro de pacotes, anti-malware, VPN, filtro de camada de aplicação ...) não é uma solução muito eficiente, pois dificultará o gerenciamento e correlação dos eventos de segurança, característica relevante das soluções mais integradas, o que pode dificultar a detecção, contenção e o tratamento de uma incidente de segurança, elevando o risco de vazamento de dados e indisponibilidade dos serviços. Além disso, exigirá muitos especialistas com conhecimento nos diversos equipamentos ou soluções adquiridas e apresentará mais custo de espaço e energia.

9.1.5. Dessa forma, essa solução **não é viável** para atender a necessidade a Presidência da República.

9.2. Solução 02: Aquisição de equipamento do tipo NGFW – Firewall Corporativo com a funcionalidade de firewall de aplicação web (WAF)

9.2.1. Nessa solução a funcionalidade de firewall de aplicações web ou proteção contra ataques de camada de aplicação é realizado pelo firewall de próxima geração e a topologia da borda é composta por dois clusters deste tipo de equipamento. O NGFW constitui-se de equipamento capaz de agregar as diversas funcionalidades de segurança entre Firewall, Antivírus, IDS /IPS, WebFilter e outros, apresentando correlacionamento de dados entre os resultados das diversas funcionalidades. Estes equipamentos podem realizar inspeção em camada de aplicação e utilizam a mesma plataforma de gerência para todas as funcionalidades. Porém a inspeção realizada da camada de aplicação não é comparável ao nível de granularidade de inspeção de um equipamento WAF dedicado que ainda disporá de balanceamento de carga e DNS. Em muitas situações, para contar nos NGFW com essa capacidade de inspeção do tráfego na camada de aplicação, faz-se necessário contratar licenciamento adicional para seu uso. O WAF dedicado garantirá maior capacidade de inspeção e análise dos pacotes de camada 7 evitando uma maior latência e desonerando o NGFW para outras análises, garantindo melhor throughput da rede.

9.2.2. Vejamos as principais diferenças entre o WAF, IPS e NGFW:

	Web Application Firewall	Intrusion Prevention System	Next-Generation Firewall
Multiprotocol Security			
IP Reputation			
Web Attack Signatures			
Web Vulnerabilities Signatures			
Automatic Policy Learning			
URL, Parameter, Cookie and Form Protection			
Leverage Vulnerability Scan Results			

9.2.3. A análise da Xlabs Security (<https://www.xlabs.com.br/>) da figura acima, demonstra que o WAF dedicado tem atuação melhor comparada ao NGFW e ao IPS no que refere-se a assinaturas de vulnerabilidades web, aprendizado automático de políticas, proteção granular de URLs (Universal Resource Location), parâmetros, cookies e formulários das aplicações e melhor resultado médio em busca de vulnerabilidades.

9.2.4. Pelo exposto, essa solução **não é viável** para o atendimento às necessidades de segurança cibernética da Presidência da República.

9.3. Solução 03: Aquisição de equipamento do tipo Firewall de Aplicações Web (WAF-Appliance)

9.3.1. Solução composta por firewall de aplicações web, balanceador e DNS. Constitui-se de equipamento capaz de agregar as diversas funcionalidades de segurança entre Firewall, Antivírus, IDS/IPS, WebFilter e outros, apresentando correlacionamento de dados entre os resultados das diversas funcionalidades. Estes equipamentos podem realizar inspeção em camada de aplicação e utilizam a mesma plataforma de gerência para todas as funcionalidades. Porém a inspeção realizada da camada de aplicação não é comparável ao nível de granularidade de inspeção de um equipamento WAF dedicado que ainda disporá de balanceamento de carga e DNS.

9.3.2. Pontos positivos desta solução:

- a) É uma evolução da já consolidada plataforma unificada do tipo UTM sendo, inclusive, muitas fornecidas pelos mesmos fornecedores de UTM;
- b) Plataforma de gerenciamento unificado para as diversas funcionalidades de segurança de redes;
- c) Possuem garantia de capacidade para análise do tráfego por funcionalidade;
- d) Apresentam o maior nível de visibilidade no monitoramento e controle de ameaças devido ao correlacionamento das informações provenientes das diferentes funcionalidades;
- e) Exige menor conhecimento técnico/operacional por parte da equipe uma vez que as ferramentas de gerenciamento já são mais intuitivas e direcionadas para a configuração dos principais cenários de segurança de redes;
- f) Apresentam praticamente todas as funcionalidades essenciais à estruturação de uma solução de segurança de redes computacionais;
- g) Apresentam, adicionalmente, a capacidade de detectar malwares e ameaças em um nível satisfatório;
- h) Podem ser adquiridas em diversos portes de capacidade conforme a capacidade da Presidência da República, resultando em formas mais eficientes de utilização dos recursos do equipamento e no custo de aquisição.

9.3.3. Pontos negativos desta solução:

- a) Podem gerar problemas no dimensionamento de capacidade da appliance uma vez que sua performance depende de quais funcionalidades estão ativadas.

9.3.4. Pelas razões supracitadas essa solução **mostrou-se viável e completa**, adequada e a solução viável para atendimento às necessidades de segurança cibernética da Presidência da República.

10. Análise comparativa de soluções

10.1. A análise comparativa das soluções foi realizada no Item 9 - Levantamento de Soluções. A solução considerada viável para atender as necessidades da Presidência da República é **Solução 03: Aquisição de equipamento do Tipo Firewall de Aplicações Web (WAF)**.

10.2. Análise da existência de software público brasileiro e adequação às políticas, os modelos e os padrões de governo:

Requisito	Solução	Sim	Não	Não se Aplica
Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 1	X		

A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 2	X		
	Solução 3	X		
A Solução é aderente às regulamentações da ICP Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X

11. Registro de soluções consideradas inviáveis

11.1. Conforme demonstrado no item 9 - Levantamento de Soluções, as seguintes soluções foram consideradas inviáveis:

- 11.1.1. Solução 01: Aquisição de conjunto de equipamentos de forma separada;
- 11.1.2. Solução 02: Aquisição de equipamento do tipo NGFW - Firewall Corporativo com a funcionalidade de firewall de aplicação web (WAF).

12. Análise comparativa de custos (TCO)

12.1. Descrição da Solução Viável: Aquisição de equipamentos do tipo Firewall de Aplicações Web - WAF (Solução 03).

12.1.1. A análise comparativa de custos foi elaborada considerando apenas as soluções técnicas e funcionalmente viáveis, nos termos do inc. III, Art. 11, da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, incluindo:

- a) cálculo dos custos totais de propriedade (Total Cost Ownership - TCO) por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução, a exemplo dos valores de aquisição dos ativos, insumos, garantia técnica estendida, manutenção, migração e treinamento; e
- b) memória de cálculo que referencie os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados.

12.1.2. Custo Total de Propriedade – Memória de Cálculo – Aquisição de Solução de Equipamentos Firewall de Aplicação (WAF):

Grupo	Item	Descrição	Código CATMAT	Qtde.	Menor Preço (R\$)	Média (R\$)	Mediana (R\$)	Maior Preço (R\$)
Único	1	Solução de Firewall de Aplicação Web (Web Application Firewall), com 2 unidades F5 BIG IP R4800, com licenciamento Premium Service e License BEST Bundle, com BIG-IQ VE + BIG-IQ Data Collection Device (DCD) e com suporte técnico e garantia de 60 meses	481646	1	3.187.090,00	4.663.846,12	5.219.848,37	5.584.600,00

	2	Serviço de instalação e configuração da Solução de firewall de aplicação Web	027111	1	60.000,00	116.540,34	89.071,02	216.100,00
	3	Treinamento da solução (8 participantes)	016837	1	100.000,00	182.943,84	163.632,00	293.300,00
Total					3.347.090,00	4.963.330,30	5.472.551,39	6.094.000,00
Valor Total de Referência					R\$ 4.880.386,46			

Obs.: Os valores apurados na tabela acima se encontram consignados na Planilha Comparativa de Preços 2024 - Cotação-Detalhado-41-2024 (SUPER nº 4956176)

12.1.3. Mapa Comparativo dos Cálculos Totais de Propriedade:

GR	IT	DESCRIÇÃO DA SOLUÇÃO	ESTIMATIVA DE TCO AO LONGO DOS ANOS (R\$)					TOTAL (R\$)
			ANO 1	ANO 2	ANO 3	ANO 4	ANO 5	
Único	1	Solução de Firewall de Aplicação Web (Web Application Firewall), com 2 unidades F5 BIG IP R4800, com licenciamento Premium Service e License BEST Bundle, com BIG-IQ VE + BIG-IQ Data Collection Device (DCD) e com suporte técnico e garantia de 60 meses	4.663.846,12	- X -	- X -	- X -	- X -	4.663.846,12
	2	Serviço de instalação e configuração da Solução de firewall de aplicação Web	116.540,34	- X -	- X -	- X -	- X -	116.540,34
	3	Treinamento da solução (8 participantes)	100.000,00	- X -	- X -	- X -	- X -	100.000,00
TOTAL			4.880.386,46	- X -	- X -	- X -	- X -	4.880.386,46

13. Descrição da solução de TIC a ser contratada

13.1. Solução de firewall de aplicações web (WAF) para prover as seguintes funcionalidades e controles de segurança:

- a) Filtro e inspeção de pacotes de camada 7;
- b) Balanceamento de carga das aplicações e DNS;
- c) Proteção contra ataques de camada 7;
- d) Publicação e balanceamento de DNS;
- e) Proteção Anti-DDoS.

13.2. A Solução de Firewall de Aplicação Web (WAF) proverá proteção contra ataques de camada de aplicação e de negação de serviços, além de publicar as aplicações da Presidência da República na Internet de forma otimizada e balancear o tráfego das aplicações entre os ativos de infraestrutura e rede da Presidência da República.

13.3. Parcelamento da solução

13.3.1. No contexto de obtenção de serviços pela administração pública, verificou-se que a legislação preza pela análise técnica e econômica para decidir sobre a divisão do objeto, senão vejamos:

Lei 14.133, Seção IV, Disposições Setoriais, Subseção I, Das Compras

"Art. 40. O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:

... § 2º Na aplicação do princípio do parcelamento, referente às compras, deverão ser considerados:

I - a viabilidade da divisão do objeto em lotes;"

13.3.2. O objeto desta contratação será em grupo único, por solução WAF e dividido em 03 itens, atendendo ao preceituado da citada Lei 14.133.

13.3.3. Um requisito fundamental para que haja viabilidade técnica e também administrativa da contratação em questão, é o de que o conjunto de serviços/soluções sejam agrupados e licitados em um único grupo, sendo assim com adjudicação para um único licitante vencedor, ou seja, não haverá parcelamento.

13.4. A definição pela contratação em grupo único, com três itens levou em consideração a viabilidade técnica de operação e gerenciamento da solução de firewall que funciona de forma integrada entre os appliances e a solução de gerência, faz-se necessário que esses itens façam parte de um mesmo agrupamento em um grupo, para garantir o gerenciamento e a interoperabilidade da operação sem prejuízos nas análises e correlação dos eventos.

14. Estimativa de custo total da contratação

Valor (R\$): 4.880.386,46

14.1. Memória de Cálculo = **R\$ 4.880.386,46** (quatro milhões, oitocentos e oitenta mil trezentos e oitenta e seis reais e quarenta e seis centavos).

15. Justificativa técnica da escolha da solução

15.1. Considera-se tecnicamente viável a **Solução 03** pelas necessidades de equipamentos para atenderem as demandas de segurança e gestão da rede da Presidência da República (PR), tendo em vista a descontinuidade dos serviços contratados (29 de dezembro de 2023).

15.2. Além de oferecer um nível maior de segurança à rede, os firewall de aplicação, com uma maior capacidade de processamento, possibilitam a implementação de novos serviços, como por exemplo, análise do tráfego. Com isso, seria possível ter uma visualização detalhada da utilização das aplicações utilizadas. Adicionalmente, o processo de identificação de ameaças são facilitados e permitem a aplicação de políticas de segurança mais eficientes.

15.3. Com o aumento no número de usuários trabalhando de casa e com o aumento na quantidade de ataques às empresas, principalmente na tentativa de sequestro de dados em troca de resgate, fez com que as necessidades do uso de firewalls para conter ataques de negação de serviço e bloquear infecções maliciosas, principalmente em casos de ataques de ransomware, aumentassem as necessidades de equipamentos capazes de comportarem uma maior e mais rápida análise do tráfego de dados na rede institucional.

16. Justificativa econômica da escolha da solução

16.1. Foi utilizado como parâmetro os preços do Painel de Preços do Governo Federal (<https://paineldepregos.planejamento.gov.br/>), no período de 05/04/2024 a 08/04/2024, com os seguintes códigos do CATMAT/CATSERV:

CATMAT/ CATSER	DESCRIÇÃO DO CATMAT/CATSER
016837	TREINAMENTO INFORMÁTICA - EQUIPAMENTO / HARDWARE
027111	SERVIÇOS DE INSTALAÇÃO DE COMPUTADORES E SEUS PERIFERICOS
481646	EQUIPAMENTO SEGURANÇA REDE, TIPO: AMPPLIANCE, APLICAÇÃO: FIREWALL

16.2. Deste modo, com os códigos acima com, foram coletados os dados e aplicado cálculo da média dos preços, obtendo-se o custo médio total estimado para a presente aquisição de **R\$ 4.880.386,46** (quatro milhões, oitocentos e oitenta mil trezentos e oitenta e seis reais e quarenta e seis centavos).

16.3. A contratação da **Solução 3** proporcionará continuidade do negócio para a Presidência da República, devido a seleção da melhor solução de segurança de perímetro para a infraestrutura de rede, tanto técnica e quanto economicamente, por um período de 60 meses.

17. Benefícios a serem alcançados com a contratação

17.1. A contratação visa obter principalmente os resultados abaixo:

17.1.1. Prover a Presidência da República uma estrutura de segurança da informação robusta incorporada por soluções de tecnologia modernas aptas para suportar todos os serviços prestados pela DITEC, e também, fornecer o alcance das necessidades do órgão fortalecendo a estratégia de segurança da informação contra ameaças avançadas de todos os tipos;

17.1.2. Garantir que a infraestrutura da rede da Presidência da República possua todos os requisitos necessários para atender as demandas internas da DITEC, e também tenha a possibilidade de ampliação de forma segura da capacidade tecnológica em demandas futuras;

17.1.3. Amplificação da camada de proteção e disponibilidade da informação;

17.1.4. Disponibilidade do ambiente de rede com segurança e visibilidade;

17.1.5. Ampliação da segurança da informação na Presidência da República;

17.1.6. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

17.1.7. Mitigação de riscos de ataques digitais;

17.1.8. Mitigação de riscos de paralização dos serviços de TI;

17.1.9. Aumento da confidencialidade, integridade, níveis de segurança da informação, da eficiência de monitoração de eventos de segurança e disponibilidade das informações;

17.1.10. Expansão da proteção atualmente existente para os novos equipamentos adquiridos ou em fase de aquisição;

17.1.11. Governança da segurança da informação em tempo próximo ao real;

17.1.12. Reter os eventos e informações de segurança em longo prazo, de acordo com as políticas da organização;

17.1.13. Reportar o estado de segurança e conformidade do ambiente de TI da Presidência da República;

17.1.14. Minimizar riscos relacionados à segurança da informação e da rede, de sistemas e de serviços corporativos;

17.1.15. Garantir a disponibilidade dos recursos do ambiente computacional da Presidência da República, além de otimizar o uso dos acessos à Rede WAN e Internet;

17.1.16. Prover a proteção da informação contra ameaças a sua confidencialidade, integridade e disponibilidade;

17.1.17. Reestruturar e modernizar a arquitetura de rede da Presidência da República;

- 17.1.18. Garantir a continuidade dos negócios da Presidência da República por intermédio de melhorias, apoio técnico e manutenções da solução a ser adquirida;
- 17.1.19. Aumentar a velocidade de conexão entre os servidores e ativos de rede do Data Center;
- 17.1.20. Prover solução de gerenciamento e monitoramento eficiente dos ativos de rede do Data Center;
- 17.1.21. Prover mecanismos de alta disponibilidade, mecanismos de segurança e balanceamento de carga entre Data Center;
- 17.1.22. Manter um ambiente licenciado, atualizado e acima de tudo seguro, levando em consideração problemas de vulnerabilidades e disponibilidade corrigidos em versões superiores as atuais.

18. Providências a serem Adotadas

18.1. Não há necessidade de adequação da infraestrutura tecnológica, elétrica, logística, espaço físico, mobiliário ou outras que se apliquem.

19. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

19.1. Justificativa da Viabilidade

19.1.1 A declaração da viabilidade da contratação expressa nesta seção apresenta a justificativa da solução escolhida, abrangendo a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade.

19.2. Nesse sentido, o planejamento em tela almeja os seguintes benefícios e resultados:

19.2.1. Proteção contra ataques aos serviços de TI da Presidência da República, mitigando riscos de indisponibilidade de serviços e vazamento de dados da Presidência da República. Otimização dos controles de segurança cibernética da pasta e alinhamento aos normativos de segurança da informação do Governo Federal e às melhores práticas e frameworks do mercado. Garantir a qualidade, o desempenho e a alta disponibilidade das informações e dos equipamentos da Presidência da República.

19.2.2. Economia no valor da aquisição.

19.3. Além disso, frisa-se que a presente contratação atende adequadamente às demandas de negócio formuladas, os benefícios a serem alcançados são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis.

19.4. Por fim, considerando as informações do presente estudo, entende-se que a presente contratação se configura tecnicamente VIÁVEL para a **Solução 03**.

20. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

NELSON GONCALVES REZENDE

Integrante Requisitante



Assinou eletronicamente em 07/06/2024 às 16:06:54.

JAN CARLOS RODRIGUES TELES

Integrante Técnico



Assinou eletronicamente em 12/06/2024 às 12:11:41.

ROBSON MARTINS GUIMARAES DA SILVA

Integrante Técnico



Assinou eletronicamente em 11/06/2024 às 10:08:31.

BRUNO PEREIRA PONTES

Autoridade competente



Assinou eletronicamente em 13/06/2024 às 16:39:49.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Especificações Técnicas - WAF, vSegunda.pdf (678.66 KB)

Anexo I - Especificações Técnicas - WAF, vSegunda.pdf

Especificações Técnicas

1. ESPECIFICAÇÕES TÉCNICAS

1.1. Para comprovação dos itens das especificações técnicas da solução, serão aceitos datasheets, documentos e cartas do fabricante dos produtos ou ainda registros da CLI (Command Line Interface) dos produtos que asseverem o atendimento aos requisitos.

1.2. A solução é composta por um cluster contendo 2 (dois) equipamentos do tipo Web Application Firewall (WAF), gerência centralizada, incluindo o fornecimento de licenças, o fornecimento de transceivers, serviços de instalação, configuração, transferência de conhecimento, garantia e suporte técnico.

1.3. Há uma grande variedade de fabricantes de Web Application Firewall. Entretanto, é importante reforçar que há um alto grau de complexidade na administração e gerenciamento destas ferramentas, e a portabilidade entre elas não é uma tarefa fácil nem rápida. A Presidência da República dispõe atualmente de equipamentos da fabricante F5 Networks, e esta equipe de planejamento da contratação considera que se deve manter o fabricante para o melhor benefício de todos os usuários que acessam os serviços da Presidência da República.

1.4. Tendo em vista que o esforço realizado numa eventual migração de equipamento para um novo fabricante acarretará em um risco de total indisponibilidade de todos os portais e serviços hospedados no Centro de Dados da Presidência da República.

1.5. Não há qualquer tipo de cerceamento da competitividade na definição do fabricante F5 para a garantia do melhor interesse da Presidência da República e para a lisura e competitividade de um procedimento licitatório idôneo, uma vez que existem ao menos 11 representantes autorizados pela fabricante para oferecerem os equipamentos solicitados, conforme pode ser observado no site do próprio fabricante: <https://www.f5.com/partners/find-a-partner?partnerLocation=Brazil&partnerPage=1>, acessado em 31 de outubro de 2023.

2. CARACTERÍSTICAS DO HARDWARE QUE CONTEMPLAM AS SEGUINTE FUNCIONALIDADES

2.1.1. Os appliances físicos devem ser novos e de primeiro uso;

2.1.2. Os equipamentos devem ser fornecidos em modo appliance, com conjunto de hardware e software dedicados, não podendo ser servidor de uso genérico, e que atendam todas as funcionalidades descritas nas Especificações técnicas mínimas;

2.1.3. Devem ser novos, sem uso prévio e entregues em perfeito estado de funcionamento. Não devem ser remanufaturados, recondicionados ou possuir reparos de qualquer espécie;

2.1.4. Não serão aceitos equipamentos ou softwares que constem em anúncio ou lista do tipo end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, produtos que serão descontinuados, perderão suporte e garantia oficiais do fabricante;

2.1.5. As funcionalidades da solução (balanceador de carga, global server load balancing, proteção para aplicação, proteção para a rede, proteção contra-ataque DDoS, DNS Application Firewall, inspeção SSL, etc) deverão ser licenciadas pelo período de 60 (sessenta) meses;

2.1.6. Deverão ser fornecidos no mínimo 2 appliances para o uso em alta disponibilidade, cada um contemplando as seguintes características/funcionalidades:

2.1.2. Distribuição de carga e otimização das aplicações.

2.1.3. Proteção contra-ataques de aplicação.

2.2. O equipamento deverá ser novo, de primeiro uso e acondicionado adequadamente em caixa lacrada de fábrica, de forma a propiciar completa segurança durante o transporte.

2.3. Equipamento do tipo appliance, possuir altura de, no máximo, 2U, deve ser instalado em rack de 19" e vem acompanhado do kit de instalação.

2.4. Processador mínimo octa core.

2.5. Possuir quantidade total de memória (RAM) de, no mínimo, 64 GB (sessenta e quatro Gigabytes).

2.6. Possuir placa dedicada a tratar tráfego SSL (hardware).

2.7. Possuir, no mínimo, um disco com 480GB de espaço de armazenamento do tipo SSD.

2.8. Possuir no mínimo 2 fontes hot swappable.

2.9. Mínimo de 01 (uma) porta console para configuração através de CLI (Command Line Interface) para cada appliance.

2.10. Possuir 1 (uma) interface Gigabit Ethernet para gerenciamento out-of-band.

2.11. Possuir, no mínimo, 4 (quatro) interfaces 1 (um) Gigabit em cobre, seja através de portas nativas ou de slots SFP com os devidos transceivers 1000BASE-T.

2.12. Deve possuir no mínimo, por appliance, 4 portas 25/10/1 GbE SPF+/SFP28/SPF ou no mínimo 6 portas 1/10 GbE SFP/SFP+ que permita fazer agregação das interfaces para comunicação com switches, em ambos os casos incluindo todos os respectivos transceivers.

2.13. Todas as portas de fibras referenciadas no item anterior devem vir em cada appliance acompanhadas dos respectivos transceivers e de 04 (quatro) cordões ópticos padrão lc/lc de no mínimo 5 metros multimodo e 04 (quatro) cordões ópticos padrão lc/lc de no mínimo 10 metros multimodo.

2.14. Desempenho por appliance:

- 2.14.1. Possuir capacidade para operar, no mínimo, 50/40 Gbps de tráfego na camada L4/L7;
- 2.14.2. Possuir capacidade de operar, no mínimo, 45.000 TPS de tráfego SSL com chaves de 2048 bits;
- 2.14.3. Possuir capacidade de operar, no mínimo, 20.000 TPS de tráfego SSL com chaves ECDSA P-256;
- 2.14.4. Possuir capacidade de operar, no mínimo, 25 Gbps de tráfego SSL;
- 2.14.5. Possuir capacidade de operar, no mínimo, 1.8 milhão de requisições por segundo na camada 7;
- 2.14.6. Possuir capacidade de operar, no mínimo, 750 mil conexões por segundo na camada 4;
- 2.14.7. Possuir capacidade de operar, até 38 milhões de conexões concorrentes L4;
- 2.14.8. Possuir painel de LCD frontal com funções básicas;
- 2.14.9. Possuir Compressão de Hardware de no mínimo 30 Gbps em tráfego HTTP/HTTPS;
- 2.14.10. Recursos de agregação de portas baseado no protocolo LACP em seus modos ativo e passivo;
- 2.14.11. Deve suportar, até 3.500.000 (três milhões e quinhentos mil) requisições HTTP por segundo na camada 4 do modelo OSI;
- 2.14.12. Deve suportar, no mínimo, 80.000.000 (oitenta milhões) de pacotes SYN/segundo, sob ataque de SYN Flood.

3. CARACTERÍSTICAS GERAIS PARA A SOLUÇÃO

- 3.1. Suportar e garantir a instalação em ambiente de alta disponibilidade.
- 3.2. Assegurar que o equipamento deverá ser capaz de trabalhar no modo Ativo/Standby, com equipamento da mesma marca e modelo.
- 3.3. A solução deve operar no modo Ativo/Ativo, mantendo o status das conexões. Aceita-se como Ativo/Ativo a utilização de dois endereços Virtuais, onde cada endereço fica ativo em um elemento e standby no outro.
- 3.4. Assegurar que a operação da solução de 2 ou mais equipamentos, quando implementada em ambiente redundante suporte sincronismo de sessão entre os dois membros. A falha do equipamento principal não deverá causar a interrupção das sessões balanceadas.
- 3.5. A solução deve fornecer todos os recursos possíveis de redundância sem nenhuma despesa com licenças adicionais.

- 3.6. A solução deve possuir escalabilidade, podendo crescer na forma de cluster adicionando novos appliances inclusive de modelos diferentes.
- 3.7. O equipamento deverá possuir sistema operacional certificado ICSA Labs podendo assim ser instalado na borda antes de qualquer equipamento de segurança.
- 3.8. A solução deve fornecer recurso de agregação de portas baseado no protocolo LACP.
- 3.9. Deve possuir suporte a LACP em modo passivo e ativo.
- 3.10. A solução deve fornecer recurso para suportar até 32 portas em um mesmo conjunto agregado.
- 3.11. Deve possuir suporte a Spanning-Tree (802.1D), Fast Spanning-Tree (802.1w, 802.1t) e Multi Spanning-Tree (802.1s).
- 3.12. Deve fornecer recurso para o transporte de múltiplas VLAN por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q.
- 3.13. Possuir suporte a IPv6.
- 3.14. A solução deve suportar múltiplas tabelas de rotas independentes.
- 3.15. O equipamento, quando habilitado para mais de uma função deverá permitir a definição da importância da função, determinando quanta CPU e memória será alocada para cada tipo de funcionalidade.
- 3.16. Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos.
- 3.17. A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6.
- 3.18. Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado da solução e informações preventivas.
- 3.19. Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software Defined Network).
- 3.20. Serviço de suporte técnico na modalidade de 24x7 (24 horas/dia e 7 dias/semana) durante 60 meses.
- 3.21. Na data da proposta e durante a vigência do contrato, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale.

3.22. Deve se integrar com sistemas de gerenciamento de containers (ex.:Kubernetes/Openshift), de modo a permitir que mudanças dinâmicas na infraestrutura de microsserviços sejam refletidas automaticamente no balanceamento de entrada, aumentando ou diminuindo a quantidade de pods, e ainda, inserindo ou removendo serviços do Big-IP.

3.23. Deve ser integrado nativamente ao Kubernetes/Openshift para realizar obalanceamento entre pods.

3.24. Deve criar os serviços de Balanceamento de Carga dinamicamente ao mesmo tempo em que uma nova aplicação é provisionada pelo Kubernetes/Openshift.

4. FUNCIONALIDADE DE GERENCIAMENTO

4.1. Implementar uma configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento.

4.2. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol).

4.3. Permitir acesso in-band via SSH.

4.4. Manter internamente múltiplos arquivos de configurações do sistema.

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

4.6. Possuir auto-complementação de comandos na CLI.

4.7. Possuir ajuda contextual.

4.8. Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos.

4.9. Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura.

4.10. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados.

4.11. Deverá ser possível receber da base RADIUS, LDAP e TACACS+ o nível de acesso (Grupo ou Permissões).

4.12. Possuir Interface Gráfica via Web.

4.13. A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando.

- 4.14. A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot.
- 4.15. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps).
- 4.16. Suportar o rollback de configuração e imagem.
- 4.17. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema.
- 4.18. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog.
- 4.19. Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento.
- 4.20. A interface Gráfica deverá permitir a reinicialização do equipamento.
- 4.21. Reinicialização do equipamento por comando na CLI.
- 4.22. Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3.
- 4.23. Possuir traps SNMP.
- 4.24. Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events.
- 4.25. Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo.
- 4.26. Implementar Debugging: CLI via console e SSH.
- 4.27. Deve possuir suporte a Link Layer Discovery Protocol (LLDP).
- 4.28. Deve ser possível enviar, pelo menos, as seguintes informações via LLDP: Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size.
- 4.29. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas.
- 4.30. A Solução deve ter suporte a sFlow.

5. DISTRIBUIÇÃO DE CARGA E OTIMIZAÇÃO DAS APLICAÇÕES

- 5.1. Suportar todas as aplicações comuns de um Switch Layer 7, como:
 - 5.1.1. Server Load-Balancing;

5.1.2. Firewall Load-Balancing;

5.1.3. Proxy Load-Balancing.

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

5.3. A solução de Load Balance deve possuir, no mínimo, capacidade de resposta aos clientes por roteamento direto (os servidores balanceados respondem diretamente aos clientes), tunelamento (a solução é capaz de utilizar servidores de redes diferentes da que está inserida) ou fullproxy (todas as transações entre clientes e servidores são intermediadas pela solução).

5.4. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente.

5.5. Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede.

5.6. Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação.

5.7. A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.

5.8. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.

5.9. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.

5.10. Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço.

5.11. Suportar os seguintes métodos de balanceamento:

5.11.1. Round Robin;

5.11.2. Least Connections;

5.11.3. Weighted Percentage (por peso);

- 5.11.4. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;
- 5.11.5. Weighted Percentage dinâmico (baseado no número de conexões);
- 5.11.6. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI.
- 5.12. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web.
- 5.13. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:
 - 5.13.1. Por cookie: inserção de um novo cookie na sessão;
 - 5.13.2. Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;
 - 5.13.3. Por endereço IP destino;
 - 5.13.4. Por endereço IP origem;
 - 5.13.5. Por sessão SSL;
 - 5.13.6. Através da análise da URL acessada;
 - 5.13.7. Através da análise de qualquer parâmetro no header HTTP;
 - 5.13.8. Através da análise do MS Terminal Services Session (MSRDP);
 - 5.13.9. Através da análise do SIP Call ID ou Source IP;
 - 5.13.10. Através da análise de qualquer informação da porção de dados (camada 7).
- 5.14. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH.
- 5.15. O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:
 - 5.15.1. Layer 3 – ICMP;
 - 5.15.2. Conexões TCP e UDP pela respectiva porta no servidor;
 - 5.15.3. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP (em especial Microsoft AD), IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI.

- 5.16. Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY).
- 5.17. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real.
- 5.18. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual.
- 5.19. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores.
- 5.20. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico:
- 5.20.1. Realizar Network Address Translation (NAT);
 - 5.20.2. Realizar Proteção contra Denial of Service (DoS);
 - 5.20.3. Realizar Proteção contra Syn flood;
 - 5.20.4. Realizar Limpeza de cabeçalho HTTP.
- 5.21. A solução deve permitir o controle da resposta ICMP por servidor virtual.
- 5.22. Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração.
- 5.23. Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares.
- 5.24. Permitir a criação de Virtual Servers com endereço IPv4 e os servidores reais com endereços IPv6.
- 5.25. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente.
- 5.26. Deve permitir compressão tipo GZIP e Deflate.
- 5.27. Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate).
- 5.28. Possuir capacidade para definir compressão especificamente para certos tipos de objetos.
- 5.29. Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições HTTP são enviadas aos servidores sem criptografia.
- 5.30. Permitir a definição de quais tipos de objeto serão armazenados ou não em cache.
- 5.31. Permitir a reescrita de requisições HTTP baseado no conteúdo da URL, possibilitando o redirecionamento de requisições HTTP para HTTPS.

- 5.32. Permitir a reescrita de respostas HTTP, possibilitando a inclusão de cabeçalho (header) customizado.
- 5.33. Suportar multiplexação TCP e Reuso de Sessão para reaproveitamento e uso eficiente de conexões entre a solução de balanceamento de aplicações e os servidores balanceados.
- 5.34. Garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados sejam realizadas com aceleração em hardware, para não onerar o sistema, este item somente é válido para solução em appliance.
- 5.35. Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo “man in the middle”, ou seja, descriptografar, otimizar e re-criptografar o tráfego SSL em comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor. Caso haja falha na leitura da conexão SSL, esta deverá, se assim definido, prosseguir em regime de passthrough.
- 5.36. A solução deve possuir a funcionalidade de espelhamento de conexões SSL.
- 5.37. A solução deve possuir a capacidade de redirecionar o SSL Offload (troca de chaves) de determinado serviço para outro appliance físico que tenha mais capacidade para tratamento SSL. Dessa forma deve ser possível otimizar recursos executando tarefas que exigem muito desempenho para serem tratadas em hardware especializado.
- 5.38. Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado.
- 5.39. Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste edital devem estar disponíveis quando a conexão segura for estabelecida usando:
- 5.39.1. Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS.
- 5.39.2. Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;
- 5.39.3. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea.
- 5.40. Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS, a solução deverá ser capaz de:
- 5.40.1. Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;

5.40.2. Encaminhar ao servidor real via cabeçalho HTTP campos específicos do certificado digital utilizado pelo cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS.

5.41. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web.

5.42. Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições POP3, IMAP e SMTP são enviadas aos servidores sem criptografia.

5.43. A solução deve possuir diversos recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto na performance das aplicações. Dentre eles deve ser possível configurar parâmetros como:

5.43.1. SSL session cache Timeout;

5.43.2. Session Ticket;

5.43.3. OCSP (Online Certificate Status Protocol) Stapling;

5.43.4. Dynamic Record Sizing;

5.43.5. ALPN (Application Layer Protocol Negotiation);

5.43.6. Perfect Forward Secrecy.

5.44. Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores.

5.45. Possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados.

5.46. Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos.

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

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

5.49. Deve ser capaz de realizar DHCP relay.

5.50. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:

5.50.1. Tempo de resposta da aplicação;

5.50.2. Latência;

5.50.3. Conexões para conjunto de servidores, servidores individuais;

5.50.4. Por URL.

5.51. A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:

5.51.1. Servidores virtuais;

5.51.2. Servidores balanceados;

5.51.3. URLs;

5.51.4. Países de origem, baseados em geolocalização (GEOIP);

5.51.5. Dispositivos de origem do cliente (user agent).

5.52. Deve possuir framework unificado para configuração da aplicação.

5.53. Deve possuir criptografia IPSEC para comunicação entre os balanceadores.

5.54. Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS.

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

5.56. A Solução deve ter suporte a sFlow.

5.57. A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6.

5.58. A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6.

5.59. A solução deve suportar Equal Cost Multipath (ECMP).

5.60. A solução deve realizar Bidirectional Forward Detection (BFD).

5.61. A solução deve ter suporte a Stream Control Transmission Protocol (SCTP).

5.62. Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI).

5.63. A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação.

- 5.64. Suportar diversas cifras e protocolos SSL/TLS, incluindo TLS 1, 1.1, 1.2, 1.3, Forward Secrecy/Perfect Forward Secrecy, RSA, ECDSA, DHE, ECDHE, AES-128, AES-256, CBC/GCM, Camellia128, Camellia256, SHA, SHA2(SHA256/384) e Chacha20-Poly1305;
- 5.65. A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA.
- 5.66. A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. O balanceador não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores:
- 5.66.1. Deve ser possível configurar o tamanho máximo da fila;
- 5.66.2. Deve ser possível configurar o tempo máximo de permanência na fila.
- 5.67. A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede.
- 5.68. A solução deve realizar Controle de Banda Dinâmico por aplicação e usuário.
- 5.69. A solução deve realizar Controle de Banda baseado em domínio de roteamento.
- 5.70. Permitir tráfego por parâmetros de QoS (Quality of Service) ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação. Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes. A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações.
- 5.71. A solução deve permitir a criação de túneis IP por domínio de roteamento utilizando GRE, IPIP, EtherIP, PPP.
- 5.72. A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP.
- 5.73. Deve fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server.
- 5.74. Possuir suporte ao protocolo SPDY e HTTP 2.0.
- 5.75. O equipamento deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL.
- 5.76. O equipamento deverá permitir a sincronização das configurações:
- 5.76.1. De forma automática;
- 5.76.2. Manualmente, forçando a sincronização apenas no momento desejado.
- 5.77. Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:

5.77.1. Compartilhar a rede de heartbeat com a rede de dados; e

5.77.2. Utilizar uma rede exclusiva para o heartbeat.

5.78. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra-ataques.

5.79. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.

5.80. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.

5.81. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:

5.81.1. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-setcookie, http-status, http-uri e http-version.

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

5.82.1. Bloqueio de tráfego;

5.82.2. Reescrita e manipulação de URL;

5.82.3. Registro de tráfego (log);

5.82.4. Adição de informação no cabeçalho HTTP;

5.82.5. Redirecionamento do tráfego para um membro específico;

5.82.6. Selecionar uma política específica para Aplicação Web.

5.83. A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:

5.83.1. Endereço IP de origem.

5.84. A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:

5.84.1. Endereço IP de origem;

5.84.2. Porta TCP ou UDP de origem;

5.84.3. Endereço IP de destino;

5.84.4. Porta TCP ou UDP de destino;

5.84.5. Protocolo de camada 4 (TCP ou UDP);

5.84.6. Data e hora da mensagem;

5.84.7. URL acessada.

5.85. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory.

5.86. A solução deve suportar controle de versão da política de configuração de forma a permitir fazer roll back de políticas aplicadas.

5.87. A solução deve ser capaz de analisar a performance de aplicações web.

5.88. A solução deve possuir relatórios das aplicações.

5.89. Deve prover métricas de aplicações como: Transações por Segundo; Tempo de latência do cliente e servidor; Throughput de requisição e resposta; Sessões.

5.90. A solução deverá gerar informações para permitir análises históricas e auxiliar nos processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações.

5.91. As informações coletadas deverão permitir a análise dos dados por aplicações, por URL's, por clientes e por servidores, permitindo assim a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução.

5.92. A solução deverá gerar informações estatísticas de acesso identificando para cada aplicação os métodos de acesso HTTP (GET e Post), o tipo de sistema operacional utilizado pelos clientes, e os browsers utilizados.

5.93. A geração de informações históricas deverá permitir:

5.93.1. O detalhamento do tempo de resposta total de carregamento de uma URL e ou Página;

5.94. Permitir a correlação de métricas de uso de rede com o comportamento das aplicações.

6. PROTEÇÃO CONTRA-ATAQUES DE APLICAÇÃO

6.1. A solução deve operar nos modos ativo-ativo e ativo-standby.

6.2. O equipamento oferecido deverá proteger a infra-estrutura web de ataques contra a camada de aplicação (Camada 7).

- 6.3. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado.
- 6.4. Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS, pois esses valores devem ser auto-ajustáveis e adaptativos de acordo com mudanças.
- 6.5. A solução deve possuir a capacidade de automaticamente capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador.
- 6.6. A solução deve suportar o uso de firewall camada 3-4 junto com firewall camada 7 no mesmo equipamento/appliance para evitar problemas com o aumento da latência.
- 6.7. O equipamento oferecido deverá possuir a certificação ICSA para Firewall de Aplicação (Web Application Firewall).
- 6.8. Permitir a utilização de um modelo positivo de segurança para proteger contra-ataques conhecidos aos protocolos HTTP e HTTPS e às aplicações web acessíveis através destes.
- 6.9. Possuir política de segurança de aplicações web pré-configurada na solução.
- 6.10. Permitir a criação de novas regras com parâmetros e expressões regulares definidos pelo administrador.
- 6.11. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes.
- 6.12. Permitir a criação de políticas diferenciadas por aplicação.
- 6.13. Permite configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies.
- 6.14. A solução WAF deve, no mínimo, funcionar como proxy reverso de aplicações.
- 6.15. A solução WAF deve, no mínimo, permitir o mapeamento de diversas aplicações em um mesmo IP virtual, enviando informações para conjuntos de servidores diferentes de acordo com a URL requisitada.
- 6.16. A solução WAF deve, no mínimo, permitir o mapeamento em um mesmo IP virtual, de acordo com a URL requisitada, que exija certificado digital de cliente para algumas aplicações e não exija para outras.
- 6.17. A solução WAF deve, no mínimo, permitir a inclusão de parâmetros customizados nos cabeçalhos (headers) HTTP, além da alteração dos existentes, para envio à aplicação de destino.

- 6.18. A solução deverá se integrar a soluções de análise (Scanner) de vulnerabilidade do site. O resultado desta análise deve ser utilizado para configurar as políticas do equipamento.
- 6.19. A solução deve permitir a integração com soluções de análise de vulnerabilidades (Scanner) de terceiros.
- 6.20. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação. Essa inspeção pode ser feita via integração ICAP. Deve ser possível integrar com diferentes softwares de Antivírus.
- 6.21. Deve se integrar com o software de Antivírus existente no ambiente da CONTRATANTE.
- 6.22. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar e aumentar a proteção contra-ataques recentes.
- 6.23. Permitir a integração com Firewall de Database de outros fabricantes.
- 6.24. A solução deve se integrar com outras soluções de segurança e análise de logs de outros fabricantes.
- 6.25. Deve possuir tecnologia de detecção de anomalias baseado nos IDs dos dispositivos, permitindo a detecção de DoS, ataques de força bruta e ataques de sequestro de sessão. Deve ser possível filtrar relatórios por IDs de dispositivos.
- 6.26. A solução deve permitir incluir em blacklist os endereços IPs que repetidamente falharem a desafios no browser. Portanto o sistema não precisa usar recursos para mitigar tráfego enviado por esses endereços Ips. Ao entrar em Blacklist o sistema automaticamente bloqueia os pacotes enviados por esse endereço por um período de tempo.
- 6.27. A solução deve suportar e fazer a proteção do tráfego em cima de protocolo WebSocket.
- 6.28. A solução deve possibilitar o uso de múltiplas formas de logging remoto ao mesmo tempo para a mesma aplicação. Portanto dever ser possível por exemplo logar os requests válidos num servidor de SIEM e os requests inválidos em outro servidor de SIEM de outra marca e modelo.
- 6.29. A solução deverá possuir funcionalidade de proteção positiva e segura contra-ataques, como:
- 6.29.1. Acesso por Força Bruta;
 - 6.29.2. Ameaças Web AJAX/JSON;
 - 6.29.3. DoS e DDoS camada 7;
 - 6.29.4. Buffer Overflow;
 - 6.29.5. Cross Site Request Forgery (CSRF);
 - 6.29.6. Cross-Site Scripting (XSS);

- 6.29.7. SQL Injection;
- 6.29.8. Cookie e Command Injection;
- 6.29.9. Code Injection.
- 6.29.10. Parameter tampering;
- 6.29.11. Cookie poisoning;
- 6.29.12. HTTP Request Smuggling;
- 6.29.13. Manipulação de campos escondidos;
- 6.29.14. Manipulação de cookies;
- 6.29.15. Roubo de sessão através de manipulação de cookies;
- 6.29.16. Sequestro de sessão;
- 6.29.17. Força bruta no browser;
- 6.29.18. XML bombs/DoS;
- 6.29.19. Checagem de consistência de formulários;
- 6.29.20. Checagem do cabeçalho do “user-agent” para identificar clientes inválidos.
- 6.30. A solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automática.
- 6.31. Deverá ser capaz de identificar e bloquear ataques através de:
 - 6.31.1. Regras de verificação personalizadas – política de segurança configurada;
 - 6.31.2. Assinaturas, com atualização periódica da base pelo fabricante;
 - 6.31.3. As assinaturas devem ser atualizadas durante o período do contrato sem que seja necessário nenhum custo a mais por parte da CONTRATANTE na aquisição de novas licenças ou subscrições. Deve fazer parte da solução de WAF ofertada;
 - 6.31.4. Ausência de tratamento de erros pela aplicação.
- 6.32. Prevenir contra vazamento de dados sensíveis (mensagens de erro HTTP, códigos das aplicações, entre outros) dos servidores de aplicação, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários.

- 6.33. Permitir a customização da resposta de bloqueio.
- 6.34. Permitir a liberação temporária ou definitiva (white-list) de endereços IP bloqueados por terem originados ataques detectados pela solução.
- 6.35. Deve permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual.
- 6.36. Deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem o limite estabelecido, por um período de tempo determinado através de configuração.
- 6.37. Deve permitir criar lista de exceção (white list) por endereço IP específico ou faixa de sub-rede.
- 6.38. A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10.
- 6.39. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle.
- 6.40. Deverá implantar, no mínimo, as seguintes funcionalidades:
- 6.40.1. Proteção contra Buffer Overflow;
 - 6.40.2. Checagem de URL;
 - 6.40.3. Checagem de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT);
 - 6.40.4. Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);
 - 6.40.5. Proteção contra Cross-site Scripting;
 - 6.40.6. Funcionalidade de Cookie Encryption;
 - 6.40.7. Checagem de consistência de formulários;
 - 6.41.8. Checagem do cabeçalho “user-agent” para identificar clientes inválido.
- 6.41. Implementar as seguintes funcionalidades:
- 6.41.1. Cloaking – Proteção contra exposição de informações do ambiente e servidores internos como:
 - 6.41.1.1. Sistema operacional e servidor web com impressão digital.

- 6.41.2. Esconder qualquer mensagem de erro HTTP dos usuários;
- 6.41.3. Remover as mensagens de erro às páginas que serão enviadas aos usuários;
- 6.41.4. Permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios.
- 6.42. Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro Xforwarded-for (XFF).
- 6.43. Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado (s) País/Países seja (m) bloqueado (s).
- 6.44. Possuir mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres), cookies, arquivos XML e elementos XML.
- 6.45. O equipamento oferecido deverá possuir uma funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação.
- 6.46. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado.
- 6.47. O equipamento oferecido deverá possuir proteção baseada em assinaturas para prover proteção contra-ataques conhecidos. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção à regra geral.
- 6.48. A atualizações de assinaturas deverão passar por um período configurável de testes, onde nenhuma requisição que viole a assinatura será bloqueada, apenas informada no relatório. Este processo deve ser automatizado, não sendo necessário criar regras específicas a cada atualização de assinatura.
- 6.49. O equipamento oferecido deverá permitir o bloqueio de ataques DoS na camada 7, possuindo também a opção de apenas registrar o ataque, sem tomar nenhuma ação de bloqueio.
- 6.50.1. O equipamento oferecido deverá possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:
- 6.50.1.1. Número de requisições por segundo enviados a uma URL específica;
- 6.50.1.2. Número de requisições por segundo enviados de um IP específico;
- 6.50.1.3. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);
- 6.50.1.4. Número máximo de transações por segundo (TPS) de um determinado IP;

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

6.50.1.6. Aumento do stress do servidor de aplicação.

6.51. O equipamento oferecido deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas. Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável.

6.52. O equipamento oferecido deverá permitir o bloqueio de determinados endereços IPs que ultrapassem um número máximo de violações por minuto. O período de bloqueio deverá ser configurável e durante este período todas as requisições do cliente serão bloqueadas automaticamente.

6.53. O equipamento oferecido deverá permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais. Robôs conhecidos do mercado, como Google, Yahoo e Microsoft Bing deverão ser liberados por padrão.

6.54. O equipamento oferecido deverá permitir o cadastro de robôs que podem acessar a aplicação.

6.55. Possuir política de segurança de aplicações pré-configuradas no equipamento para pelo menos as seguintes aplicações:

6.55.1. Microsoft ActiveSync v1.0, v2.0;

6.55.2. Microsoft OWA in Exchange 2003, 2007, 2010 e as versões mais recentes;

6.55.3. Microsoft SharePoint 2010 e as versões mais recentes;

6.55.4. Oracle 10g Portal;

6.55.5. Oracle Application 11i;

6.55.6. Oracle PeopleSoft Portal.

6.56. O equipamento oferecido deverá implementar proteção ao JSON (JavaScript Object Notation).

6.57. Possuir firewall XML integrado – suporte a filtro e validação de funções XML específicas da aplicação.

6.58. Implementar a segurança de web services, através dos seguintes métodos:

6.58.1. Criptografar/Decriptografar partes das mensagens SOAP;

- 6.58.2. Assinar digitalmente partes das mensagens SOAP;
- 6.58.3. Verificação de partes das mensagens SOAP.
- 6.59. Prevenir o vazamento de informações, permitindo o bloqueio ou a remoção dos dados confidenciais.
- 6.60. Prevenir que erros de aplicação ou infra-estrutura sejam mostrados ao usuário.
- 6.61. Deverá ter integração, via ICAP, com servidor de anti-vírus para verificação dos arquivos a serem carregados nos servidores.
- 6.62. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle.
- 6.63. Deverá proteger o protocolo FTP com pelo menos os seguintes métodos:
 - 6.63.1. Determinar os comandos FTP permitidos;
 - 6.63.2. Requests FTP anônimos;
 - 6.63.3. Checar compliance com o protocolo FTP;
 - 6.63.4. Proteger contra-ataques de força bruta nos logins.
- 6.64. Deverá proteger o protocolo SMTP com pelo menos os seguintes métodos:
 - 6.64.1. A comunicação deve ser aderente a RFC 2821;
 - 6.64.2. Limitar o número de mensagens;
 - 6.64.3. Validar registro SPF do DNS;
 - 6.64.4. Determinar quais métodos SMTP podem ser utilizados.
- 6.65. Deverá armazenar os logs localmente ou exportar para Syslog server.
- 6.66. Deverá proteger contra ataques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs serão examinadas.
- 6.67. Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determinado site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal.
- 6.68. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados: Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade e PCI Compliance.

- 6.69. Deverá permitir o agendamento de relatórios a serem entregues por email.
- 6.70. Fornecer os seguintes Gráficos de alertas por:
- 6.70.1. Política de segurança;
 - 6.70.2. Tipos de ataques;
 - 6.70.3. Violações;
 - 6.70.4. URL;
 - 6.70.5. Endereços IP;
 - 6.70.6. Países;
 - 6.70.7. Severidade;
 - 6.70.8. Código de resposta;
 - 6.70.9. Métodos;
 - 6.70.10. Protocolos;
 - 6.70.11. Vírus;
 - 6.70.12. Usuário;
 - 6.70.13. Sessão.
- 6.71. Deverá exportar as requisições que contém os ataques, pelo menos nos formatos PDF e binário.
- 6.72. Deve possuir relatório em tempo real sobre ataques DoS L7, atualizado automaticamente.
- 6.73. A solução deve mostrar o impacto de ataques DoS L7 na performance e memória do servidor.
- 6.74. Os logs devem indicar o momento de início e final de um ataque DoS L7.
- 6.75. Possuir método de mitigação de DoS L7 baseado em: CAPTCHA; Descarte de todas as requisições de um determinado IP e/ou país suspeito; Geolocalização, incluindo a prevenção com CAPTCHA para países suspeitos que ultrapassem os thresholds; Defesa proativa contra Bot, através da injeção de um desafio JavaScript para detectar se é um usuário legítimo ou robô.
- 6.76. A solução deve permitir que ao detectar um falso positivo, o administrador aceite a requisição e atualize a política automaticamente.

- 6.77. A solução ao se integrar com um Scanner de vulnerabilidade deve mostrar quais a vulnerabilidades podem ser resolvidas automaticamente (pela própria solução de WAF) e quais podem ser resolvidas manualmente, pelo próprio administrador. No caso de resolução manual, deve ainda mostrar um guia com os passos necessários para resolver aquela vulnerabilidade, inclusive com a avisos de possíveis consequências na aplicação Web.
- 6.78. A solução deve classificar o nível de violação de uma requisição, possuindo pelo menos 5 níveis, onde o nível 5 é referente a violação mais grave e, portanto, deve ter prioridade.
- 6.79. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual.
- 6.80. Suportar os protocolos HTTP/1.0, HTTP/1.1 e HTTP/2.0.
- 6.81. Suportar codificação HTML "application/x-www-form-urlencoded".
- 6.82. Suportar Cookies v0 e v1.
- 6.83. Suportar codificação fragmentada (chunked encoding) em requisições e respostas.
- 6.84. Suportar compressão de requisições e respostas.
- 6.85. Suportar validação de protocolo, como:
- 6.85.1. Possibilidade de restringir uso de métodos;
 - 6.85.2. Possibilidade de restringir protocolos e versões de protocolos;
 - 6.85.3. Strict (per-RFC) Request Validation;
 - 6.85.4. Validar caracteres URL-encoded; e
 - 6.85.5. Validação de codificação fora de padrão %uXXYY.
- 6.86. Suportar restrições de HTML, como:
- 6.86.1. Tamanho do nome de parâmetros;
 - 6.86.2. Tamanho dos valores de parâmetros; e
 - 6.86.3. Combinação de tamanho de parâmetros (nome e valores).
- 6.87. Suportar POST no upload de arquivo.
- 6.88. Permitir configurar ou oferecer restrições para tamanho individual de arquivo.

- 6.89. Permitir customizar a lógica na inspeção de upload de arquivos.
- 6.90. Suporte para os métodos Basic, Digest e NTLM para autenticação.
- 6.91. Suporte para autenticação por back end tipo LDAP e Microsoft Active Directory.
- 6.92. Capacidade de filtrar cabeçalhos, corpo e status de respostas.
- 6.93. Suportar as seguintes técnicas de detecção:
 - 6.93.1. URL-decoding;
 - 6.93.2. Terminação Null Byte String;
 - 6.93.3. Paths auto-referenciados;
 - 6.93.4. Case de caracteres misturados;
 - 6.93.5. Uso excessivo de espaços em branco;
 - 6.93.6. Remoção de comentários;
 - 6.93.7. Decodificação de entidades HTML; e
 - 6.93.8. Caracteres de escape.
- 6.94. Possuir registro de logs com as seguintes características:
 - 6.94.1. Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo par requisição/resposta;
 - 6.94.2. Os registros de log de acesso e eventos devem ser armazenados em arquivo ou em banco de dados que permita a exportação ou em outro formato aberto como CSV ou TXT, podendo ainda serem armazenados localmente ou carregados (upload) em servidor de log via FTP ou SCP ou armazenados em servidor externo de banco de dados;
 - 6.94.3. Permitir configurar a retenção dos logs por tempo e volume; e
 - 6.94.4. Ter capacidade para detecção, remoção ou codificação de dados sensíveis do log.
- 6.95. A solução deverá gerar relatórios com as seguintes características:
 - 6.95.1. Permitir a filtragem por data ou hora, endereço IP e tipo de incidente;
 - 6.95.2. Permitir a geração de relatórios sob demanda ou pré-programados periodicamente (diário e semanal); e
 - 6.95.3. Permitir a geração de relatórios em formatos PDF/A (versão aberta) e HTML.

6.96. Possuir as seguintes características de gerenciamento:

6.96.1. Facilidade para liberação de regras aprendidas automaticamente que estejam gerando grande quantidade de falso positivo;

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

6.96.3. Facilidade para aplicar diferentes regras para diversas aplicações;

6.96.4. Capacidade para customizar regras de negação de serviço;

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

6.96.6. Capacidade para desfazer a aplicação de uma regra.

6.97. Possuir mecanismos que garantam a capacidade de gerenciamento do equipamento sob condições de alto tráfego.

6.98. A solução deve apresentar perfil de aprendizagem automática com:

6.98.1. Capacidade de aprendizagem automática sem intervenção humana; e

6.98.2. Capacidade de inspeção das regras criadas automaticamente.

6.99. Permitir o gerenciamento da configuração com as seguintes características:

6.99.1. Gerenciamento por autenticação dos usuários e as autorizações baseadas em perfis (roles); e

6.99.2. Capacidade de gerenciamento remoto dos equipamentos.

6.100. Apresentar logs e relatórios administrativos com as seguintes características:

6.100.1. Capacidade para identificar e notificar falhas do sistema ou perda de performance;

6.100.2. Capacidade de agregação de informações para simplificar a revisão das atividades do dispositivo; e

6.100.3. Capacidade para gerar estatísticas de serviço e sistema.

6.101. Possuir suporte a XML:

6.101.1. Para proteção de WebServices;

6.101.2. Em conformidade com a especificação WS-I básico; e

6.101.3. Com capacidade de restringir métodos do Webservice via definição em WSDL.

6.102. Suportar funções de camuflagem (cloaking), como:

6.102.1. Esconder qualquer mensagem de erro http dos usuários; e

6.102.2. Remover as mensagens de erro das páginas que serão enviadas aos usuários.

6.103. Proteger a aplicação Web contra robôs sofisticados através da combinação de desafios enviados ao browser do usuário e técnicas avançadas de análise comportamental.

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

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

6.106. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego com o stress do servidor de aplicação para determinar uma condição de DDoS.

6.107. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação.

6.108. Deve possuir uma proteção proativa contra-ataques automatizados por robôs e outras ferramentas de ataque.

6.109. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário.

6.110. Deve proteger esses dados criptografados de malwares e keyloggers.

6.111. Deve suportar a criptografia de sessões HTTP desde o browser do usuário, provendo proteção contra interceptação por terceiros e evitando ataques do tipo Man in the Browser e Keyloggers.

6.112. Deve possuir proteção contra-ataques DDoS, através da análise de comportamento de tráfego usando técnicas de análise de dados e Machine Learning.

6.113. Através da análise contínua de carga e monitoração de saúde de servidores, deve ser possível identificar anomalias e mitigá-las.

6.114. Deve ajudar a prevenir contra-ataques de Credential Stuffing, onde bases de credenciais expostas na Internet são usados para tentativa de acesso de outras aplicações Web.

6.115. A solução deve possuir lista dinâmica de endereços IP globais com atividades maliciosas:

6.116. Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro Xforwarded-for (XFF).

6.117. Deve possuir, pelo menos, as seguintes categorias de endereços IP: Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing Proxy, Anonymous Proxy.

6.118. Possuir linguagem de script que possibilite a interação com o payload das requisições e inclusive alterações.

7. DNS

7.1. A solução deve operar em, no mínimo, a seguintes formas:

7.1.1. DNS autoritativo;

7.1.2. DNS secundário;

7.1.3. DNS resolver;

7.1.4. DNS cache;

7.1.5. Balanceamento de DNS servers.

7.1.6. DNSSec;

7.1.7. A solução deve ser capaz de realizar transferência de zonas para múltiplos servidores DNS Primários responsáveis por diferentes zonas;

7.1.8. Capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;

7.1.9. A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;

7.1.10. A solução deve servir as respostas as requisições onde o DNS é o autoritativo a partir da memória RAM;

7.1.11. A solução deve possuir certificação ICASA.

7.2. A solução deve possuir proteções contra-ataques DNS, no mínimo:

7.2.1. Inspeção de protocolo;

7.2.2. Validação de protocolo.

7.2.3. UDP flood;

7.2.4. Pacotes mal formados;

7.2.5. Ataque Teardrop;

7.2.6. Ataque ICMP;

7.2.7. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra-ataques.

7.3. A solução deve ser capaz de realizar balanceamento dos servidores DNS.

7.4. A solução deve ser capaz de realizar filtragem de pacotes.

7.5. A solução deve prover segurança do protocolo DNS, protegendo contra-ataques de negação de serviço, NXDOMAIN e reflexão e amplificação de DNS.

7.6. A solução deve prover segurança do protocolo DNS, protegendo contra-ataques de Cache Poisoning.

7.7. A solução deve realizar stateful inspection.

7.8. A solução deve possuir base de Geolocalização IP.

7.9. A solução deve implementar DNS64.

7.10. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT.

7.11. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente.

7.12. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura.

7.13. Deve prover as respostas a queries DNS da própria RAM CACHE.

7.14. A solução deve ser capaz de realizar IP Anycast.

7.15. A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso.

7.16. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento.

7.17. A solução de alta disponibilidade será realizada baseada em respostas a requisições DNS. A resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas.

7.18. A solução deverá aceitar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição.

7.19. Deve ser possível ajustar quantos endereços são enviados em uma única resposta.

7.20. Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido.

7.21. Suportar pelo menos os seguintes algoritmos de balanceamento:

7.21.1. Round Robin;

7.21.2. Global Availability;

7.21.3. Ratio;

7.21.4. LDNS Persist;

7.21.5. Geografia;

7.21.6. Disponibilidade da Aplicação;

7.21.7. Capacidade do Virtual Server;

7.21.8. Least Connections;

7.21.9. Pacotes por segundo;

7.21.10. Round trip time;

7.21.11. Hops;

7.21.12. Packet Completion Rate;

7.21.13. QoS definido pelo usuário;

7.21.14. Kilobytes per Second.

7.22. Implementar persistência da conexão do usuário entre aplicações ou data centers.

7.23. A solução deverá suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo.

- 7.24. A solução deverá permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada.
- 7.25. A solução deverá permitir que a contingência seja automática, mas que o retorno seja manual.
- 7.26. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6).
- 7.27. Possuir suporte a IPv6 no balanceamento global entre datacenters.
- 7.28. Ter capacidade de tratar informações das camadas L4-L7 (FTP, SMTP, URL, HTTP Header, TCP e UDP) para a tomada de decisão de encaminhamento a servidor real, em IPv4 e IPv6.
- 7.29. Deverá possuir a funcionalidade de resposta rápida a queries DNS, permitindo respostas mais rápidas para zonas que seja autoritativo.
- 7.30. A solução deve possuir suporte a Response Policy Zones (RPZ), mecanismo de firewall usado por DNS recursivo para permitir o tratamento customizado da resolução de nomes. Portanto a solução deve ser capaz de filtrar queries DNS para domínios considerados maliciosos e retornar respostas customizadas.
- 7.31. A solução deve suportar edns-client-subnet (ECS) para tanto responder requisições de clientes (Balanceamento de Carga Global de Servidores) ou encaminhar requisições de clientes (screening).
- 7.32. Baseado no ECS DNS deve ser possível preservar o endereço IP da subnet do cliente ao invés do LDNS para tomar decisões.
- 7.33. A solução deve funcionar pelo menos das seguintes formas:
- 7.33.1. Usar o ECS para tomar decisões de Balanceamento de Carga Global de Servidores baseado em topologia (Subnets);
- 7.33.2. Injetar o ECS (proxy requests) para outros servidores DNS.
- 7.34. A solução deve fazer persistência baseado no endereço IP do cliente (ECS), significando que se o cliente mudar de LDNS resolver (suporte ECS), o Balanceamento de Carga Global de Servidores deve usar a persistência existente para manter o cliente no mesmo Datacenter.
- 7.35. O serviço deverá ser implementado sobre uma infraestrutura de hardware e software dedicada ou em conjunto com equipamento Anti-DDoS. O hardware empregado deverá ser do tipo appliance, específico para operar softwares de DNS Firewall. O software e o hardware empregados deverão corresponder a uma solução de notória eficácia já em uso no mercado nacional. O serviço deve ter suporte a IPv6, registros AAAA e zonas reversas IPv6.
- 7.36. Infraestrutura de hardware e software destinada à função de resolução de nomes DNS de uso exclusivo da CONTRATANTE.

7.37. O serviço deve ter a habilidade de detectar, monitorar, controlar e mitigar ataques baseados em DNS sem gerar nenhum impacto ao tráfego válido de DNS.

7.38. A solução deverá ter serviço de resolução de nomes destinado a armazenar, de forma “autoritativa”, as zonas do CONTRATANTE e o IP reverso do bloco CIDR do CONTRATANTE.

7.39. Os equipamentos que atenderão ao serviço deverão ser estruturados de forma redundante, permitindo o failover completo na ocorrência de falhas, suportando, no mínimo, o modo de operação ativo-ativo. Um nó deverá suportar sozinho todos os requisitos de performance solicitados neste projeto.

7.40. Para o devido dimensionamento do serviço cada equipamento isolado deve possuir desempenho DNS de pelo menos 50.000 QPS (50 mil Queries Per Second – Consultas Por Segundo).

7.41. O serviço deverá possuir capacidade para resolver consultas para as quais não tem autoridade (ou seja, da zona “.”, tipo “hint”), com a finalidade de atender somente às consultas DNS oriundas da rede interna do CONTRATANTE, bem como dos demais Serviços Gerenciados de Segurança e servidores instalados no Data Center.

7.42. O serviço deve ter, pelo menos, as seguintes características de segurança:

7.43. Deve permitir o uso de lista negra para bloquear domínios DNS.

7.44. Deve possuir capacidade de criação de ACLs para bloqueio de domínios e redes maliciosas.

7.45. Prover uma linha de defesa para bloquear tentativas de acesso a sites maliciosos impedindo a resolução de nomes de domínio que hospedem tais conteúdos maliciosos minimizando possíveis infecções de Malware, Trojan, Spyware, Ransomware e softwares de comando e controle (BotNet).

7.46. Registrar todas as tentativas de comunicação com os nomes de domínio que hospedem conteúdo malicioso. Estes registros devem conter: IP de origem, destino, data e hora do acesso.

7.47. Deve suportar no mínimo os seguintes métodos de controle: apenas logar, bloquear o dado ou substituir o nome do domínio.

7.48. A solução deverá suportar mecanismo de “assinaturas”, ou técnicas semelhantes, que permitam ao fabricante disponibilizar regras de bloqueios contra novos ataques conforme surgimento.

7.49. O serviço deverá permitir que o administrador crie regras customizadas de bloqueio, da seguinte maneira:

7.49.1. Bloqueio de nomes de domínio totalmente qualificados em consultas de DNS feitas via TCP ou UDP;

7.49.2. Bloqueio de endereços de origem IPv4 ou IPv6 em consultas realizadas via TCP ou UDP. Esta regra deverá permitir a configuração de endereços de hosts ou de redes.

7.50. Configuração de limites de quantidades de consultas de DNS (rate limit) realizadas via TCP ou UDP por nome de domínio totalmente qualificado.

7.51. De acordo com o IP de origem, configurar limite (rate limit) para consultas realizadas via TCP ou UDP.

7.52. Criar “Listas brancas” que permitam a realização de qualquer número de consultas de DNS por segundo, para determinado endereço IP de origem.

7.53. O serviço deverá proteger no mínimo contra os seguintes ataques de DNS:

7.53.1. Reflexão;

7.53.2. Anomalias de Protocolo;

7.53.3. Negação de Serviço;

7.53.4. Negação de Serviços Distribuídos;

7.53.5. Amplificação;

7.53.6. Tunelamento;

7.53.7. Reconhecimento;

7.53.8. Explorações (Exploit);

7.53.9. Envenenamento do cache;

7.53.10. Excessos (Floods).

7.54. O serviço deve permitir que os administradores efetuem busca de endereços de rede, subrede e endereços IP através de filtros.

7.55. A administração do serviço deve permitir definir diferentes níveis de grupos e usuários para administração.

7.56. O serviço deve possuir capacidade de reverter configurações sem a necessidade de restauração de backup.

7.57. O serviço deverá fornecer pelo menos os seguintes relatórios:

7.57.1. Tendência de latência de resposta de DNS;

- 7.57.2. Nomes de domínios de DNS mais requisitados;
- 7.57.3. Tendência de uso do cache de DNS;
- 7.57.4. Top clientes de DNS;
- 7.57.5. Taxa de consultas de DNS por tipo de registro;
- 7.57.6. Tendências de respostas de DNS;
- 7.57.7. Taxa de consultas de DNS diária por servidor;
- 7.57.8. Pico de consultas diárias de DNS por servidor;
- 7.57.9. Top DNS NXDOMAIN/No error;
- 7.57.10. Top SERVFAIL enviados e recebidos;
- 7.57.11. Top clientes por domínio de DNS;
- 7.57.12. Nomes de domínios com conteúdo malicioso;
- 7.57.13. Principais domínios maliciosos;
- 7.57.14. Principais acessos ao DNS Firewall;
- 7.57.15. Quantidade de eventos registrados por horário;
- 7.57.16. Quantidade de eventos por severidade;
- 7.57.17. Quantidade de eventos por regra;
- 7.57.18. Quantidade de eventos por tendência;
- 7.57.19. Quantidade de eventos por categoria.
- 7.58. Deve permitir a criação visões (“views”) para tratamento diferenciado de consultas conforme origem das requisições.
- 7.59. Deve implementar DNSSEC com suporte a NSEC3 (RFC 5155).

8. ANTI-DDOS L4-L7

- 8.1. Deve suportar as funcionalidades de segurança para proteção DDoS.
- 8.2. Deve suportar proteção contra todos os tipos de ataques Denial of Service (DoS e DDoS).
- 8.3. A solução deve proteger de ataques DDoS que utilizem SSL.

8.4. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego com o stress do servidor de aplicação para determinar uma condição de DDoS.

8.5. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação.

8.6. Deve permitir proteção contra-ataques DDoS, através da análise de comportamento de tráfego usando técnicas de análise de dados e Machine Learning.

8.7. Deve permitir proteger contra-ataques de DNS DDoS utilizando mecanismo que bloqueie somente as requisições maliciosas e permita requisições legítimas aos domínios existentes.

8.8. Deve suportar Network Address Translation (NAT).

8.9. Deve limitar o número de conexões.

8.10. Deve suportar Listas de Controle de Acesso (ACL).

8.11. Deve permitir o log de ataques do tipo DoS.

8.12. A solução deve possuir ferramenta flexível baseado em linguagem de programação open-source para customizar e aumentar o nível de segurança contra-ataques DDoS, incluindo a possibilidade de interação com base de reputação de endereços IP e estatísticas de tráfego.

8.13. A solução deve suportar relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DDoS.

8.14. Deve possuir suporte ao envio de SNMP traps para cada ataque DDoS detectado.

8.15. A solução deve possuir uma ferramenta de teste de pacotes, através da qual deve ser possível realizar testes de pacotes com atributos específicos através da solução anti -DoS.

9. SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO

9.1. A Licitante vencedora será inteiramente responsável pela migração da solução atual para a nova solução, de forma a não comprometer o funcionamento dos sistemas, recursos ou equipamentos atualmente em operação.

9.2. Serão contemplados todos os serviços de instalação física de todos os componentes adquiridos, desde a montagem até a energização dos equipamentos.

9.3. Deverá ser fornecido documentação de toda a implementação e configuração dos produtos adquiridos.

9.4. Após no máximo 5 (cinco) dias úteis da assinatura do contrato, deverá ser realizada uma reunião presencial no Contratante, com a participação de no mínimo 1 (um) preposto da

Contratada e os representantes da equipe do Contratante, com o objetivo de elaborar o plano de migração.

9.5. A Contratada deverá apresentar, em até 15 (quinze) dias úteis da assinatura do contrato, para aprovação do Contratante, o projeto executivo contendo o plano detalhado de instalação, configuração e migração, especificando os procedimentos e cronograma a serem adotados.

9.6. O Contratante fará análise e validação do projeto executivo contendo o plano detalhado de instalação, configuração e migração, em até 5 (cinco) dias úteis, apontado as devidas correções no documento, ficando a Contratada responsável por ajustar o plano em até 7 (sete) dias úteis, conforme as alterações apontadas pela Contratante.

9.7. Fica a critério do Contratante, definir o horário de instalação e configuração dos equipamentos, podendo tais procedimentos serem executados em feriados ou finais de semana e em horário noturno.

9.8. A Contratada não poderá realizar terceirização dos serviços objeto deste termo de referência, sendo responsável pela execução do serviço objeto desta contratação.

9.9. Os serviços de instalação e configuração, para cada um dos itens, devem ser executados por técnicos da futura contratada, certificados pelo fabricante dos equipamentos fornecidos, sendo necessária a apresentação de documentação original que comprove a validade desta (s) certificação (ões) enquanto durar o contrato, que pode ser solicitada a qualquer momento.

9.10. A futura CONTRATADA deverá apresentar um Projeto Executivo que deve conter, no mínimo, as seguintes informações:

9.10.1. Objetivo dos serviços;

9.10.2. Plano de gerenciamento de mudanças, detalhando passo a passo o escopo da migração;

9.10.3. Cronograma das atividades que serão realizadas, com os prazos estimados e as diretrizes para cada atividade;

9.10.4. Projeto lógico de configuração e diagrama de interconexão dos equipamentos;

9.10.5. Nome (s) do (s) gerente (s) de projetos responsável (is) e do (s) técnico (s) responsável (is) pela execução dos serviços;

9.10.6. Lista de todos os elementos instalados contendo:

- a) Nome e endereço IP do equipamento.
- b) Equipamento e porta na qual o equipamento foi conectado.
- c) Local de instalação (prédio, andar, sala).
- d) Número de série do equipamento.

9.11. O Projeto Executivo deverá ser entregue pela futura CONTRATADA em até 15 (quinze) dias úteis após a assinatura do contrato, o qual deverá ser aprovado pela CONTRATANTE. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes.

9.12. A instalação e configuração da solução compreenderá dentre outros atendimentos, no mínimo, os seguintes requisitos:

9.12.1. Acondicionamento dos equipamentos nos locais de instalação, incluindo a desembalagem, a montagem de todos os componentes que integram a solução, a instalação dos conjuntos montados nos rack padrão 19" da CONTRATANTE, a energização do equipamento, incluindo o fornecimento de eventuais réguas, caso necessário, devendo seguir obrigatoriamente os manuais técnicos do fabricante;

9.12.2. Instalação dos transceivers e outros acessórios em seus respectivos slots;

9.12.3. Ligações de rede dos equipamentos a infraestrutura da CONTRATANTE, incluindo o fornecimento, quando necessário, de:

9.12.3.1. Cordões ópticos OM4 com, no mínimo, 2 (dois) metros de comprimento para ligações em fibra;

9.12.3.1. Patch-cords UTP CAT6A com, no mínimo, 2 (dois) metros de comprimento para ligações em par metálico.

9.12.4. Os cabos/cordões necessários para a interligação de servidores, usuários e outras conexões que não as estritamente fornecidas são de responsabilidade da CONTRATANTE, ou seja, cabe a CONTRATADA interligar os equipamentos fornecidos;

9.12.5. Upgrade ou Downgrade do firmware;

9.12.6. A realização dos ajustes de hardware e software necessários ao funcionamento do ambiente e a instalação da solução de gerenciamento;

9.12.7. Conexão das interfaces de gerenciamento a nova rede out-of-band e testes de acesso a ferramenta de gerência para administração;

9.12.8. Configuração e teste de envio de Traps SNMP. Verificações dos recursos e o seu perfeito funcionamento e integração com os demais, conforme as melhores práticas indicadas pelo fabricante;

9.12.9. A identificação dos equipamentos e de todas as suas conexões.

9.13. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, podendo estas ser realizadas presencialmente, por telefone ou via conferência web, devendo a futura CONTRATADA sugerir as configurações de acordo com

normas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas.

9.14. A Contratada deverá configurar todas as funcionalidades do produto licenciadas e solicitadas pela Contratante.

9.15. As configurações deverão seguir fielmente a padronização previamente estabelecida pela CONTRATANTE.

9.16. Durante o processo de instalação e configuração deverá ser realizada transferência de conhecimento para a equipe da Contratante.

9.17. A futura CONTRATADA deverá fazer análise do ambiente tecnológico atual, devendo a CONTRATANTE fornecer todas as informações necessárias sobre a infraestrutura instalada, de modo que se possa garantir a continuidade dos serviços prestados pelo órgão durante a migração, mantendo a disponibilidade dos serviços básicos de rede (resolução de nomes, endereçamento dinâmico, autenticação dos usuários, etc.) e dos demais serviços de retaguarda (aplicativos, correio eletrônico, banco de dados, Internet, etc.).

9.18. A substituição da infraestrutura atual deve ser planejada e executada de modo que não cause interrupções e paralisações não programadas, ou qualquer outro tipo de transtorno ao correto funcionamento do ambiente operacional da CONTRATANTE; caso não seja possível manter a disponibilidade dos serviços básicos no momento da instalação, as manobras de implantação deverão ser realizadas durante janela de manutenção agendada previamente, em horários que não comprometam o funcionamento das atividades do órgão, inclusive aos sábados, domingos e feriados.

9.19. Ao término do serviço deve ser fornecido um relatório detalhado (as-built) contendo todas as configurações realizadas, com comentários sobre os principais comandos e as justificativas das opções de parametrização de modo a facilitar a posterior administração da solução e a continuidade de seu funcionamento.

9.20. O relatório deve conter, no mínimo, as seguintes informações:

9.20.1. Diagrama de arquitetura da solução;

9.20.2. Procedimento operacional detalhado com as etapas de instalação e configuração;

9.20.3. Informações de monitoramento da solução;

9.20.4. Informações pertinentes a posterior continuidade e manutenção da solução;

9.20.5. Referências da documentação oficial do produto.

9.21. A critério da CONTRATANTE, poderá ser elaborado um único as-built contendo todas as informações de todos os equipamentos e softwares instalados/configurados.

9.22. O serviço de instalação e configuração somente será concluído após a apresentação pela contratada do projeto executivo, as-built e o recebimento definitivo do serviço pela contratante.

9.23. A contratada deverá monitorar o ambiente da contratante por ao menos 15 dias após o final e aprovação da instalação e configuração pela contratante e atuar imediatamente no caso de evento ou falha das configurações ou equipamentos.

10. GERENCIAMENTO CENTRALIZADO

10.1. A solução de gerenciamento deve fornecer um ponto de controle unificado para todo o cluster de equipamentos da solução.

10.2. A solução de gerenciamento centralizada deve ser capaz de armazenar logs, eventos.

10.3. Seja capaz de realizar operações de backup;

10.4. Deve ser capaz de realizar o licenciamento dos componentes do cluster;

10.5. Deve ser capaz de realizar monitoramento e gerenciamento do cluster;

10.6. Ser capaz de gerenciar usuários, limitando os acessos dos usuários de acordo com seus níveis de acesso;

10.7. Deve realizar coleta de dados do cluster com objetivo de armazenar e gerenciar os dados;

10.8. Deve ser capaz de armazenar backups de eventos, alertas e dados estatísticos para requisitos de recuperação de desastres do cluster;

10.9. Realizar backups automático de imagens e configurações;

10.10. Monitoramento por meio de painéis, relatórios e alertas;

10.11. Deve ser capaz de permitir realização de análises detalhadas por aplicativo;

10.12. Gerenciar licenças do cluster;

10.13. Garantir políticas consistentes de segurança e gerenciamento de tráfego em toda a sua infraestrutura;

10.14. Criar, provisionar e implantar novos dispositivos e serviços de aplicativos;

10.15. Caso a solução de gerenciamento centralizado ofertada seja virtualizado, a solução deve ser compatível com as plataformas vmware;

10.16. Deve fornecer controle de acesso baseado em função (RBAC);

10.17. Ser capaz de associar funções a usuários e grupos locais ou a outros usuários e grupos de servidores remotos do Active Directory (AD), TACACS+, RADIUS ou LDAP;

- 10.18. Deve permitir o gerenciamento de solicitações de certificados Let's Encrypt;
- 10.19. Deve ser capaz de gerar relatórios de alertas de segurança;
- 10.20. Permitir geração de relatórios de segurança por tipo de dispositivo, aplicativo, anomalias, DDoS, atividade de bot, políticas de segurança diferenciais e políticas não utilizadas;
- 10.21. Deve ser capaz de agendar e gerar automaticamente relatórios;

11. SUPORTE TÉCNICO

11.1. O serviço de suporte técnico deve ser prestado conforme especificação a seguir:

11.1.1. O licitante vencedor deverá fornecer serviço de suporte técnico on-site e remotamente, sempre que for necessário à Presidência da República para solucionar problemas, instalar, configurar e reconfigurar o software ou dirimir dúvidas técnicas relacionadas as soluções ofertadas.

11.1.2. A escolha entre o suporte técnico on-site ou remoto será realizada pela contratante e ocorrerá na ocasião da abertura de cada ordem de serviços.

11.1.3. O licitante vencedor deverá iniciar o atendimento de acordo com os prazos definidos no Instrumento de Medição de Resultado, a contar da abertura da Ordem de Serviço e esse prazo para o início do atendimento para ambos os tipos de suporte On-site, e remoto é o mesmo.

11.1.4. O suporte técnico será realizado 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, incluindo feriados, conforme Instrumento de Medição de Resultado.

11.1.5. O término do atendimento não poderá ultrapassar o prazo estipulado no Instrumento de Medição de Resultado.

11.1.6. Os serviços de suporte técnico, a serem prestados, abrangem atividades que não são cobertas pela garantia ou pelo suporte técnico do fornecedor/fabricante, que garante a resolução de problemas referentes a falhas e defeitos.

11.1.7. O serviço será remunerado mensalmente.

11.1.8. A Ordem de Serviço poderá ser aberta por e-mail e telefone, e na ocasião da assinatura do contrato, o licitante vencedor deverá fornecer as informações para a abertura de Ordens de Serviço.

11.1.9. A empresa deverá possuir no mínimo 2 (dois) técnicos certificados pelo fabricante da solução.

11.1.10. O suporte técnico iniciará a partir da data de recebimento definitivo da solução.

11.2. Instrumento de Medição de Resultado:

11.2.1. As soluções ofertadas devem estar cobertas por garantia total fornecida pelo fabricante.

11.2.2. Durante o período de suporte, o licitante vencedor deverá atender às solicitações da PR, feitas por meio da Coordenação-Geral de Infraestrutura Tecnológica, em qualquer horário, respeitando as condições e níveis de serviço especificados a seguir.

11.2.3. O Instrumento de Medição de Resultado (IMR) será contado a partir da abertura de ordem de serviço e será classificado conforme as severidades especificadas a seguir.

11.2.4. Severidade ALTA: Esse nível de severidade é aplicado quando há indisponibilidade de componentes da solução ou as aplicações que são acessadas por meio da solução estão indisponíveis:

Dias Úteis		Sábados, Domingos e Feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
04 horas	04 horas	04 horas	04 horas

11.2.5. Severidade MÉDIA: Esse nível de severidade é aplicado quando há falha no uso da solução, estando ainda disponível, porém apresentando problemas ou instabilidade:

Dias Úteis		Sábados, Domingos e Feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
08 horas	24 horas	08 horas	24 horas

11.2.6. Severidade BAIXA: Esse nível de severidade é aplicado para a instalação, configuração, manutenções preventivas, aplicações de firmwares e esclarecimento técnico relativo ao uso da solução. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados:

Dias Úteis		Sábados, Domingos e Feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
24 horas	72 horas	Não se aplica	Não se aplica

11.2.7. Haverá multa em caso de atraso na prestação dos serviços de acordo com a seguinte tabela:

Multa	Classificação IMR	Limite da Incidência
Para infração descrita na alínea “b” do subitem 13.1 do Termo de Referência, a multa será de 5% (cinco por cento) a 10% (dez por cento), do valor do Contrato	Severidade Crítica	180 dias

Compensatória, para a inexecução total do contrato prevista na alínea “c” do subitem 13.1 do Termo de Referência, a multa será de 1% (um por cento) a 5% (cinco por cento), do valor do Contrato	Severidade Alta	180 dias
Para infração descrita na alínea “d” do subitem 13.1 do Termo de Referência, a multa será de 0,5% (cinco décimos por cento) a 1% (um por cento), do valor do Contrato	Severidade Média	90 dias
Moratória de 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida	Severidade Baixa	15 dias
Referência: Item “13. Infrações e Sanções Administrativas” do Termo de Referência.		

11.2.8. Serão considerados para efeitos dos níveis exigidos:

11.2.8.1. Prazo de Atendimento: Tempo decorrido entre a solicitação efetuada pela Equipe Técnica da PR à Prestadora de Serviço e o efetivo início dos trabalhos de manutenção;

11.2.8.2. Prazo de Solução Definitiva: Tempo decorrido entre a solicitação efetuada pela Equipe Técnica do PR à Prestadora de Serviço e a efetiva recolocação dos equipamentos em seu pleno estado de funcionamento e operação normais.

11.2.9. A contagem do prazo de atendimento e solução definitiva de cada solicitação será a partir da notificação ao licitante vencedor, até o momento da comunicação da solução definitiva do problema e aceite pela equipe técnica da PR.

11.2.10. O atendimento às solicitações de severidade ALTA deverá ser realizado nas instalações da PR (on-site) e não poderá ser interrompido até o completo restabelecimento do serviço, mesmo que se estenda para períodos noturnos, sábados, domingos e feriados. Nesse caso, não poderá implicar em custos adicionais à PR. A interrupção do suporte técnico de uma solicitação desse tipo de severidade por parte do licitante vencedor e que não tenha sido previamente autorizado pela PR, poderá ensejar em aplicação de glosas previstas.

11.2.11. As ordens de serviços classificadas com severidade MÉDIA, quando não solucionados no prazo definido, poderão ser automaticamente escaladas para a severidade ALTA, sendo que os prazos de atendimento e solução definitiva do problema, bem como glosas previstas, serão automaticamente ajustados para o novo nível. A interrupção do suporte técnico de uma solicitação desse tipo de severidade por parte do licitante vencedor e que não tenha sido previamente autorizado pela PR, poderá ensejar em aplicação de glosas previstas.

11.2.12. Depois de concluído o suporte técnico, o licitante vencedor comunicará o fato à Equipe Técnica da PR e solicitará autorização para o fechamento do chamado. Caso a PR não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pelo licitante vencedor. Nesse caso, a PR fornecerá as pendências relativas à solicitação em aberto.

11.2.13. A PR encaminhará ao licitante vencedor, quando da reunião de apresentação inicial, relação nominal da equipe técnica autorizada a abrir e fechar solicitações de suporte técnico.

11.2.14. Por necessidade excepcional de serviço, a PR também poderá solicitar a escalção de chamado para níveis superiores de severidade. Nesse caso, a escalção deverá ser justificada e os prazos dos chamados passarão a contar do início novamente.

11.2.15. O pagamento das faturas estará sujeito à glosa quando não houver cumprimento dos níveis de serviço exigidos ou quaisquer outras que impliquem em glosas previstas.

12. CAPACITAÇÃO

12.1. A capacitação deverá ser realizada no idioma português do Brasil.

12.2. O material didático utilizado na capacitação deve estar no idioma inglês ou português do Brasil.

12.3. O instrutor que ministrará a capacitação da solução deve possuir certificação do fabricante da solução ofertada.

12.4. A documentação exigida em relação ao instrutor deverá ser apresentada na assinatura do contrato.

12.5. A capacitação deverá possuir uma carga horária mínima de 40 horas.

12.6. A capacitação deverá abordar no mínimo sobre a instalação, configuração, administração e resolução de problemas da solução ofertada.

12.7. Deve ser emitido um certificado para cada servidor que participar da capacitação e tiver frequência mínima de 70% (setenta por cento).

12.8. A capacitação será realizada DE FORMA ON-LINE OU PRESENCIAL em Brasília em local definido pelo licitante vencedor.

12.9. O licitante vencedor irá capacitar 8 (oito) servidores da PR.

12.10. A capacitação deve ser realizada em até 90 (noventa) dias corridos, contados a partir da solicitação oficial deste serviço.

12.11. É permitida a subcontratação desse item.

Estudo Técnico Preliminar 25/2024

1. Informações Básicas

Número do processo: 00094.000097/2024-34

2. Introdução

2.1. Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no DFD-Doc de Formalização da Demanda TIC-L14133/21 14 (SUPER nº 4907637), 29 de janeiro de 2024, e Documento de Formalização da Demanda nº 248/2023 - Aquisição de Solução de Firewall de Rede, atualizado (SUPER nº 5718054), bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação.

3. Descrição da necessidade

3.1. Aquisição de solução de equipamento firewall de aplicação web, para proteção do perímetro da rede de dados, dos ativos de hardware e software e das aplicações web da Presidência da República, compreendendo gerência centralizada, instalação e configuração da solução, com garantia e suporte técnico pelo período de 60 (sessenta) meses, conforme condições, quantidades e exigências estabelecidas neste Estudo Técnico e seus anexos.

3.2. Contextualização

3.2.1. Em 2015, a Presidência da República contratou a solução de firewall de aplicação web, por intermédio do processo nº 00094.001125/2015-40, Contrato Administrativo nº 206/2015, com garantia e suporte de software e hardware do fabricante por 48 meses.

3.2.2. Em 13/06/2019, o suporte do fabricante ao software e ao hardware encerrou, gerando a necessidade da instrução de um novo processo licitatório, sob nº 00094.000279/2019-48, para a contratação de serviço para garantir as atualizações corretivas e evolutivas desta solução, bem como garantir a manutenção do hardware utilizado pela solução durante o novo período de vigência contratual. Essa necessidade originou o Contrato Administrativo nº 58/2020, firmado entre a Presidência da República e a empresa ISH Tecnologia S/A, com vigência de 29/12/2020 a 29/12/2023, ou seja, por 36 meses. Portanto, em 29 de dezembro de 2023, se encerrou o suporte de software e hardware do equipamento do fabricante f5.

3.2.3. A aquisição de Solução de Equipamento Firewall de Aplicação Web (WAF), foi objeto do Pregão Eletrônico nº 67/2023, promovida pela Diretoria de Tecnologia, com sessão pública realizada em 21/12/2023, às 09:30h (horário de Brasília). Todavia, somente o **Grupo 1** - Aquisição de Solução de Equipamentos Firewall de Próxima Geração (NGFW) foi homologada e adjudicada pela autoridade competente. O **Grupo 2** - Aquisição de Solução de Equipamentos Firewall de Aplicação Web (WAF) restou fracassado e homologado pela autoridade competente, já que os interessados não preenchem os requisitos estipulados pelo edital do Pregão Eletrônico nº 67/2023.

3.2.4. Cabe aqui um esclarecimento quanto ao valor apurado na cotação de preços, consignado na Cotação-Detalhada-381/2023, onde o valor do somatório das medianas dos item nº 01, nº 02 e nº 3, ficou muito aquém dos valores ofertados no Pregão Eletrônico nº 67/2023, fato que resultou no fracasso da licitação.

3.3. Tendo em vista o encerramento do suporte e garantia da solução de firewall de aplicação web e o fracasso do **Grupo 2** - Aquisição de Solução de Equipamentos Firewall de Aplicação Web (WAF) do edital do Pregão Eletrônico nº 67/2023, se faz necessária a instrução de processo licitatório para a contratação de aquisição da citada solução que visa proteger o perímetro interno e externo da Presidência da República, sendo capaz de gerir o controle do tráfego de dados e proteger contra malwares e outras ameaças de forma pró ativa e eficiente.

3.4. A referida solução é essencial para a análise e bloqueio dos ataques cibernéticos, direcionados aos portais e sistemas hospedados na infraestrutura tecnológica desta Presidência da República.

4. Área requisitante

Área Requisitante	Responsável
Diretoria de Tecnologia, da Secretaria de Administração, da Secretaria-Executiva da Casa Civil	Bruno Pereira Pontes
Coordenação-Geral de Infraestrutura Tecnológica, da Diretoria de Tecnologia	Walter Lopes Neto

5. Necessidades de Negócio

- 5.1. Aquisição de solução de firewall de aplicação web (WAF), provendo visibilidade detalhada e controle do tráfego e proteção da rede.
- 5.2. Prover proteção contra-ataques que explorem vulnerabilidade das aplicações da Presidência da República.
- 5.3. Prover proteção contra-ataques na borda da rede da Presidência da República, por meio da inspeção do tráfego de entrada e saída da rede.
- 5.4. Alta disponibilidade das soluções de proteção da rede.
- 5.5. Garantir o acesso balanceado e otimizado às aplicações.
- 5.6. Prover performance e acesso seguro e confiável às aplicações.
- 5.7. Garantir a publicação na internet das aplicações da Presidência da República.
- 5.8. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014).
- 5.9. Manter a integridade dos dados e das informações sensíveis dos sistemas da Presidência da República.
- 5.10. Melhorar o nível de qualidade do serviço das aplicações internas da Presidência da República.
- 5.11. Melhorar a experiência do usuário ao acessar os serviços da Presidência da República fora da rede interna.
- 5.12. Prover o acesso com segurança a rede corporativa dos empregados em trabalho remoto.
- 5.13. Atender à Política de Segurança da Informação nos Órgãos e Entidades da Administração Pública Federal.
- 5.14. Garantir a qualidade, o desempenho e a alta disponibilidade das informações e dos equipamentos da Presidência da República.
- 5.15. Garantir a continuidade dos serviços aos usuários da Presidência da República.
- 5.16. Manter a infraestrutura de alto desempenho adequada para o tráfego de informações e sistemas críticos de TIC.
- 5.17. Manter o licenciamento em conformidade com o parque tecnológico.
- 5.18. Manter o parque tecnológico atualizado e padronizado.
- 5.19. Obter atualizações, correções e evoluções durante o período de vigência do contrato.

5.20. Capacidade de suportar ataques e ajustar o ambiente para fazer frente as mudanças ou restabelecimento dos serviços de forma mais célere em caso de problemas na rede.

5.21. Prover escalabilidade, redundância e resiliência para os serviços de tecnologia da informação da Presidência da República.

5.22. Prover disponibilidade, integridade, confidencialidade e autenticidade dos dados e informações.

5.23. Detalhamento dos Bens, Soluções e Serviços.

5.23.1. O detalhamento das especificações e características dos bens, solução e serviços decorrentes, se encontram consignados no Anexo I, do presente Estudo.

6. Necessidades Tecnológicas

6.1. Firewall de Aplicação Web - WAF

6.1.1. O WAF é um tipo de firewall criado para combater as ameaças que estão além das capacidades dos firewalls tradicionais. Ele cria uma barreira entre o seu serviço baseado na web e todo o resto da Internet, bloqueando e protegendo sua aplicação de ações criminosas, como manipulação de conteúdo exibido, conhecida como “pixação”, injeções indevidas em banco de dados de padrão SQL (Structured Query Language) ou simplesmente “SQL Injection”, determinados tipos de fraudes em acesso administrativo e várias outras espécies de ciberataques.

7. Demais requisitos necessários e suficientes à escolha da solução de TIC

7.1. Melhorar substancialmente o nível de segurança da informação da Presidência da República.

7.2. Permitir ao time de segurança da informação ter visibilidade das aplicações e os riscos que elas trazem para o ambiente.

7.3. Prover gestão e visibilidade relacionado as vulnerabilidades dos dispositivos.

7.4. Melhorar a experiência do usuário no acesso externo ao ambiente da Presidência da República.

7.5. Gerenciar as aplicações com políticas e controles baseado nas normativas de segurança e na LGPD.

7.6. Garantia e suporte técnico por 60 meses.

7.7. Equipamentos devem manter-se funcional após vencimento de licenças.

7.8. Manter base local de assinaturas de segurança após o vencimento das licenças.

7.9. Requisitos sociais, ambientais e culturais.

7.9.1. Os profissionais da CONTRATADA deverão trajar-se de maneira adequada, quando no ambiente da Presidência da República, e usar linguagem respeitosa e formal no trato com a Gestão e/ou Fiscalização Contratual, os dirigentes da Presidência da República e usuários, em consonância com as regras e normas internas.

7.9.2. Os serviços prestados pela CONTRATADA deverão pautar-se sempre no uso racional de recursos e equipamentos, de modo a evitar e prevenir o desperdício de insumos e material.

7.9.3. A CONTRATADA deverá atender, no que couber, os critérios de sustentabilidade ambiental previstos na Instrução Normativa SGD nº 94, de 23 de dezembro de 2022.

7.10. Requisitos de adequação do ambiente da Presidência da República para viabilizar a execução contratual

7.10.1. Será necessário disponibilizar espaço para acomodação dos equipamentos e acessórios na Coordenação de Centro de Dados, da Diretoria de Tecnologia, Anexo I, do Palácio do Planalto, Brasília/DF.

7.10.2. Os racks de equipamentos deverão ter um espaço de 1 U por equipamento e infraestrutura elétrica e de climatização necessária.

7.11. Requisitos de Capacitação

7.11.1. A transferência de conhecimento deve garantir que toda a informação gerada durante os processos de instalação e migração seja integralmente apresentada pela equipe da contratada, por meio de métodos expositivos, realização prática das atividades, apresentação de resumos, esquemas, relatórios ou qualquer outro documento que viabilize ou facilite a absorção da tecnologia do novo ambiente pela equipe da contratante.

7.12. Requisitos Legais

7.12.1. Deverão ser cumpridos os procedimentos, normas, modelos e regulamentos vigentes na Presidência da República.

7.12.2. O presente processo de contratação deve estar aderente à Constituição da República Federativa do Brasil de 1988 e as seguintes legislações vigentes:

7.12.2.1. Lei nº 14.133, de 1º de abril de 2021 (Nova Lei de Licitações);

7.12.2.2. Lei nº 13.709/2018: Lei Geral de proteção de Dados Pessoais - LGPD, dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

7.12.2.3. Decreto nº 10.024, de 20 de setembro de 2019, regulamenta os novos procedimentos para realização do pregão eletrônico nas aquisições de bens e contratações de serviços comuns, inclusive serviços comuns de engenharia, bem como dispõe sobre o uso da dispensa eletrônica, no âmbito da administração pública federal;

7.12.2.4. Instrução Normativa nº 40, de 22 de maio de 2020, dispõe sobre a elaboração dos Estudos Técnicos Preliminares - ETP - para a aquisição de bens e a contratação de serviços e obras, no âmbito da Administração Pública federal direta, autárquica e fundacional, e sobre o Sistema ETP digital;

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

7.12.2.6. Portaria SGD/MGI nº 1.070, de 1º de junho de 2023, estabelece o modelo de contratação de serviços de operação de infraestrutura e atendimento a usuários de Tecnologia da Informação e Comunicação, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

7.13. Requisitos de Garantia, Suporte e Manutenção

7.13.1. O prazo de execução da garantia contratual dos bens, complementar à garantia legal, é de, no mínimo, 60 meses, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data da assinatura do termo de recebimento definitivo do objeto.

7.13.2. O prazo de execução contratual do suporte e manutenção, é de, no mínimo, 60 meses, contado a partir do primeiro dia útil subsequente à data da assinatura do termo de recebimento definitivo do objeto.

7.13.3. A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

7.13.4. A garantia abrange a realização da manutenção corretiva dos bens pela própria Contratada, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

7.13.5. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

7.13.6. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

7.13.7. A Contratada realizará a reparação ou substituição dos bens que apresentarem vício ou defeito.

7.13.8. Durante a execução contratual será possível a troca dos equipamentos por versão superiores as estabelecidas neste Termo de Referência, sem qualquer ônus adicional a CONTRATANTE, caso os produtos apresentem defeito no período de vigência contratual. Entretanto, é necessária aceitação prévia e formal da equipe de gestão e fiscalização contratual.

7.13.9. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da Contratada.

7.13.10. A garantia legal ou contratual do objeto tem prazo de vigência próprio e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

7.13.11. Os requisitos e procedimentos referentes a garantia e suporte da solução, encontram-se pormenorizados no Termo de Referência.

7.13.12. O detalhamento dos requisitos de garantia e suporte encontram-se pormenorizados no Termo de Referência.

7.13.13. Duração da garantia e suporte

7.13.13.1. Nos processos de aquisições de bens de Tecnologia da Informação - TI, devido às suas características técnicas e por serem investimentos de alto custo, será sempre necessário que esses bens sejam acompanhados de uma garantia e de suporte para fins de assegurar o perfeito funcionamento da solução.

7.13.13.2. Em orientações anteriores de “BOAS PRÁTICAS, ORIENTAÇÕES E VEDAÇÕES PARA CONTRATAÇÃO DE ATIVOS DE TIC”, a antiga Secretaria de Tecnologia da informação do Ministério do Planejamento (Portaria MP/STI nº 20 /2016) padronizou que, nas elaborações das especificações técnicas de ativos de TI, deveriam ser observados:

“1.2.1 Os ativos de TI devem ser adquiridos com garantia de funcionamento provida pelo fornecedor durante sua vida útil, salvo quando justificado o contrário e com relação ao ativo em específico.

1.2.2. Tal procedimento se justifica pelo fato de que, de forma geral a contratação, a posteriori, de serviços de manutenção para ativos fora de garantia, usualmente é mais onerosa para a Administração do que quando o bem é adquirido com garantia para toda sua vida útil. Ainda, os contratos de manutenção têm seus custos elevados na medida em que os bens mantidos se tornam obsoletos. Ou seja, quanto mais antigo for o ativo de TI, menor seu valor comercial e maior será seu custo de manutenção, devido à dificuldade de provimento de peças de reposição e do maior risco do fornecedor descumprir os níveis de serviço exigidos para reparo desses equipamentos.

1.2.3. Tem-se, portanto, que um dos fatores que para definição do posicionamento adequado da tecnologia (item 1.1) é o tempo de vida útil previsto para utilização do ativo e, por conseguinte, o tempo de garantia de funcionamento a ser contratado.”

7.13.13.3. Se estabeleceu também a vida útil dos Ativos de Rede, tais como servidores de rede, aplicação, equipamentos de backup, armazenamento, segurança, entre outros:

“1.4.5.1 Para aquisição de servidores de rede, aplicação, equipamentos de backup, armazenamento, segurança, entre outros, deve-se considerar o tempo de vida útil mínimo de 5 (cinco) anos para fins de posicionamento da tecnologia e de garantia de funcionamento.”

7.13.13.4. Ressalta-se que os equipamentos a serem adquiridos nessa contratação, firewalls de próxima geração e de aplicações Web, são equipamentos de rede, de segurança e de aplicação, e, portanto, considera-se o tempo de vida útil desses equipamentos de no mínimo 5 anos (60 meses), devendo ser adquiridos com garantia de funcionamento (suporte e garantia) provida pelo fornecedor durante sua vida útil.

8. Estimativa da demanda - quantidade de bens e serviços

8.1. Atualmente a Presidência da República conta com 2 (dois) firewall de aplicação Web do fabricante F5, modelo BIG-IP 7055 SERIES, 01 BIG-IP Virtual Edition, instalados no Centro de Dados, Anexo I, do Palácio do Planalto.

8.2. Quantidade de bens e serviços

8.2.1. Para atendimento às necessidades, será necessária 01 Solução de firewalls de aplicações web. Segue abaixo o quadro com a estimativa e demanda de soluções necessárias para o completo atendimento da necessidade da Presidência da República:

GRUPO	ITEM	DESCRIÇÃO	UNIDADE	QTDE	JUSTIFICATIVA/MEMÓRIA DE CÁLCULO
Único	1	Solução de Firewall de Aplicação Web (Web Application Firewall), com 2 unidades F5 BIG IP R4800, com licenciamento Premium Service e License BEST Bundle, com BIG-IQ VE + BIG-IQ Data Collection Device (DCD) e com suporte técnico e garantia de 60 meses	Solução	1	Quantitativo referente a 1 Solução que funcionará no Centro de Dados, Anexo I, do Palácio do Planalto, baseado na descrição e nos requisitos tecnológicos
	2	Serviço de instalação e configuração da Solução de firewall de aplicação Web	Serviço	1	Quantitativo referente a instalação e configuração da solução baseada nas melhores práticas: Solução de firewall de aplicação Web (Web Application Firewall) e seus componentes de segurança
	3	Treinamento da solução (8 participantes)	Serviço	1	1 Turma com 8 participantes

9. Levantamento de soluções

9.1. Solução 01: Aquisição de conjunto de equipamentos de forma separada.

9.1.1. Solução composta por um conjunto de equipamentos, appliances, que tratam, cada um, de uma funcionalidade específica. Neste caso a solução nunca será composta apenas por um equipamento e, portanto, apresentará maiores dificuldades de gerenciamento das funcionalidades, pois cada equipamento terá sua plataforma de gerência.

9.1.2. Pontos positivos desta solução:

- a) Estrutura da solução mais robusta possível;
- b) Apresenta a possibilidade de aquisição de appliance dedicado para apenas uma funcionalidade considerada essencial para estruturar ou adicionar a infraestrutura de rede existente, e que necessite maior robustez;
- c) Podem ser contratadas separadamente conforme a necessidade da Presidência da República.

9.1.3. Pontos negativos desta solução:

- a) Exige gerenciamento descentralizado das soluções, pois cada appliance apresenta sua plataforma própria de gerência;
- b) Necessita de equipe técnica maior e mais capacitada para operacionalização dos equipamentos;
- c) O custo de soluções segregadas geralmente é maior que as integradas;

d) Dificuldade para correlacionar e analisar eventos em plataformas distintas o que impacta no poder e na tempestividade da reação do órgão diante de incidentes de segurança;

e) Ocupam mais espaço no Data Center e apresentam maior consumo de energia.

9.1.4. A aquisição de equipamentos específicos para cada funcionalidade (balanceamento, filtro de pacotes, anti-malware, VPN, filtro de camada de aplicação ...) não é uma solução muito eficiente, pois dificultará o gerenciamento e correlação dos eventos de segurança, característica relevante das soluções mais integradas, o que pode dificultar a detecção, contenção e o tratamento de uma incidente de segurança, elevando o risco de vazamento de dados e indisponibilidade dos serviços. Além disso, exigirá muitos especialistas com conhecimento nos diversos equipamentos ou soluções adquiridas e apresentará mais custo de espaço e energia.

9.1.5. Dessa forma, essa solução **não é viável** para atender a necessidade a Presidência da República.

9.2. Solução 02: Aquisição de equipamento do tipo NGFW – Firewall Corporativo com a funcionalidade de firewall de aplicação web (WAF)

9.2.1. Nessa solução a funcionalidade de firewall de aplicações web ou proteção contra ataques de camada de aplicação é realizado pelo firewall de próxima geração e a topologia da borda é composta por dois clusters deste tipo de equipamento. O NGFW constitui-se de equipamento capaz de agregar as diversas funcionalidades de segurança entre Firewall, Antivírus, IDS /IPS, WebFilter e outros, apresentando correlacionamento de dados entre os resultados das diversas funcionalidades. Estes equipamentos podem realizar inspeção em camada de aplicação e utilizam a mesma plataforma de gerência para todas as funcionalidades. Porém a inspeção realizada da camada de aplicação não é comparável ao nível de granularidade de inspeção de um equipamento WAF dedicado que ainda disporá de balanceamento de carga e DNS. Em muitas situações, para contar nos NGFW com essa capacidade de inspeção do tráfego na camada de aplicação, faz-se necessário contratar licenciamento adicional para seu uso. O WAF dedicado garantirá maior capacidade de inspeção e análise dos pacotes de camada 7 evitando uma maior latência e desonerando o NGFW para outras análises, garantindo melhor throughput da rede.

9.2.2. Vejamos as principais diferenças entre o WAF, IPS e NGFW:

	Web Application Firewall	Intrusion Prevention System	Next-Generation Firewall
Multiprotocol Security			
IP Reputation			
Web Attack Signatures			
Web Vulnerabilities Signatures			
Automatic Policy Learning			
URL, Parameter, Cookie and Form Protection			
Leverage Vulnerability Scan Results			

9.2.3. A análise da Xlabs Security (<https://www.xlabs.com.br/>) da figura acima, demonstra que o WAF dedicado tem atuação melhor comparada ao NGFW e ao IPS no que refere-se a assinaturas de vulnerabilidades web, aprendizado automático de políticas, proteção granular de URLs (Universal Resource Location), parâmetros, cookies e formulários das aplicações e melhor resultado médio em busca de vulnerabilidades.

9.2.4. Pelo exposto, essa solução **não é viável** para o atendimento às necessidades de segurança cibernética da Presidência da República.

9.3. Solução 03: Aquisição de equipamento do tipo Firewall de Aplicações Web (WAF-Appliance)

9.3.1. Solução composta por firewall de aplicações web, balanceador e DNS. Constitui-se de equipamento capaz de agregar as diversas funcionalidades de segurança entre Firewall, Antivírus, IDS/IPS, WebFilter e outros, apresentando correlacionamento de dados entre os resultados das diversas funcionalidades. Estes equipamentos podem realizar inspeção em camada de aplicação e utilizam a mesma plataforma de gerência para todas as funcionalidades. Porém a inspeção realizada da camada de aplicação não é comparável ao nível de granularidade de inspeção de um equipamento WAF dedicado que ainda disporá de balanceamento de carga e DNS.

9.3.2. Pontos positivos desta solução:

- a) É uma evolução da já consolidada plataforma unificada do tipo UTM sendo, inclusive, muitas fornecidas pelos mesmos fornecedores de UTM;
- b) Plataforma de gerenciamento unificado para as diversas funcionalidades de segurança de redes;
- c) Possuem garantia de capacidade para análise do tráfego por funcionalidade;
- d) Apresentam o maior nível de visibilidade no monitoramento e controle de ameaças devido ao correlacionamento das informações provenientes das diferentes funcionalidades;
- e) Exige menor conhecimento técnico/operacional por parte da equipe uma vez que as ferramentas de gerenciamento já são mais intuitivas e direcionadas para a configuração dos principais cenários de segurança de redes;
- f) Apresentam praticamente todas as funcionalidades essenciais à estruturação de uma solução de segurança de redes computacionais;
- g) Apresentam, adicionalmente, a capacidade de detectar malwares e ameaças em um nível satisfatório;
- h) Podem ser adquiridas em diversos portes de capacidade conforme a capacidade da Presidência da República, resultando em formas mais eficientes de utilização dos recursos do equipamento e no custo de aquisição.

9.3.3. Pontos negativos desta solução:

- a) Podem gerar problemas no dimensionamento de capacidade da appliance uma vez que sua performance depende de quais funcionalidades estão ativadas.

9.3.4. Pelas razões supracitadas essa solução **mostrou-se viável e completa**, adequada e a solução viável para atendimento às necessidades de segurança cibernética da Presidência da República.

10. Análise comparativa de soluções

10.1. A análise comparativa das soluções foi realizada no Item 9 - Levantamento de Soluções. A solução considerada viável para atender as necessidades da Presidência da República é **Solução 03: Aquisição de equipamento do Tipo Firewall de Aplicações Web (WAF)**.

10.2. Análise da existência de software público brasileiro e adequação às políticas, os modelos e os padrões de governo:

Requisito	Solução	Sim	Não	Não se Aplica
Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3	X		
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 1	X		

A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 2	X		
	Solução 3	X		
A Solução é aderente às regulamentações da ICP Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X

11. Registro de soluções consideradas inviáveis

11.1. Conforme demonstrado no item 9 - Levantamento de Soluções, as seguintes soluções foram consideradas inviáveis:

- 11.1.1. Solução 01: Aquisição de conjunto de equipamentos de forma separada;
- 11.1.2. Solução 02: Aquisição de equipamento do tipo NGFW - Firewall Corporativo com a funcionalidade de firewall de aplicação web (WAF).

12. Análise comparativa de custos (TCO)

12.1. Descrição da Solução Viável: Aquisição de equipamentos do tipo Firewall de Aplicações Web - WAF (Solução 03).

12.1.1. A análise comparativa de custos foi elaborada considerando apenas as soluções técnicas e funcionalmente viáveis, nos termos do inc. III, Art. 11, da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, incluindo:

- a) cálculo dos custos totais de propriedade (Total Cost Ownership - TCO) por meio da obtenção dos custos inerentes ao ciclo de vida dos bens e serviços de cada solução, a exemplo dos valores de aquisição dos ativos, insumos, garantia técnica estendida, manutenção, migração e treinamento; e
- b) memória de cálculo que referencie os preços e os custos utilizados na análise, com vistas a permitir a verificação da origem dos dados.

12.1.2. Custo Total de Propriedade – Memória de Cálculo – Aquisição de Solução de Equipamentos Firewall de Aplicação (WAF):

Grupo	Item	Descrição	Código CATMAT	Qtde.	Menor Preço (R\$)	Média (R\$)	Mediana (R\$)	Maior Preço (R\$)
Único	1	Solução de Firewall de Aplicação Web (Web Application Firewall), com 2 unidades F5 BIG IP R4800, com licenciamento Premium Service e License BEST Bundle, com BIG-IQ VE + BIG-IQ Data Collection Device (DCD) e com suporte técnico e garantia de 60 meses	481646	1	3.187.090,00	4.663.846,12	5.219.848,37	5.584.600,00

	2	Serviço de instalação e configuração da Solução de firewall de aplicação Web	027111	1	60.000,00	116.540,34	89.071,02	216.100,00
	3	Treinamento da solução (8 participantes)	016837	1	100.000,00	182.943,84	163.632,00	293.300,00
Total					3.347.090,00	4.963.330,30	5.472.551,39	6.094.000,00
Valor Total de Referência					R\$ 4.880.386,46			

Obs.: Os valores apurados na tabela acima se encontram consignados na Planilha Comparativa de Preços 2024 - Cotação-Detalhado-41-2024 (SUPER nº 4956176)

12.1.3. Mapa Comparativo dos Cálculos Totais de Propriedade:

GR	IT	DESCRIÇÃO DA SOLUÇÃO	ESTIMATIVA DE TCO AO LONGO DOS ANOS (R\$)					TOTAL (R\$)
			ANO 1	ANO 2	ANO 3	ANO 4	ANO 5	
Único	1	Solução de Firewall de Aplicação Web (Web Application Firewall), com 2 unidades F5 BIG IP R4800, com licenciamento Premium Service e License BEST Bundle, com BIG-IQ VE + BIG-IQ Data Collection Device (DCD) e com suporte técnico e garantia de 60 meses	4.663.846,12	- X -	- X -	- X -	- X -	4.663.846,12
	2	Serviço de instalação e configuração da Solução de firewall de aplicação Web	116.540,34	- X -	- X -	- X -	- X -	116.540,34
	3	Treinamento da solução (8 participantes)	100.000,00	- X -	- X -	- X -	- X -	100.000,00
TOTAL			4.880.386,46	- X -	- X -	- X -	- X -	4.880.386,46

13. Descrição da solução de TIC a ser contratada

13.1. Solução de firewall de aplicações web (WAF) para prover as seguintes funcionalidades e controles de segurança:

- a) Filtro e inspeção de pacotes de camada 7;
- b) Balanceamento de carga das aplicações e DNS;
- c) Proteção contra ataques de camada 7;
- d) Publicação e balanceamento de DNS;
- e) Proteção Anti-DDoS.

13.2. A Solução de Firewall de Aplicação Web (WAF) proverá proteção contra ataques de camada de aplicação e de negação de serviços, além de publicar as aplicações da Presidência da República na Internet de forma otimizada e balancear o tráfego das aplicações entre os ativos de infraestrutura e rede da Presidência da República.

13.3. Parcelamento da solução

13.3.1. No contexto de obtenção de serviços pela administração pública, verificou-se que a legislação preza pela análise técnica e econômica para decidir sobre a divisão do objeto, senão vejamos:

Lei 14.133, Seção IV, Disposições Setoriais, Subseção I, Das Compras

"Art. 40. O planejamento de compras deverá considerar a expectativa de consumo anual e observar o seguinte:

... § 2º Na aplicação do princípio do parcelamento, referente às compras, deverão ser considerados:

I - a viabilidade da divisão do objeto em lotes;"

13.3.2. O objeto desta contratação será em grupo único, por solução WAF e dividido em 03 itens, atendendo ao preceituado da citada Lei 14.133.

13.3.3. Um requisito fundamental para que haja viabilidade técnica e também administrativa da contratação em questão, é o de que o conjunto de serviços/soluções sejam agrupados e licitados em um único grupo, sendo assim com adjudicação para um único licitante vencedor, ou seja, não haverá parcelamento.

13.4. A definição pela contratação em grupo único, com três itens levou em consideração a viabilidade técnica de operação e gerenciamento da solução de firewall que funciona de forma integrada entre os appliances e a solução de gerência, faz-se necessário que esses itens façam parte de um mesmo agrupamento em um grupo, para garantir o gerenciamento e a interoperabilidade da operação sem prejuízos nas análises e correlação dos eventos.

14. Estimativa de custo total da contratação

Valor (R\$): 4.880.386,46

14.1. Memória de Cálculo = **R\$ 4.880.386,46** (quatro milhões, oitocentos e oitenta mil trezentos e oitenta e seis reais e quarenta e seis centavos).

15. Justificativa técnica da escolha da solução

15.1. Considera-se tecnicamente viável a **Solução 03** pelas necessidades de equipamentos para atenderem as demandas de segurança e gestão da rede da Presidência da República (PR), tendo em vista a descontinuidade dos serviços contratados (29 de dezembro de 2023).

15.2. Além de oferecer um nível maior de segurança à rede, os firewall de aplicação, com uma maior capacidade de processamento, possibilitam a implementação de novos serviços, como por exemplo, análise do tráfego. Com isso, seria possível ter uma visualização detalhada da utilização das aplicações utilizadas. Adicionalmente, o processo de identificação de ameaças são facilitados e permitem a aplicação de políticas de segurança mais eficientes.

15.3. Com o aumento no número de usuários trabalhando de casa e com o aumento na quantidade de ataques às empresas, principalmente na tentativa de sequestro de dados em troca de resgate, fez com que as necessidades do uso de firewalls para conter ataques de negação de serviço e bloquear infecções maliciosas, principalmente em casos de ataques de ransomware, aumentassem as necessidades de equipamentos capazes de comportarem uma maior e mais rápida análise do tráfego de dados na rede institucional.

16. Justificativa econômica da escolha da solução

16.1. Foi utilizado como parâmetro os preços do Painel de Preços do Governo Federal (<https://paineldepregos.planejamento.gov.br/>), no período de 05/04/2024 a 08/04/2024, com os seguintes códigos do CATMAT/CATSERV:

CATMAT/ CATSER	DESCRIÇÃO DO CATMAT/CATSER
016837	TREINAMENTO INFORMÁTICA - EQUIPAMENTO / HARDWARE
027111	SERVIÇOS DE INSTALAÇÃO DE COMPUTADORES E SEUS PERIFERICOS
481646	EQUIPAMENTO SEGURANÇA REDE, TIPO: AMPPLIANCE, APLICAÇÃO: FIREWALL

16.2. Deste modo, com os códigos acima com, foram coletados os dados e aplicado cálculo da média dos preços, obtendo-se o custo médio total estimado para a presente aquisição de **R\$ 4.880.386,46** (quatro milhões, oitocentos e oitenta mil trezentos e oitenta e seis reais e quarenta e seis centavos).

16.3. A contratação da **Solução 3** proporcionará continuidade do negócio para a Presidência da República, devido a seleção da melhor solução de segurança de perímetro para a infraestrutura de rede, tanto técnica e quanto economicamente, por um período de 60 meses.

17. Benefícios a serem alcançados com a contratação

17.1. A contratação visa obter principalmente os resultados abaixo:

17.1.1. Prover a Presidência da República uma estrutura de segurança da informação robusta incorporada por soluções de tecnologia modernas aptas para suportar todos os serviços prestados pela DITEC, e também, fornecer o alcance das necessidades do órgão fortalecendo a estratégia de segurança da informação contra ameaças avançadas de todos os tipos;

17.1.2. Garantir que a infraestrutura da rede da Presidência da República possua todos os requisitos necessários para atender as demandas internas da DITEC, e também tenha a possibilidade de ampliação de forma segura da capacidade tecnológica em demandas futuras;

17.1.3. Amplificação da camada de proteção e disponibilidade da informação;

17.1.4. Disponibilidade do ambiente de rede com segurança e visibilidade;

17.1.5. Ampliação da segurança da informação na Presidência da República;

17.1.6. Adequação às legislações vigentes, tais como LGPD – Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e Marco Civil da Internet Lei nº 12.965/2014);

17.1.7. Mitigação de riscos de ataques digitais;

17.1.8. Mitigação de riscos de paralização dos serviços de TI;

17.1.9. Aumento da confidencialidade, integridade, níveis de segurança da informação, da eficiência de monitoração de eventos de segurança e disponibilidade das informações;

17.1.10. Expansão da proteção atualmente existente para os novos equipamentos adquiridos ou em fase de aquisição;

17.1.11. Governança da segurança da informação em tempo próximo ao real;

17.1.12. Reter os eventos e informações de segurança em longo prazo, de acordo com as políticas da organização;

17.1.13. Reportar o estado de segurança e conformidade do ambiente de TI da Presidência da República;

17.1.14. Minimizar riscos relacionados à segurança da informação e da rede, de sistemas e de serviços corporativos;

17.1.15. Garantir a disponibilidade dos recursos do ambiente computacional da Presidência da República, além de otimizar o uso dos acessos à Rede WAN e Internet;

17.1.16. Prover a proteção da informação contra ameaças a sua confidencialidade, integridade e disponibilidade;

17.1.17. Reestruturar e modernizar a arquitetura de rede da Presidência da República;

- 17.1.18. Garantir a continuidade dos negócios da Presidência da República por intermédio de melhorias, apoio técnico e manutenções da solução a ser adquirida;
- 17.1.19. Aumentar a velocidade de conexão entre os servidores e ativos de rede do Data Center;
- 17.1.20. Prover solução de gerenciamento e monitoramento eficiente dos ativos de rede do Data Center;
- 17.1.21. Prover mecanismos de alta disponibilidade, mecanismos de segurança e balanceamento de carga entre Data Center;
- 17.1.22. Manter um ambiente licenciado, atualizado e acima de tudo seguro, levando em consideração problemas de vulnerabilidades e disponibilidade corrigidos em versões superiores as atuais.

18. Providências a serem Adotadas

18.1. Não há necessidade de adequação da infraestrutura tecnológica, elétrica, logística, espaço físico, mobiliário ou outras que se apliquem.

19. Declaração de Viabilidade

Esta equipe de planejamento declara **viável** esta contratação.

19.1. Justificativa da Viabilidade

19.1.1 A declaração da viabilidade da contratação expressa nesta seção apresenta a justificativa da solução escolhida, abrangendo a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade.

19.2. Nesse sentido, o planejamento em tela almeja os seguintes benefícios e resultados:

19.2.1. Proteção contra ataques aos serviços de TI da Presidência da República, mitigando riscos de indisponibilidade de serviços e vazamento de dados da Presidência da República. Otimização dos controles de segurança cibernética da pasta e alinhamento aos normativos de segurança da informação do Governo Federal e às melhores práticas e frameworks do mercado. Garantir a qualidade, o desempenho e a alta disponibilidade das informações e dos equipamentos da Presidência da República.

19.2.2. Economia no valor da aquisição.

19.3. Além disso, frisa-se que a presente contratação atende adequadamente às demandas de negócio formuladas, os benefícios a serem alcançados são adequados, os custos previstos são compatíveis e caracterizam a economicidade, os riscos envolvidos são administráveis.

19.4. Por fim, considerando as informações do presente estudo, entende-se que a presente contratação se configura tecnicamente VIÁVEL para a **Solução 03**.

20. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

NELSON GONCALVES REZENDE

Integrante Requisitante



Assinou eletronicamente em 07/06/2024 às 16:06:54.

JAN CARLOS RODRIGUES TELES

Integrante Técnico



Assinou eletronicamente em 12/06/2024 às 12:11:41.

ROBSON MARTINS GUIMARAES DA SILVA

Integrante Técnico



Assinou eletronicamente em 11/06/2024 às 10:08:31.

BRUNO PEREIRA PONTES

Autoridade competente



Assinou eletronicamente em 13/06/2024 às 16:39:49.

Lista de Anexos

Atenção: Apenas arquivos nos formatos ".pdf", ".txt", ".jpg", ".jpeg", ".gif" e ".png" enumerados abaixo são anexados diretamente a este documento.

- Anexo I - Especificações Técnicas - WAF, vSegunda.pdf (678.66 KB)

Anexo I - Especificações Técnicas - WAF, vSegunda.pdf

Especificações Técnicas

1. ESPECIFICAÇÕES TÉCNICAS

1.1. Para comprovação dos itens das especificações técnicas da solução, serão aceitos datasheets, documentos e cartas do fabricante dos produtos ou ainda registros da CLI (Command Line Interface) dos produtos que asseverem o atendimento aos requisitos.

1.2. A solução é composta por um cluster contendo 2 (dois) equipamentos do tipo Web Application Firewall (WAF), gerência centralizada, incluindo o fornecimento de licenças, o fornecimento de transceivers, serviços de instalação, configuração, transferência de conhecimento, garantia e suporte técnico.

1.3. Há uma grande variedade de fabricantes de Web Application Firewall. Entretanto, é importante reforçar que há um alto grau de complexidade na administração e gerenciamento destas ferramentas, e a portabilidade entre elas não é uma tarefa fácil nem rápida. A Presidência da República dispõe atualmente de equipamentos da fabricante F5 Networks, e esta equipe de planejamento da contratação considera que se deve manter o fabricante para o melhor benefício de todos os usuários que acessam os serviços da Presidência da República.

1.4. Tendo em vista que o esforço realizado numa eventual migração de equipamento para um novo fabricante acarretará em um risco de total indisponibilidade de todos os portais e serviços hospedados no Centro de Dados da Presidência da República.

1.5. Não há qualquer tipo de cerceamento da competitividade na definição do fabricante F5 para a garantia do melhor interesse da Presidência da República e para a lisura e competitividade de um procedimento licitatório idôneo, uma vez que existem ao menos 11 representantes autorizados pela fabricante para oferecerem os equipamentos solicitados, conforme pode ser observado no site do próprio fabricante: <https://www.f5.com/partners/find-a-partner?partnerLocation=Brazil&partnerPage=1>, acessado em 31 de outubro de 2023.

2. CARACTERÍSTICAS DO HARDWARE QUE CONTEMPLAM AS SEGUINTE FUNCCIONALIDADES

2.1.1. Os appliances físicos devem ser novos e de primeiro uso;

2.1.2. Os equipamentos devem ser fornecidos em modo appliance, com conjunto de hardware e software dedicados, não podendo ser servidor de uso genérico, e que atendam todas as funcionalidades descritas nas Especificações técnicas mínimas;

2.1.3. Devem ser novos, sem uso prévio e entregues em perfeito estado de funcionamento. Não devem ser remanufaturados, recondicionados ou possuir reparos de qualquer espécie;

2.1.4. Não serão aceitos equipamentos ou softwares que constem em anúncio ou lista do tipo end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, produtos que serão descontinuados, perderão suporte e garantia oficiais do fabricante;

2.1.5. As funcionalidades da solução (balanceador de carga, global server load balancing, proteção para aplicação, proteção para a rede, proteção contra-ataque DDoS, DNS Application Firewall, inspeção SSL, etc) deverão ser licenciadas pelo período de 60 (sessenta) meses;

2.1.6. Deverão ser fornecidos no mínimo 2 appliances para o uso em alta disponibilidade, cada um contemplando as seguintes características/funcionalidades:

2.1.2. Distribuição de carga e otimização das aplicações.

2.1.3. Proteção contra-ataques de aplicação.

2.2. O equipamento deverá ser novo, de primeiro uso e acondicionado adequadamente em caixa lacrada de fábrica, de forma a propiciar completa segurança durante o transporte.

2.3. Equipamento do tipo appliance, possuir altura de, no máximo, 2U, deve ser instalado em rack de 19" e vem acompanhado do kit de instalação.

2.4. Processador mínimo octa core.

2.5. Possuir quantidade total de memória (RAM) de, no mínimo, 64 GB (sessenta e quatro Gigabytes).

2.6. Possuir placa dedicada a tratar tráfego SSL (hardware).

2.7. Possuir, no mínimo, um disco com 480GB de espaço de armazenamento do tipo SSD.

2.8. Possuir no mínimo 2 fontes hot swappable.

2.9. Mínimo de 01 (uma) porta console para configuração através de CLI (Command Line Interface) para cada appliance.

2.10. Possuir 1 (uma) interface Gigabit Ethernet para gerenciamento out-of-band.

2.11. Possuir, no mínimo, 4 (quatro) interfaces 1 (um) Gigabit em cobre, seja através de portas nativas ou de slots SFP com os devidos transceivers 1000BASE-T.

2.12. Deve possuir no mínimo, por appliance, 4 portas 25/10/1 GbE SPF+/SFP28/SPF ou no mínimo 6 portas 1/10 GbE SFP/SFP+ que permita fazer agregação das interfaces para comunicação com switches, em ambos os casos incluindo todos os respectivos transceivers.

2.13. Todas as portas de fibras referenciadas no item anterior devem vir em cada appliance acompanhadas dos respectivos transceivers e de 04 (quatro) cordões ópticos padrão lc/lc de no mínimo 5 metros multimodo e 04 (quatro) cordões ópticos padrão lc/lc de no mínimo 10 metros multimodo.

2.14. Desempenho por appliance:

- 2.14.1. Possuir capacidade para operar, no mínimo, 50/40 Gbps de tráfego na camada L4/L7;
- 2.14.2. Possuir capacidade de operar, no mínimo, 45.000 TPS de tráfego SSL com chaves de 2048 bits;
- 2.14.3. Possuir capacidade de operar, no mínimo, 20.000 TPS de tráfego SSL com chaves ECDSA P-256;
- 2.14.4. Possuir capacidade de operar, no mínimo, 25 Gbps de tráfego SSL;
- 2.14.5. Possuir capacidade de operar, no mínimo, 1.8 milhão de requisições por segundo na camada 7;
- 2.14.6. Possuir capacidade de operar, no mínimo, 750 mil conexões por segundo na camada 4;
- 2.14.7. Possuir capacidade de operar, até 38 milhões de conexões concorrentes L4;
- 2.14.8. Possuir painel de LCD frontal com funções básicas;
- 2.14.9. Possuir Compressão de Hardware de no mínimo 30 Gbps em tráfego HTTP/HTTPS;
- 2.14.10. Recursos de agregação de portas baseado no protocolo LACP em seus modos ativo e passivo;
- 2.14.11. Deve suportar, até 3.500.000 (três milhões e quinhentos mil) requisições HTTP por segundo na camada 4 do modelo OSI;
- 2.14.12. Deve suportar, no mínimo, 80.000.000 (oitenta milhões) de pacotes SYN/segundo, sob ataque de SYN Flood.

3. CARACTERÍSTICAS GERAIS PARA A SOLUÇÃO

- 3.1. Suportar e garantir a instalação em ambiente de alta disponibilidade.
- 3.2. Assegurar que o equipamento deverá ser capaz de trabalhar no modo Ativo/Standby, com equipamento da mesma marca e modelo.
- 3.3. A solução deve operar no modo Ativo/Ativo, mantendo o status das conexões. Aceita-se como Ativo/Ativo a utilização de dois endereços Virtuais, onde cada endereço fica ativo em um elemento e standby no outro.
- 3.4. Assegurar que a operação da solução de 2 ou mais equipamentos, quando implementada em ambiente redundante suporte sincronismo de sessão entre os dois membros. A falha do equipamento principal não deverá causar a interrupção das sessões balanceadas.
- 3.5. A solução deve fornecer todos os recursos possíveis de redundância sem nenhuma despesa com licenças adicionais.

- 3.6. A solução deve possuir escalabilidade, podendo crescer na forma de cluster adicionando novos appliances inclusive de modelos diferentes.
- 3.7. O equipamento deverá possuir sistema operacional certificado ICSA Labs podendo assim ser instalado na borda antes de qualquer equipamento de segurança.
- 3.8. A solução deve fornecer recurso de agregação de portas baseado no protocolo LACP.
- 3.9. Deve possuir suporte a LACP em modo passivo e ativo.
- 3.10. A solução deve fornecer recurso para suportar até 32 portas em um mesmo conjunto agregado.
- 3.11. Deve possuir suporte a Spanning-Tree (802.1D), Fast Spanning-Tree (802.1w, 802.1t) e Multi Spanning-Tree (802.1s).
- 3.12. Deve fornecer recurso para o transporte de múltiplas VLAN por uma única porta (ou por um conjunto agregado de portas) utilizando o protocolo 802.1q.
- 3.13. Possuir suporte a IPv6.
- 3.14. A solução deve suportar múltiplas tabelas de rotas independentes.
- 3.15. O equipamento, quando habilitado para mais de uma função deverá permitir a definição da importância da função, determinando quanta CPU e memória será alocada para cada tipo de funcionalidade.
- 3.16. Possuir capacidade para gerenciar os recursos disponíveis de acordo com as funções habilitadas nos equipamentos.
- 3.17. A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6.
- 3.18. Possuir ferramenta online web gratuita na qual seja possível carregar as configurações e receber diagnóstico da solução com informações sobre atualizações, melhores práticas, estado da solução e informações preventivas.
- 3.19. Possuir suporte à funcionalidade de VXLAN, essencial para integração com o ambiente de virtualização (Software Defined Network).
- 3.20. Serviço de suporte técnico na modalidade de 24x7 (24 horas/dia e 7 dias/semana) durante 60 meses.
- 3.21. Na data da proposta e durante a vigência do contrato, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale.

3.22. Deve se integrar com sistemas de gerenciamento de containers (ex.:Kubernetes/Openshift), de modo a permitir que mudanças dinâmicas na infraestrutura de microsserviços sejam refletidas automaticamente no balanceamento de entrada, aumentando ou diminuindo a quantidade de pods, e ainda, inserindo ou removendo serviços do Big-IP.

3.23. Deve ser integrado nativamente ao Kubernetes/Openshift para realizar obalanceamento entre pods.

3.24. Deve criar os serviços de Balanceamento de Carga dinamicamente ao mesmo tempo em que uma nova aplicação é provisionada pelo Kubernetes/Openshift.

4. FUNCIONALIDADE DE GERENCIAMENTO

4.1. Implementar uma configuração de endereçamento IP estático ou dinâmico (DHCP/BOOTP) para o gerenciamento.

4.2. Implementar o SNTP (Simple Network Time Protocol) ou NTP (Network Time Protocol).

4.3. Permitir acesso in-band via SSH.

4.4. Manter internamente múltiplos arquivos de configurações do sistema.

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

4.6. Possuir auto-complementação de comandos na CLI.

4.7. Possuir ajuda contextual.

4.8. Interface por linha de comando (CLI – Command Line Interface) que possibilite a configuração dos equipamentos.

4.9. Possuir, no mínimo, Três níveis de usuários na GUI – Super-Usuário, Usuário com permissões reduzidas, e usuário Somente Leitura.

4.10. Os usuários de gerência deverão poder ser autenticados em bases remotas. No mínimo RADIUS, LDAP e TACACS+ deverão ser suportados.

4.11. Deverá ser possível receber da base RADIUS, LDAP e TACACS+ o nível de acesso (Grupo ou Permissões).

4.12. Possuir Interface Gráfica via Web.

4.13. A interface Gráfica deverá permitir a atualização do sistema operacional e/ou a instalação de patches ou Hotfixes sem o uso da linha de comando.

- 4.14. A interface gráfica deverá permitir a configuração de qual partição o equipamento deverá dar o boot.
- 4.15. Possuir um comando, via CLI, que mostre o tráfego de utilização das interfaces (bps e pps).
- 4.16. Suportar o rollback de configuração e imagem.
- 4.17. Possuir e fornecer geração de mensagens de syslog para eventos relevantes ao sistema.
- 4.18. Possuir configuração de múltiplos syslog servers para os quais o equipamento irá enviar as mensagens de syslog.
- 4.19. Possuir armazenamento de mensagens de syslog em dispositivo interno ao equipamento.
- 4.20. A interface Gráfica deverá permitir a reinicialização do equipamento.
- 4.21. Reinicialização do equipamento por comando na CLI.
- 4.22. Possuir recurso de gerência via SNMP e implementar SNMPv1, SNMPv2c e SNMPV3.
- 4.23. Possuir traps SNMP.
- 4.24. Possui suporte a monitoração utilizando RMON através de pelo menos 4 grupos: statistics, history, alarms e events.
- 4.25. Os logs de sistema devem ter a opção de ser armazenados internamente ao sistema ou em servidor externo.
- 4.26. Implementar Debugging: CLI via console e SSH.
- 4.27. Deve possuir suporte a Link Layer Discovery Protocol (LLDP).
- 4.28. Deve ser possível enviar, pelo menos, as seguintes informações via LLDP: Port ID, TTL, Port Description, System Name, System Description, Management Address, Port VLAN ID, Port and Protocol VLAN ID, VLAN Name, Protocol Identity, Link Aggregation, Maximum Frame Size.
- 4.29. A Solução deve ter a capacidade de permitir a criação de MIBs customizadas.
- 4.30. A Solução deve ter suporte a sFlow.

5. DISTRIBUIÇÃO DE CARGA E OTIMIZAÇÃO DAS APLICAÇÕES

- 5.1. Suportar todas as aplicações comuns de um Switch Layer 7, como:
 - 5.1.1. Server Load-Balancing;

5.1.2. Firewall Load-Balancing;

5.1.3. Proxy Load-Balancing.

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

5.3. A solução de Load Balance deve possuir, no mínimo, capacidade de resposta aos clientes por roteamento direto (os servidores balanceados respondem diretamente aos clientes), tunelamento (a solução é capaz de utilizar servidores de redes diferentes da que está inserida) ou fullproxy (todas as transações entre clientes e servidores são intermediadas pela solução).

5.4. A solução deve permitir o encapsulamento, em camada 3, do tráfego entre o balanceador e o servidor para tráfego IPv4 e IPv6, quando o balanceamento é realizado apenas em direção ao servidor, onde a resposta do servidor real é enviada diretamente ao cliente.

5.5. Permitir a clonagem de pools, de forma que a solução envie uma cópia do tráfego para um pool adicional, como por exemplo um pool de IDSs ou Sniffers, para fins de análise de tráfego de rede ou mesmo para identificação de padrões de acesso não permitidos ou indicações de atividade maliciosas ou ataques de rede.

5.6. Possuir recursos para balancear servidores com qualquer hardware, sistema operacional e tipo de aplicação.

5.7. A solução deve possuir recurso de ativação de grupo prioritário, no qual o administrador pode especificar a quantidade mínima de servidores que devem estar disponíveis em cada grupo e a prioridade dos grupos.

5.8. Caso o número de servidores disponíveis fique menor do que o estipulado pelo administrador, a solução deve automaticamente distribuir o tráfego para o próximo grupo com maior prioridade não afetando o serviço.

5.9. Caso o número de servidores disponíveis volte ao valor mínimo estipulado pelo administrador, a solução deve automaticamente retirar o grupo com menor prioridade de balanceamento, voltando ao estado original.

5.10. Possuir capacidade de abrir um número reduzido de conexões TCP com o servidor e inserir os HTTP requests gerado pelos clientes nestas conexões, reduzindo a necessidade de estabelecimento de conexões nos servidores e aumentando a performance do serviço.

5.11. Suportar os seguintes métodos de balanceamento:

5.11.1. Round Robin;

5.11.2. Least Connections;

5.11.3. Weighted Percentage (por peso);

- 5.11.4. Servidor ou equipamento com resposta mais rápida baseado no tráfego real;
- 5.11.5. Weighted Percentage dinâmico (baseado no número de conexões);
- 5.11.6. Dinâmico, baseado em parâmetros de um determinado servidor ou equipamento, coletados via SNMP ou WMI.
- 5.12. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web.
- 5.13. Possuir recursos para balancear as sessões novas, mas preservar sessões existentes no mesmo servidor, implementando persistência de sessão dos seguintes tipos:
 - 5.13.1. Por cookie: inserção de um novo cookie na sessão;
 - 5.13.2. Por cookie: utilização do valor do cookie da aplicação, sem adição de cookie;
 - 5.13.3. Por endereço IP destino;
 - 5.13.4. Por endereço IP origem;
 - 5.13.5. Por sessão SSL;
 - 5.13.6. Através da análise da URL acessada;
 - 5.13.7. Através da análise de qualquer parâmetro no header HTTP;
 - 5.13.8. Através da análise do MS Terminal Services Session (MSRDP);
 - 5.13.9. Através da análise do SIP Call ID ou Source IP;
 - 5.13.10. Através da análise de qualquer informação da porção de dados (camada 7).
- 5.14. A solução deve utilizar Cache Array Routing Protocol (CARP) no algoritmo de HASH.
- 5.15. O equipamento oferecido deverá suportar os seguintes métodos de monitoramento dos servidores reais:
 - 5.15.1. Layer 3 – ICMP;
 - 5.15.2. Conexões TCP e UDP pela respectiva porta no servidor;
 - 5.15.3. Devem existir monitores predefinidos para, no mínimo, os seguintes protocolos: ICMP, HTTP, HTTPS, Diameter, FTP, SASP, SMB, RADIUS, MSSQL, NNTP, ORACLE, RPC, LDAP (em especial Microsoft AD), IMAP, SMTP, POP3, SIP, Real Server, SOAP, SNMP e WMI.

- 5.16. Possuir recursos para balanceamento de carga de servidores SIP para VoIP (equipamento SIP PROXY).
- 5.17. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor real.
- 5.18. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor virtual.
- 5.19. Possuir recursos para limitar o número de sessões estabelecidas com cada grupo de servidores.
- 5.20. Possuir recursos para limitar o número de sessões estabelecidas com cada servidor físico:
- 5.20.1. Realizar Network Address Translation (NAT);
 - 5.20.2. Realizar Proteção contra Denial of Service (DoS);
 - 5.20.3. Realizar Proteção contra Syn flood;
 - 5.20.4. Realizar Limpeza de cabeçalho HTTP.
- 5.21. A solução deve permitir o controle da resposta ICMP por servidor virtual.
- 5.22. Possuir recursos para que a configuração seja baseada em perfis, permitindo uma fácil administração.
- 5.23. Possuir capacidade de geração e gestão de perfis hierarquizados, permitindo maior facilidade na administração de políticas similares.
- 5.24. Permitir a criação de Virtual Servers com endereço IPv4 e os servidores reais com endereços IPv6.
- 5.25. Possuir recursos para executar compressão de conteúdo HTTP, para reduzir a quantidade de informações enviadas ao cliente.
- 5.26. Deve permitir compressão tipo GZIP e Deflate.
- 5.27. Definir qual tipo de compressão será habilitada (gzip1 a gzip9, deflate).
- 5.28. Possuir capacidade para definir compressão especificamente para certos tipos de objetos.
- 5.29. Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições HTTP são enviadas aos servidores sem criptografia.
- 5.30. Permitir a definição de quais tipos de objeto serão armazenados ou não em cache.
- 5.31. Permitir a reescrita de requisições HTTP baseado no conteúdo da URL, possibilitando o redirecionamento de requisições HTTP para HTTPS.

- 5.32. Permitir a reescrita de respostas HTTP, possibilitando a inclusão de cabeçalho (header) customizado.
- 5.33. Suportar multiplexação TCP e Reuso de Sessão para reaproveitamento e uso eficiente de conexões entre a solução de balanceamento de aplicações e os servidores balanceados.
- 5.34. Garantir que na aceleração de SSL, tanto a troca de chaves quanto a criptografia dos dados sejam realizadas com aceleração em hardware, para não onerar o sistema, este item somente é válido para solução em appliance.
- 5.35. Deve possuir capacidade de importação dos certificados e chaves criptográficas, para transações seguras entre cliente/servidor, podendo assim operar em modo “man in the middle”, ou seja, descriptografar, otimizar e re-criptografar o tráfego SSL em comprometer a segurança da conexão SSL estabelecida previamente entre cliente/servidor. Caso haja falha na leitura da conexão SSL, esta deverá, se assim definido, prosseguir em regime de passthrough.
- 5.36. A solução deve possuir a funcionalidade de espelhamento de conexões SSL.
- 5.37. A solução deve possuir a capacidade de redirecionar o SSL Offload (troca de chaves) de determinado serviço para outro appliance físico que tenha mais capacidade para tratamento SSL. Dessa forma deve ser possível otimizar recursos executando tarefas que exigem muito desempenho para serem tratadas em hardware especializado.
- 5.38. Possuir recursos para configurar o equipamento para recriptografar em SSL a requisição ao enviar para o servidor, permitindo as demais otimizações em ambiente 100% criptografado.
- 5.39. Todas as funcionalidades de inspeção, proteção e aceleração de tráfego criptografado através de SSL/TLS especificadas neste edital devem estar disponíveis quando a conexão segura for estabelecida usando:
- 5.39.1. Autenticação do servidor por parte do cliente, através da verificação da validade do certificado digital fornecido pelo lado servidor durante o processo de estabelecimento do túnel SSL/TLS.
- 5.39.2. Autenticação do cliente por parte do servidor, através da solicitação e verificação da validade do certificado digital fornecido pelo cliente durante o processo de estabelecimento do túnel SSL/TLS. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea;
- 5.39.3. Ambas as autenticações acima mencionadas ocorrendo de forma simultânea.
- 5.40. Ao realizar inspeção, proteção, OffLoad e aceleração de tráfego criptografado através de SSL/TLS, a solução deverá ser capaz de:
- 5.40.1. Encaminhar ao servidor real via cabeçalho HTTP ou de forma transparente, todo o certificado digital utilizado pelo lado cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS;

5.40.2. Encaminhar ao servidor real via cabeçalho HTTP campos específicos do certificado digital utilizado pelo cliente para se autenticar perante o servidor durante o processo de estabelecimento do túnel SSL/TLS.

5.41. A solução deve permitir aplicar criptografia de cookies para a proteção dos cookies utilizados pela aplicação web.

5.42. Possuir recursos para fazer aceleração de SSL, onde os certificados digitais são instalados no equipamento e as requisições POP3, IMAP e SMTP são enviadas aos servidores sem criptografia.

5.43. A solução deve possuir diversos recursos relacionados ao uso de criptografia com o objetivo de otimizar e minimizar o impacto na performance das aplicações. Dentre eles deve ser possível configurar parâmetros como:

5.43.1. SSL session cache Timeout;

5.43.2. Session Ticket;

5.43.3. OCSP (Online Certificate Status Protocol) Stapling;

5.43.4. Dynamic Record Sizing;

5.43.5. ALPN (Application Layer Protocol Negotiation);

5.43.6. Perfect Forward Secrecy.

5.44. Suportar a utilização de memória RAM como cache de objetos HTTP, para responder às requisições dos usuários sem utilizar recursos dos servidores.

5.45. Possuir capacidade, no uso do recurso de cache, em definir quais tipos de objeto serão armazenados em cache e quais nunca devem ser cacheados.

5.46. Garantir que o recurso de cache possa ajustar quanta memória será utilizada para armazenar objetos.

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

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

5.49. Deve ser capaz de realizar DHCP relay.

5.50. Deve possuir relatórios das aplicações, com pelos menos os seguintes gráficos:

5.50.1. Tempo de resposta da aplicação;

5.50.2. Latência;

5.50.3. Conexões para conjunto de servidores, servidores individuais;

5.50.4. Por URL.

5.51. A ferramenta de relatórios deve possuir pelo menos os seguintes filtros para a geração dos gráficos:

5.51.1. Servidores virtuais;

5.51.2. Servidores balanceados;

5.51.3. URLs;

5.51.4. Países de origem, baseados em geolocalização (GEOIP);

5.51.5. Dispositivos de origem do cliente (user agent).

5.52. Deve possuir framework unificado para configuração da aplicação.

5.53. Deve possuir criptografia IPSEC para comunicação entre os balanceadores.

5.54. Quando licenciada, a solução deve ter a capacidade de realizar cache transparente das respostas DNS.

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

5.56. A Solução deve ter suporte a sFlow.

5.57. A solução deve possuir múltiplos domínios de roteamento em IPv4 e IPv6.

5.58. A solução deve permitir que cada domínio de roteamento utilize BGP, OSPF e RIP em IPv4 e IPv6.

5.59. A solução deve suportar Equal Cost Multipath (ECMP).

5.60. A solução deve realizar Bidirectional Forward Detection (BFD).

5.61. A solução deve ter suporte a Stream Control Transmission Protocol (SCTP).

5.62. Deve ter suporte a Transport Layer Security (TLS) Server Name Indication (SNI).

5.63. A solução deve possuir monitor HTTP/HTTPS com autenticação NTLM embutida, que permita verificar se o HTTP/HTTPS está operando assim como a plataforma de autenticação.

- 5.64. Suportar diversas cifras e protocolos SSL/TLS, incluindo TLS 1, 1.1, 1.2, 1.3, Forward Secrecy/Perfect Forward Secrecy, RSA, ECDSA, DHE, ECDHE, AES-128, AES-256, CBC/GCM, Camellia128, Camellia256, SHA, SHA2(SHA256/384) e Chacha20-Poly1305;
- 5.65. A solução deve ter suporte a criptografia Perfect Forward Secrecy não apenas para troca de chaves RSA.
- 5.66. A solução deve ser capaz de colocar em fila as requisições TCP que excedam a capacidade de conexões do grupo de servidores ou de um servidor. O balanceador não deverá descartar as conexões que excedam o número de conexões do servidor ou do grupo de servidores:
- 5.66.1. Deve ser possível configurar o tamanho máximo da fila;
- 5.66.2. Deve ser possível configurar o tempo máximo de permanência na fila.
- 5.67. A solução deve realizar Controle de Banda Estático para grupos de aplicações e rede.
- 5.68. A solução deve realizar Controle de Banda Dinâmico por aplicação e usuário.
- 5.69. A solução deve realizar Controle de Banda baseado em domínio de roteamento.
- 5.70. Permitir tráfego por parâmetros de QoS (Quality of Service) ou rate-shaping, com pelo menos 2 (duas) filas para priorização de tráfego baseada na camada de aplicação. Através dessa priorização de tráfego e restrição de largura de banda deverá ser possível permitir um melhor nível de serviço para clientes preferenciais em detrimento dos demais clientes. A solução deve permitir a priorização de tráfego de entrada para determinadas aplicações.
- 5.71. A solução deve permitir a criação de túneis IP por domínio de roteamento utilizando GRE, IPIP, EtherIP, PPP.
- 5.72. A solução deve permitir a criação de túneis IP transparente utilizando GRE e IPIP.
- 5.73. Deve fornecer recursos para o uso de servidores (reals) no mesmo Virtual Server.
- 5.74. Possuir suporte ao protocolo SPDY e HTTP 2.0.
- 5.75. O equipamento deve possuir suporte ao espelhamento de conexões FTP, Telnet, HTTP, UDP, SSL.
- 5.76. O equipamento deverá permitir a sincronização das configurações:
- 5.76.1. De forma automática;
- 5.76.2. Manualmente, forçando a sincronização apenas no momento desejado.
- 5.77. Permitir a configuração das interfaces de alta disponibilidade do cluster (heartbeat), com opções para:

5.77.1. Compartilhar a rede de heartbeat com a rede de dados; e

5.77.2. Utilizar uma rede exclusiva para o heartbeat.

5.78. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra-ataques.

5.79. A solução deve possuir linguagem de programação open-source que permita a manipulação do tráfego de entrada e saída, viabilizando assim a alteração de parâmetros no cabeçalho e no corpo das mensagens.

5.80. Essa linguagem de programação deve permitir a importação de pacotes, garantindo assim que a agilidade e flexibilidade no compartilhamento dos scripts.

5.81. Permitir a criação de políticas através de interface gráfica web para manipulação de tráfego através de lógica para pelo menos os seguintes operadores:

5.81.1. GEOIP, http-basic-auth, http-cookie, http-header, http-host, http-method, http-referer, http-setcookie, http-status, http-uri e http-version.

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

5.82.1. Bloqueio de tráfego;

5.82.2. Reescrita e manipulação de URL;

5.82.3. Registro de tráfego (log);

5.82.4. Adição de informação no cabeçalho HTTP;

5.82.5. Redirecionamento do tráfego para um membro específico;

5.82.6. Selecionar uma política específica para Aplicação Web.

5.83. A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:

5.83.1. Endereço IP de origem.

5.84. A solução deverá ser capaz de fazer log de todas as sessões, onde os registros deverão conter:

5.84.1. Endereço IP de origem;

5.84.2. Porta TCP ou UDP de origem;

5.84.3. Endereço IP de destino;

5.84.4. Porta TCP ou UDP de destino;

5.84.5. Protocolo de camada 4 (TCP ou UDP);

5.84.6. Data e hora da mensagem;

5.84.7. URL acessada.

5.85. A solução deve possuir políticas de uso de senhas administrativas tais como: nível de complexidade, período de validade e travamento de conta devido a erros múltiplos de login de forma nativa ou no mínimo integrado a uma base Active Directory.

5.86. A solução deve suportar controle de versão da política de configuração de forma a permitir fazer roll back de políticas aplicadas.

5.87. A solução deve ser capaz de analisar a performance de aplicações web.

5.88. A solução deve possuir relatórios das aplicações.

5.89. Deve prover métricas de aplicações como: Transações por Segundo; Tempo de latência do cliente e servidor; Throughput de requisição e resposta; Sessões.

5.90. A solução deverá gerar informações para permitir análises históricas e auxiliar nos processos de manutenções preventivas, de troubleshooting, de planejamento de capacidade e de análise da experiência dos usuários finais no acesso das aplicações.

5.91. As informações coletadas deverão permitir a análise dos dados por aplicações, por URL's, por clientes e por servidores, permitindo assim a identificação mais precisa dos eventuais ofensores do tráfego suportado pela solução.

5.92. A solução deverá gerar informações estatísticas de acesso identificando para cada aplicação os métodos de acesso HTTP (GET e Post), o tipo de sistema operacional utilizado pelos clientes, e os browsers utilizados.

5.93. A geração de informações históricas deverá permitir:

5.93.1. O detalhamento do tempo de resposta total de carregamento de uma URL e ou Página;

5.94. Permitir a correlação de métricas de uso de rede com o comportamento das aplicações.

6. PROTEÇÃO CONTRA-ATAQUES DE APLICAÇÃO

6.1. A solução deve operar nos modos ativo-ativo e ativo-standby.

6.2. O equipamento oferecido deverá proteger a infra-estrutura web de ataques contra a camada de aplicação (Camada 7).

- 6.3. Deve possuir tecnologia para mitigação de DDoS em camada 7 baseado em análise comportamental, usando o aprendizado.
- 6.4. Não deve haver a necessidade de intervenção de usuário para configurar thresholds DoS, pois esses valores devem ser auto-ajustáveis e adaptativos de acordo com mudanças.
- 6.5. A solução deve possuir a capacidade de automaticamente capturar tráfego no formato TCP Dump relativos a ataques DoS L7, Web Scraping e força bruta permitindo uma análise mais aprofundada por parte do administrador.
- 6.6. A solução deve suportar o uso de firewall camada 3-4 junto com firewall camada 7 no mesmo equipamento/appliance para evitar problemas com o aumento da latência.
- 6.7. O equipamento oferecido deverá possuir a certificação ICSA para Firewall de Aplicação (Web Application Firewall).
- 6.8. Permitir a utilização de um modelo positivo de segurança para proteger contra-ataques conhecidos aos protocolos HTTP e HTTPS e às aplicações web acessíveis através destes.
- 6.9. Possuir política de segurança de aplicações web pré-configurada na solução.
- 6.10. Permitir a criação de novas regras com parâmetros e expressões regulares definidos pelo administrador.
- 6.11. Permitir a criação de políticas diferenciadas por aplicação e por URL, onde cada aplicação e URL poderão ter políticas totalmente diferentes.
- 6.12. Permitir a criação de políticas diferenciadas por aplicação.
- 6.13. Permite configurar de forma granular, por aplicação protegida, restrições de métodos HTTP permitidos, tipos ou versões de protocolos, tipos de caracteres e versões utilizadas de cookies.
- 6.14. A solução WAF deve, no mínimo, funcionar como proxy reverso de aplicações.
- 6.15. A solução WAF deve, no mínimo, permitir o mapeamento de diversas aplicações em um mesmo IP virtual, enviando informações para conjuntos de servidores diferentes de acordo com a URL requisitada.
- 6.16. A solução WAF deve, no mínimo, permitir o mapeamento em um mesmo IP virtual, de acordo com a URL requisitada, que exija certificado digital de cliente para algumas aplicações e não exija para outras.
- 6.17. A solução WAF deve, no mínimo, permitir a inclusão de parâmetros customizados nos cabeçalhos (headers) HTTP, além da alteração dos existentes, para envio à aplicação de destino.

- 6.18. A solução deverá se integrar a soluções de análise (Scanner) de vulnerabilidade do site. O resultado desta análise deve ser utilizado para configurar as políticas do equipamento.
- 6.19. A solução deve permitir a integração com soluções de análise de vulnerabilidades (Scanner) de terceiros.
- 6.20. A solução deve permitir a inspeção de upload de arquivos para os servidores de aplicação. Essa inspeção pode ser feita via integração ICAP. Deve ser possível integrar com diferentes softwares de Antivírus.
- 6.21. Deve se integrar com o software de Antivírus existente no ambiente da CONTRATANTE.
- 6.22. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar e aumentar a proteção contra-ataques recentes.
- 6.23. Permitir a integração com Firewall de Database de outros fabricantes.
- 6.24. A solução deve se integrar com outras soluções de segurança e análise de logs de outros fabricantes.
- 6.25. Deve possuir tecnologia de detecção de anomalias baseado nos IDs dos dispositivos, permitindo a detecção de DoS, ataques de força bruta e ataques de sequestro de sessão. Deve ser possível filtrar relatórios por IDs de dispositivos.
- 6.26. A solução deve permitir incluir em blacklist os endereços IPs que repetidamente falharem a desafios no browser. Portanto o sistema não precisa usar recursos para mitigar tráfego enviado por esses endereços Ips. Ao entrar em Blacklist o sistema automaticamente bloqueia os pacotes enviados por esse endereço por um período de tempo.
- 6.27. A solução deve suportar e fazer a proteção do tráfego em cima de protocolo WebSocket.
- 6.28. A solução deve possibilitar o uso de múltiplas formas de logging remoto ao mesmo tempo para a mesma aplicação. Portanto dever ser possível por exemplo logar os requests válidos num servidor de SIEM e os requests inválidos em outro servidor de SIEM de outra marca e modelo.
- 6.29. A solução deverá possuir funcionalidade de proteção positiva e segura contra-ataques, como:
- 6.29.1. Acesso por Força Bruta;
 - 6.29.2. Ameaças Web AJAX/JSON;
 - 6.29.3. DoS e DDoS camada 7;
 - 6.29.4. Buffer Overflow;
 - 6.29.5. Cross Site Request Forgery (CSRF);
 - 6.29.6. Cross-Site Scripting (XSS);

- 6.29.7. SQL Injection;
- 6.29.8. Cookie e Command Injection;
- 6.29.9. Code Injection.
- 6.29.10. Parameter tampering;
- 6.29.11. Cookie poisoning;
- 6.29.12. HTTP Request Smuggling;
- 6.29.13. Manipulação de campos escondidos;
- 6.29.14. Manipulação de cookies;
- 6.29.15. Roubo de sessão através de manipulação de cookies;
- 6.29.16. Sequestro de sessão;
- 6.29.17. Força bruta no browser;
- 6.29.18. XML bombs/DoS;
- 6.29.19. Checagem de consistência de formulários;
- 6.29.20. Checagem do cabeçalho do “user-agent” para identificar clientes inválidos.
- 6.30. A solução deve suportar o uso de páginas de login AJAX/JSON tanto com configuração manual como descoberta automática.
- 6.31. Deverá ser capaz de identificar e bloquear ataques através de:
 - 6.31.1. Regras de verificação personalizadas – política de segurança configurada;
 - 6.31.2. Assinaturas, com atualização periódica da base pelo fabricante;
 - 6.31.3. As assinaturas devem ser atualizadas durante o período do contrato sem que seja necessário nenhum custo a mais por parte da CONTRATANTE na aquisição de novas licenças ou subscrições. Deve fazer parte da solução de WAF ofertada;
 - 6.31.4. Ausência de tratamento de erros pela aplicação.
- 6.32. Prevenir contra vazamento de dados sensíveis (mensagens de erro HTTP, códigos das aplicações, entre outros) dos servidores de aplicação, retirando os dados ou mascarando a informação nas páginas enviadas aos usuários.

- 6.33. Permitir a customização da resposta de bloqueio.
- 6.34. Permitir a liberação temporária ou definitiva (white-list) de endereços IP bloqueados por terem originados ataques detectados pela solução.
- 6.35. Deve permitir limitar o número de conexões e requisições por IP de origem para cada endereço IP Virtual.
- 6.36. Deve permitir adicionar, automaticamente e manualmente, em uma lista de bloqueio, os endereços IP de origem que ultrapassarem o limite estabelecido, por um período de tempo determinado através de configuração.
- 6.37. Deve permitir criar lista de exceção (white list) por endereço IP específico ou faixa de sub-rede.
- 6.38. A solução deve suportar o modelo de segurança positiva definido pelo OWASP, pelo menos o que consta no TOP 10.
- 6.39. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle.
- 6.40. Deverá implantar, no mínimo, as seguintes funcionalidades:
- 6.40.1. Proteção contra Buffer Overflow;
 - 6.40.2. Checagem de URL;
 - 6.40.3. Checagem de métodos HTTP utilizados (GET, POST, HEAD, OPTIONS, PUT, TRACE, DELETE, CONNECT);
 - 6.40.4. Proteção contra envios de comandos SQL escondidos nas requisições enviadas a bases de dados (SQL Injection);
 - 6.40.5. Proteção contra Cross-site Scripting;
 - 6.40.6. Funcionalidade de Cookie Encryption;
 - 6.40.7. Checagem de consistência de formulários;
 - 6.41.8. Checagem do cabeçalho “user-agent” para identificar clientes inválido.
- 6.41. Implementar as seguintes funcionalidades:
- 6.41.1. Cloaking – Proteção contra exposição de informações do ambiente e servidores internos como:
 - 6.41.1.1. Sistema operacional e servidor web com impressão digital.

- 6.41.2. Esconder qualquer mensagem de erro HTTP dos usuários;
- 6.41.3. Remover as mensagens de erro às páginas que serão enviadas aos usuários;
- 6.41.4. Permitir a utilização de uma página HTML informativa e personalizável como HTTP Response aos bloqueios.
- 6.42. Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro Xforwarded-for (XFF).
- 6.43. Deve suportar a criação de políticas por geo-localização, permitindo que o tráfego de determinado (s) País/Países seja (m) bloqueado (s).
- 6.44. Possuir mecanismo de aprendizado automático capaz de identificar todos os conteúdos das aplicações, incluindo URLs, parâmetros URLs, campos de formulários, o que se espera de cada campo (tipo de dado, tamanho de caracteres), cookies, arquivos XML e elementos XML.
- 6.45. O equipamento oferecido deverá possuir uma funcionalidade de criação automática de políticas, onde a política de segurança é criada e atualizada automaticamente baseando-se no tráfego real observado à aplicação.
- 6.46. O perfil aprendido de forma automatizada pode ser ajustado, editado ou bloqueado.
- 6.47. O equipamento oferecido deverá possuir proteção baseada em assinaturas para prover proteção contra-ataques conhecidos. Deverá ser possível desabilitar algumas assinaturas específicas em determinados parâmetros, como uma exceção à regra geral.
- 6.48. A atualizações de assinaturas deverão passar por um período configurável de testes, onde nenhuma requisição que viole a assinatura será bloqueada, apenas informada no relatório. Este processo deve ser automatizado, não sendo necessário criar regras específicas a cada atualização de assinatura.
- 6.49. O equipamento oferecido deverá permitir o bloqueio de ataques DoS na camada 7, possuindo também a opção de apenas registrar o ataque, sem tomar nenhuma ação de bloqueio.
- 6.50.1. O equipamento oferecido deverá possuir as seguintes formas de detecção de ataques DoS na camada de aplicação:
- 6.50.1.1. Número de requisições por segundo enviados a uma URL específica;
- 6.50.1.2. Número de requisições por segundo enviados de um IP específico;
- 6.50.1.3. Detecção através de código executado no cliente com o objetivo de detectar interação humana ou comportamento de robôs (bots);
- 6.50.1.4. Número máximo de transações por segundo (TPS) de um determinado IP;

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

6.50.1.6. Aumento do stress do servidor de aplicação.

6.51. O equipamento oferecido deverá permitir o bloqueio de ataques de força bruta de usuário/senha em páginas de acesso (login) que protegem áreas restritas. Este bloqueio deve limitar o número máximo de tentativas e o tempo do bloqueio deverá ser configurável.

6.52. O equipamento oferecido deverá permitir o bloqueio de determinados endereços IPs que ultrapassem um número máximo de violações por minuto. O período de bloqueio deverá ser configurável e durante este período todas as requisições do cliente serão bloqueadas automaticamente.

6.53. O equipamento oferecido deverá permitir o bloqueio de robôs (bots) que acessam a aplicação através de detecção automática, não dependendo de cadastros manuais. Robôs conhecidos do mercado, como Google, Yahoo e Microsoft Bing deverão ser liberados por padrão.

6.54. O equipamento oferecido deverá permitir o cadastro de robôs que podem acessar a aplicação.

6.55. Possuir política de segurança de aplicações pré-configuradas no equipamento para pelo menos as seguintes aplicações:

6.55.1. Microsoft ActiveSync v1.0, v2.0;

6.55.2. Microsoft OWA in Exchange 2003, 2007, 2010 e as versões mais recentes;

6.55.3. Microsoft SharePoint 2010 e as versões mais recentes;

6.55.4. Oracle 10g Portal;

6.55.5. Oracle Application 11i;

6.55.6. Oracle PeopleSoft Portal.

6.56. O equipamento oferecido deverá implementar proteção ao JSON (JavaScript Object Notation).

6.57. Possuir firewall XML integrado – suporte a filtro e validação de funções XML específicas da aplicação.

6.58. Implementar a segurança de web services, através dos seguintes métodos:

6.58.1. Criptografar/Decriptografar partes das mensagens SOAP;

- 6.58.2. Assinar digitalmente partes das mensagens SOAP;
- 6.58.3. Verificação de partes das mensagens SOAP.
- 6.59. Prevenir o vazamento de informações, permitindo o bloqueio ou a remoção dos dados confidenciais.
- 6.60. Prevenir que erros de aplicação ou infra-estrutura sejam mostrados ao usuário.
- 6.61. Deverá ter integração, via ICAP, com servidor de anti-vírus para verificação dos arquivos a serem carregados nos servidores.
- 6.62. Permitir o uso do parâmetro HTTP X-Forwarded-For como parte da política de controle.
- 6.63. Deverá proteger o protocolo FTP com pelo menos os seguintes métodos:
 - 6.63.1. Determinar os comandos FTP permitidos;
 - 6.63.2. Requests FTP anônimos;
 - 6.63.3. Checar compliance com o protocolo FTP;
 - 6.63.4. Proteger contra-ataques de força bruta nos logins.
- 6.64. Deverá proteger o protocolo SMTP com pelo menos os seguintes métodos:
 - 6.64.1. A comunicação deve ser aderente a RFC 2821;
 - 6.64.2. Limitar o número de mensagens;
 - 6.64.3. Validar registro SPF do DNS;
 - 6.64.4. Determinar quais métodos SMTP podem ser utilizados.
- 6.65. Deverá armazenar os logs localmente ou exportar para Syslog server.
- 6.66. Deverá proteger contra ataques CSRF (Cross-Site Request Forgery), podendo ser possível especificar quais URLs serão examinadas.
- 6.67. Deverá possuir controle de fluxo por aplicação permitindo definir o fluxo de acesso de uma URL para outra da mesma aplicação. Dessa forma qualquer tentativa de acesso a um determinado site que não siga o fluxo passando pelas URLs pré-definidas deverá ser bloqueado como uma tentativa de acesso ilegal.
- 6.68. A solução deve fornecer relatórios consolidados de ataques com pelo menos os seguintes dados: Resumo geral com as políticas ativas, anomalias e estatísticas de tráfego, Ataques DoS, Ataques de Força Bruta, Ataques de Robôs, Violações, URL, Endereços IP, Países, Severidade e PCI Compliance.

- 6.69. Deverá permitir o agendamento de relatórios a serem entregues por email.
- 6.70. Fornecer os seguintes Gráficos de alertas por:
- 6.70.1. Política de segurança;
 - 6.70.2. Tipos de ataques;
 - 6.70.3. Violações;
 - 6.70.4. URL;
 - 6.70.5. Endereços IP;
 - 6.70.6. Países;
 - 6.70.7. Severidade;
 - 6.70.8. Código de resposta;
 - 6.70.9. Métodos;
 - 6.70.10. Protocolos;
 - 6.70.11. Vírus;
 - 6.70.12. Usuário;
 - 6.70.13. Sessão.
- 6.71. Deverá exportar as requisições que contém os ataques, pelo menos nos formatos PDF e binário.
- 6.72. Deve possuir relatório em tempo real sobre ataques DoS L7, atualizado automaticamente.
- 6.73. A solução deve mostrar o impacto de ataques DoS L7 na performance e memória do servidor.
- 6.74. Os logs devem indicar o momento de início e final de um ataque DoS L7.
- 6.75. Possuir método de mitigação de DoS L7 baseado em: CAPTCHA; Descarte de todas as requisições de um determinado IP e/ou país suspeito; Geolocalização, incluindo a prevenção com CAPTCHA para países suspeitos que ultrapassem os thresholds; Defesa proativa contra Bot, através da injeção de um desafio JavaScript para detectar se é um usuário legítimo ou robô.
- 6.76. A solução deve permitir que ao detectar um falso positivo, o administrador aceite a requisição e atualize a política automaticamente.

- 6.77. A solução ao se integrar com um Scanner de vulnerabilidade deve mostrar quais a vulnerabilidades podem ser resolvidas automaticamente (pela própria solução de WAF) e quais podem ser resolvidas manualmente, pelo próprio administrador. No caso de resolução manual, deve ainda mostrar um guia com os passos necessários para resolver aquela vulnerabilidade, inclusive com a avisos de possíveis consequências na aplicação Web.
- 6.78. A solução deve classificar o nível de violação de uma requisição, possuindo pelo menos 5 níveis, onde o nível 5 é referente a violação mais grave e, portanto, deve ter prioridade.
- 6.79. A solução deve possuir proteção de DDoS L7 baseado em análise comportamental, sem precisar de nenhuma configuração manual.
- 6.80. Suportar os protocolos HTTP/1.0, HTTP/1.1 e HTTP/2.0.
- 6.81. Suportar codificação HTML "application/x-www-form-urlencoded".
- 6.82. Suportar Cookies v0 e v1.
- 6.83. Suportar codificação fragmentada (chunked encoding) em requisições e respostas.
- 6.84. Suportar compressão de requisições e respostas.
- 6.85. Suportar validação de protocolo, como:
- 6.85.1. Possibilidade de restringir uso de métodos;
 - 6.85.2. Possibilidade de restringir protocolos e versões de protocolos;
 - 6.85.3. Strict (per-RFC) Request Validation;
 - 6.85.4. Validar caracteres URL-encoded; e
 - 6.85.5. Validação de codificação fora de padrão %uXXYY.
- 6.86. Suportar restrições de HTML, como:
- 6.86.1. Tamanho do nome de parâmetros;
 - 6.86.2. Tamanho dos valores de parâmetros; e
 - 6.86.3. Combinação de tamanho de parâmetros (nome e valores).
- 6.87. Suportar POST no upload de arquivo.
- 6.88. Permitir configurar ou oferecer restrições para tamanho individual de arquivo.

- 6.89. Permitir customizar a lógica na inspeção de upload de arquivos.
- 6.90. Suporte para os métodos Basic, Digest e NTLM para autenticação.
- 6.91. Suporte para autenticação por back end tipo LDAP e Microsoft Active Directory.
- 6.92. Capacidade de filtrar cabeçalhos, corpo e status de respostas.
- 6.93. Suportar as seguintes técnicas de detecção:
 - 6.93.1. URL-decoding;
 - 6.93.2. Terminação Null Byte String;
 - 6.93.3. Paths auto-referenciados;
 - 6.93.4. Case de caracteres misturados;
 - 6.93.5. Uso excessivo de espaços em branco;
 - 6.93.6. Remoção de comentários;
 - 6.93.7. Decodificação de entidades HTML; e
 - 6.93.8. Caracteres de escape.
- 6.94. Possuir registro de logs com as seguintes características:
 - 6.94.1. Em cada registro de log de acesso deve ser inserido um identificador de transação HTTP que deve ser único, envolvendo par requisição/resposta;
 - 6.94.2. Os registros de log de acesso e eventos devem ser armazenados em arquivo ou em banco de dados que permita a exportação ou em outro formato aberto como CSV ou TXT, podendo ainda serem armazenados localmente ou carregados (upload) em servidor de log via FTP ou SCP ou armazenados em servidor externo de banco de dados;
 - 6.94.3. Permitir configurar a retenção dos logs por tempo e volume; e
 - 6.94.4. Ter capacidade para detecção, remoção ou codificação de dados sensíveis do log.
- 6.95. A solução deverá gerar relatórios com as seguintes características:
 - 6.95.1. Permitir a filtragem por data ou hora, endereço IP e tipo de incidente;
 - 6.95.2. Permitir a geração de relatórios sob demanda ou pré-programados periodicamente (diário e semanal); e
 - 6.95.3. Permitir a geração de relatórios em formatos PDF/A (versão aberta) e HTML.

6.96. Possuir as seguintes características de gerenciamento:

6.96.1. Facilidade para liberação de regras aprendidas automaticamente que estejam gerando grande quantidade de falso positivo;

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

6.96.3. Facilidade para aplicar diferentes regras para diversas aplicações;

6.96.4. Capacidade para customizar regras de negação de serviço;

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

6.96.6. Capacidade para desfazer a aplicação de uma regra.

6.97. Possuir mecanismos que garantam a capacidade de gerenciamento do equipamento sob condições de alto tráfego.

6.98. A solução deve apresentar perfil de aprendizagem automática com:

6.98.1. Capacidade de aprendizagem automática sem intervenção humana; e

6.98.2. Capacidade de inspeção das regras criadas automaticamente.

6.99. Permitir o gerenciamento da configuração com as seguintes características:

6.99.1. Gerenciamento por autenticação dos usuários e as autorizações baseadas em perfis (roles); e

6.99.2. Capacidade de gerenciamento remoto dos equipamentos.

6.100. Apresentar logs e relatórios administrativos com as seguintes características:

6.100.1. Capacidade para identificar e notificar falhas do sistema ou perda de performance;

6.100.2. Capacidade de agregação de informações para simplificar a revisão das atividades do dispositivo; e

6.100.3. Capacidade para gerar estatísticas de serviço e sistema.

6.101. Possuir suporte a XML:

6.101.1. Para proteção de WebServices;

6.101.2. Em conformidade com a especificação WS-I básico; e

6.101.3. Com capacidade de restringir métodos do WebService via definição em WSDL.

6.102. Suportar funções de camuflagem (cloaking), como:

6.102.1. Esconder qualquer mensagem de erro http dos usuários; e

6.102.2. Remover as mensagens de erro das páginas que serão enviadas aos usuários.

6.103. Proteger a aplicação Web contra robôs sofisticados através da combinação de desafios enviados ao browser do usuário e técnicas avançadas de análise comportamental.

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

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

6.106. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego com o stress do servidor de aplicação para determinar uma condição de DDoS.

6.107. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação.

6.108. Deve possuir uma proteção proativa contra-ataques automatizados por robôs e outras ferramentas de ataque.

6.109. Deve proteger informações sensíveis e confidenciais da interceptação por terceiros, através da criptografia de dados quando ainda no browser do usuário.

6.110. Deve proteger esses dados criptografados de malwares e keyloggers.

6.111. Deve suportar a criptografia de sessões HTTP desde o browser do usuário, provendo proteção contra interceptação por terceiros e evitando ataques do tipo Man in the Browser e Keyloggers.

6.112. Deve possuir proteção contra-ataques DDoS, através da análise de comportamento de tráfego usando técnicas de análise de dados e Machine Learning.

6.113. Através da análise contínua de carga e monitoração de saúde de servidores, deve ser possível identificar anomalias e mitigá-las.

6.114. Deve ajudar a prevenir contra-ataques de Credential Stuffing, onde bases de credenciais expostas na Internet são usados para tentativa de acesso de outras aplicações Web.

6.115. A solução deve possuir lista dinâmica de endereços IP globais com atividades maliciosas:

6.116. Deve ser possível verificar o endereço de origem do pacote IP no cabeçalho IP e no parâmetro Xforwarded-for (XFF).

6.117. Deve possuir, pelo menos, as seguintes categorias de endereços IP: Windows Exploits, Web Attacks, Botnets, Scanners, Denial of Service, Reputation, Phishing Proxy, Anonymous Proxy.

6.118. Possuir linguagem de script que possibilite a interação com o payload das requisições e inclusive alterações.

7. DNS

7.1. A solução deve operar em, no mínimo, a seguintes formas:

7.1.1. DNS autoritativo;

7.1.2. DNS secundário;

7.1.3. DNS resolver;

7.1.4. DNS cache;

7.1.5. Balanceamento de DNS servers.

7.1.6. DNSSec;

7.1.7. A solução deve ser capaz de realizar transferência de zonas para múltiplos servidores DNS Primários responsáveis por diferentes zonas;

7.1.8. Capacidade de uso de chave criptográfica TSIG para comunicação segura entre servidores DNS, obedecendo no mínimo os padrões: HMAC MD5, HMAC SHA-1 ou HMAC SHA-256;

7.1.9. A solução deve realizar o offload dos servidores de DNS, funcionando como o DNS secundário;

7.1.10. A solução deve servir as respostas as requisições onde o DNS é o autoritativo a partir da memória RAM;

7.1.11. A solução deve possuir certificação ICASA.

7.2. A solução deve possuir proteções contra-ataques DNS, no mínimo:

7.2.1. Inspeção de protocolo;

7.2.2. Validação de protocolo.

7.2.3. UDP flood;

7.2.4. Pacotes mal formados;

7.2.5. Ataque Teardrop;

7.2.6. Ataque ICMP;

7.2.7. Permitir que regras customizadas em linguagem aberta possam ser utilizadas para customizar a distribuição dinâmica de tráfego e aumentar a proteção contra-ataques.

7.3. A solução deve ser capaz de realizar balanceamento dos servidores DNS.

7.4. A solução deve ser capaz de realizar filtragem de pacotes.

7.5. A solução deve prover segurança do protocolo DNS, protegendo contra-ataques de negação de serviço, NXDOMAIN e reflexão e amplificação de DNS.

7.6. A solução deve prover segurança do protocolo DNS, protegendo contra-ataques de Cache Poisoning.

7.7. A solução deve realizar stateful inspection.

7.8. A solução deve possuir base de Geolocalização IP.

7.9. A solução deve implementar DNS64.

7.10. A solução deve suportar pelo menos os seguintes tipos de requisição DNS: SOA, A, AAAA, CNAME, DNAME, HINFO, MX, NS, PTR, SRV, TXT.

7.11. Deve ser capaz de gerar estatísticas sobre consultas de DNS por: Aplicação, nome da query, tipo da query, endereço IP do cliente.

7.12. Deve ser possível configurar a solução de modo inline a estrutura de DNS existente e transparente sem requerer grandes mudanças na infraestrutura.

7.13. Deve prover as respostas a queries DNS da própria RAM CACHE.

7.14. A solução deve ser capaz de realizar IP Anycast.

7.15. A solução deve ser capaz de realizar DNSSec, independente da estrutura dos servidores DNS em uso.

7.16. A solução de alta disponibilidade não deve depender de BGP ou outro protocolo de roteamento.

7.17. A solução de alta disponibilidade será realizada baseada em respostas a requisições DNS. A resposta a requisições DNS devem conter apenas endereços que estejam disponíveis no momento, e balanceadas por usuário, de acordo com as políticas definidas.

7.18. A solução deverá aceitar resolução de nomes baseada em topologia, onde requisições de DNS são respondidas baseado no país, continente, ou endereço IP de onde veio a requisição.

7.19. Deve ser possível ajustar quantos endereços são enviados em uma única resposta.

7.20. Suporte a monitoração de estado de saúde de servidores, serviços e links de conexão a provedor de serviço, garantindo a disponibilidade do serviço oferecido.

7.21. Suportar pelo menos os seguintes algoritmos de balanceamento:

7.21.1. Round Robin;

7.21.2. Global Availability;

7.21.3. Ratio;

7.21.4. LDNS Persist;

7.21.5. Geografia;

7.21.6. Disponibilidade da Aplicação;

7.21.7. Capacidade do Virtual Server;

7.21.8. Least Connections;

7.21.9. Pacotes por segundo;

7.21.10. Round trip time;

7.21.11. Hops;

7.21.12. Packet Completion Rate;

7.21.13. QoS definido pelo usuário;

7.21.14. Kilobytes per Second.

7.22. Implementar persistência da conexão do usuário entre aplicações ou data centers.

7.23. A solução deverá suportar o controle de grupos de aplicações, e permitir que um usuário seja redirecionado para outro datacenter quando houver falha em qualquer das aplicações de um mesmo grupo.

- 7.24. A solução deverá permitir que as políticas sejam configuradas individualmente por aplicação sendo balanceada.
- 7.25. A solução deverá permitir que a contingência seja automática, mas que o retorno seja manual.
- 7.26. A solução deve ser capaz de lidar com clientes IPv6 quando o site atende apenas com IPv4 (requests AAAA ou A6).
- 7.27. Possuir suporte a IPv6 no balanceamento global entre datacenters.
- 7.28. Ter capacidade de tratar informações das camadas L4-L7 (FTP, SMTP, URL, HTTP Header, TCP e UDP) para a tomada de decisão de encaminhamento a servidor real, em IPv4 e IPv6.
- 7.29. Deverá possuir a funcionalidade de resposta rápida a queries DNS, permitindo respostas mais rápidas para zonas que seja autoritativo.
- 7.30. A solução deve possuir suporte a Response Policy Zones (RPZ), mecanismo de firewall usado por DNS recursivo para permitir o tratamento customizado da resolução de nomes. Portanto a solução deve ser capaz de filtrar queries DNS para domínios considerados maliciosos e retornar respostas customizadas.
- 7.31. A solução deve suportar edns-client-subnet (ECS) para tanto responder requisições de clientes (Balanceamento de Carga Global de Servidores) ou encaminhar requisições de clientes (screening).
- 7.32. Baseado no ECS DNS deve ser possível preservar o endereço IP da subnet do cliente ao invés do LDNS para tomar decisões.
- 7.33. A solução deve funcionar pelo menos das seguintes formas:
- 7.33.1. Usar o ECS para tomar decisões de Balanceamento de Carga Global de Servidores baseado em topologia (Subnets);
- 7.33.2. Injetar o ECS (proxy requests) para outros servidores DNS.
- 7.34. A solução deve fazer persistência baseado no endereço IP do cliente (ECS), significando que se o cliente mudar de LDNS resolver (suporte ECS), o Balanceamento de Carga Global de Servidores deve usar a persistência existente para manter o cliente no mesmo Datacenter.
- 7.35. O serviço deverá ser implementado sobre uma infraestrutura de hardware e software dedicada ou em conjunto com equipamento Anti-DDoS. O hardware empregado deverá ser do tipo appliance, específico para operar softwares de DNS Firewall. O software e o hardware empregados deverão corresponder a uma solução de notória eficácia já em uso no mercado nacional. O serviço deve ter suporte a IPv6, registros AAAA e zonas reversas IPv6.
- 7.36. Infraestrutura de hardware e software destinada à função de resolução de nomes DNS de uso exclusivo da CONTRATANTE.

7.37. O serviço deve ter a habilidade de detectar, monitorar, controlar e mitigar ataques baseados em DNS sem gerar nenhum impacto ao tráfego válido de DNS.

7.38. A solução deverá ter serviço de resolução de nomes destinado a armazenar, de forma “autoritativa”, as zonas do CONTRATANTE e o IP reverso do bloco CIDR do CONTRATANTE.

7.39. Os equipamentos que atenderão ao serviço deverão ser estruturados de forma redundante, permitindo o failover completo na ocorrência de falhas, suportando, no mínimo, o modo de operação ativo-ativo. Um nó deverá suportar sozinho todos os requisitos de performance solicitados neste projeto.

7.40. Para o devido dimensionamento do serviço cada equipamento isolado deve possuir desempenho DNS de pelo menos 50.000 QPS (50 mil Queries Per Second – Consultas Por Segundo).

7.41. O serviço deverá possuir capacidade para resolver consultas para as quais não tem autoridade (ou seja, da zona “.”, tipo “hint”), com a finalidade de atender somente às consultas DNS oriundas da rede interna do CONTRATANTE, bem como dos demais Serviços Gerenciados de Segurança e servidores instalados no Data Center.

7.42. O serviço deve ter, pelo menos, as seguintes características de segurança:

7.43. Deve permitir o uso de lista negra para bloquear domínios DNS.

7.44. Deve possuir capacidade de criação de ACLs para bloqueio de domínios e redes maliciosas.

7.45. Prover uma linha de defesa para bloquear tentativas de acesso a sites maliciosos impedindo a resolução de nomes de domínio que hospedem tais conteúdos maliciosos minimizando possíveis infecções de Malware, Trojan, Spyware, Ransomware e softwares de comando e controle (BotNet).

7.46. Registrar todas as tentativas de comunicação com os nomes de domínio que hospedem conteúdo malicioso. Estes registros devem conter: IP de origem, destino, data e hora do acesso.

7.47. Deve suportar no mínimo os seguintes métodos de controle: apenas logar, bloquear o dado ou substituir o nome do domínio.

7.48. A solução deverá suportar mecanismo de “assinaturas”, ou técnicas semelhantes, que permitam ao fabricante disponibilizar regras de bloqueios contra novos ataques conforme surgimento.

7.49. O serviço deverá permitir que o administrador crie regras customizadas de bloqueio, da seguinte maneira:

7.49.1. Bloqueio de nomes de domínio totalmente qualificados em consultas de DNS feitas via TCP ou UDP;

7.49.2. Bloqueio de endereços de origem IPv4 ou IPv6 em consultas realizadas via TCP ou UDP. Esta regra deverá permitir a configuração de endereços de hosts ou de redes.

7.50. Configuração de limites de quantidades de consultas de DNS (rate limit) realizadas via TCP ou UDP por nome de domínio totalmente qualificado.

7.51. De acordo com o IP de origem, configurar limite (rate limit) para consultas realizadas via TCP ou UDP.

7.52. Criar “Listas brancas” que permitam a realização de qualquer número de consultas de DNS por segundo, para determinado endereço IP de origem.

7.53. O serviço deverá proteger no mínimo contra os seguintes ataques de DNS:

7.53.1. Reflexão;

7.53.2. Anomalias de Protocolo;

7.53.3. Negação de Serviço;

7.53.4. Negação de Serviços Distribuídos;

7.53.5. Amplificação;

7.53.6. Tunelamento;

7.53.7. Reconhecimento;

7.53.8. Explorações (Exploit);

7.53.9. Envenenamento do cache;

7.53.10. Excessos (Floods).

7.54. O serviço deve permitir que os administradores efetuem busca de endereços de rede, subrede e endereços IP através de filtros.

7.55. A administração do serviço deve permitir definir diferentes níveis de grupos e usuários para administração.

7.56. O serviço deve possuir capacidade de reverter configurações sem a necessidade de restauração de backup.

7.57. O serviço deverá fornecer pelo menos os seguintes relatórios:

7.57.1. Tendência de latência de resposta de DNS;

- 7.57.2. Nomes de domínios de DNS mais requisitados;
- 7.57.3. Tendência de uso do cache de DNS;
- 7.57.4. Top clientes de DNS;
- 7.57.5. Taxa de consultas de DNS por tipo de registro;
- 7.57.6. Tendências de respostas de DNS;
- 7.57.7. Taxa de consultas de DNS diária por servidor;
- 7.57.8. Pico de consultas diárias de DNS por servidor;
- 7.57.9. Top DNS NXDOMAIN/No error;
- 7.57.10. Top SERVFAIL enviados e recebidos;
- 7.57.11. Top clientes por domínio de DNS;
- 7.57.12. Nomes de domínios com conteúdo malicioso;
- 7.57.13. Principais domínios maliciosos;
- 7.57.14. Principais acessos ao DNS Firewall;
- 7.57.15. Quantidade de eventos registrados por horário;
- 7.57.16. Quantidade de eventos por severidade;
- 7.57.17. Quantidade de eventos por regra;
- 7.57.18. Quantidade de eventos por tendência;
- 7.57.19. Quantidade de eventos por categoria.
- 7.58. Deve permitir a criação visões (“views”) para tratamento diferenciado de consultas conforme origem das requisições.
- 7.59. Deve implementar DNSSEC com suporte a NSEC3 (RFC 5155).

8. ANTI-DDOS L4-L7

- 8.1. Deve suportar as funcionalidades de segurança para proteção DDoS.
- 8.2. Deve suportar proteção contra todos os tipos de ataques Denial of Service (DoS e DDoS).
- 8.3. A solução deve proteger de ataques DDoS que utilizem SSL.

8.4. Deve aprender automaticamente o comportamento da aplicação e combinar o comportamento heurístico do tráfego com o stress do servidor de aplicação para determinar uma condição de DDoS.

8.5. Ao detectar uma condição de DDoS, assinaturas dinâmicas devem ser automaticamente criadas e implementadas em tempo real para proteção da aplicação.

8.6. Deve permitir proteção contra-ataques DDoS, através da análise de comportamento de tráfego usando técnicas de análise de dados e Machine Learning.

8.7. Deve permitir proteger contra-ataques de DNS DDoS utilizando mecanismo que bloqueie somente as requisições maliciosas e permita requisições legítimas aos domínios existentes.

8.8. Deve suportar Network Address Translation (NAT).

8.9. Deve limitar o número de conexões.

8.10. Deve suportar Listas de Controle de Acesso (ACL).

8.11. Deve permitir o log de ataques do tipo DoS.

8.12. A solução deve possuir ferramenta flexível baseado em linguagem de programação open-source para customizar e aumentar o nível de segurança contra-ataques DDoS, incluindo a possibilidade de interação com base de reputação de endereços IP e estatísticas de tráfego.

8.13. A solução deve suportar relatórios com a detecção e mitigação dos ataques, incluindo a consolidação através de relatórios analíticos de DDoS.

8.14. Deve possuir suporte ao envio de SNMP traps para cada ataque DDoS detectado.

8.15. A solução deve possuir uma ferramenta de teste de pacotes, através da qual deve ser possível realizar testes de pacotes com atributos específicos através da solução anti -DoS.

9. SERVIÇO DE INSTALAÇÃO E CONFIGURAÇÃO

9.1. A Licitante vencedora será inteiramente responsável pela migração da solução atual para a nova solução, de forma a não comprometer o funcionamento dos sistemas, recursos ou equipamentos atualmente em operação.

9.2. Serão contemplados todos os serviços de instalação física de todos os componentes adquiridos, desde a montagem até a energização dos equipamentos.

9.3. Deverá ser fornecido documentação de toda a implementação e configuração dos produtos adquiridos.

9.4. Após no máximo 5 (cinco) dias úteis da assinatura do contrato, deverá ser realizada uma reunião presencial no Contratante, com a participação de no mínimo 1 (um) preposto da

Contratada e os representantes da equipe do Contratante, com o objetivo de elaborar o plano de migração.

9.5. A Contratada deverá apresentar, em até 15 (quinze) dias úteis da assinatura do contrato, para aprovação do Contratante, o projeto executivo contendo o plano detalhado de instalação, configuração e migração, especificando os procedimentos e cronograma a serem adotados.

9.6. O Contratante fará análise e validação do projeto executivo contendo o plano detalhado de instalação, configuração e migração, em até 5 (cinco) dias úteis, apontado as devidas correções no documento, ficando a Contratada responsável por ajustar o plano em até 7 (sete) dias úteis, conforme as alterações apontadas pela Contratante.

9.7. Fica a critério do Contratante, definir o horário de instalação e configuração dos equipamentos, podendo tais procedimentos serem executados em feriados ou finais de semana e em horário noturno.

9.8. A Contratada não poderá realizar terceirização dos serviços objeto deste termo de referência, sendo responsável pela execução do serviço objeto desta contratação.

9.9. Os serviços de instalação e configuração, para cada um dos itens, devem ser executados por técnicos da futura contratada, certificados pelo fabricante dos equipamentos fornecidos, sendo necessária a apresentação de documentação original que comprove a validade desta (s) certificação (ões) enquanto durar o contrato, que pode ser solicitada a qualquer momento.

9.10. A futura CONTRATADA deverá apresentar um Projeto Executivo que deve conter, no mínimo, as seguintes informações:

9.10.1. Objetivo dos serviços;

9.10.2. Plano de gerenciamento de mudanças, detalhando passo a passo o escopo da migração;

9.10.3. Cronograma das atividades que serão realizadas, com os prazos estimados e as diretrizes para cada atividade;

9.10.4. Projeto lógico de configuração e diagrama de interconexão dos equipamentos;

9.10.5. Nome (s) do (s) gerente (s) de projetos responsável (is) e do (s) técnico (s) responsável (is) pela execução dos serviços;

9.10.6. Lista de todos os elementos instalados contendo:

- a) Nome e endereço IP do equipamento.
- b) Equipamento e porta na qual o equipamento foi conectado.
- c) Local de instalação (prédio, andar, sala).
- d) Número de série do equipamento.

9.11. O Projeto Executivo deverá ser entregue pela futura CONTRATADA em até 15 (quinze) dias úteis após a assinatura do contrato, o qual deverá ser aprovado pela CONTRATANTE. Os serviços não poderão ser iniciados antes da apresentação e assinatura de concordância de ambas as partes.

9.12. A instalação e configuração da solução compreenderá dentre outros atendimentos, no mínimo, os seguintes requisitos:

9.12.1. Acondicionamento dos equipamentos nos locais de instalação, incluindo a desembalagem, a montagem de todos os componentes que integram a solução, a instalação dos conjuntos montados nos rack padrão 19" da CONTRATANTE, a energização do equipamento, incluindo o fornecimento de eventuais réguas, caso necessário, devendo seguir obrigatoriamente os manuais técnicos do fabricante;

9.12.2. Instalação dos transceivers e outros acessórios em seus respectivos slots;

9.12.3. Ligações de rede dos equipamentos a infraestrutura da CONTRATANTE, incluindo o fornecimento, quando necessário, de:

9.12.3.1. Cordões ópticos OM4 com, no mínimo, 2 (dois) metros de comprimento para ligações em fibra;

9.12.3.1. Patch-cords UTP CAT6A com, no mínimo, 2 (dois) metros de comprimento para ligações em par metálico.

9.12.4. Os cabos/cordões necessários para a interligação de servidores, usuários e outras conexões que não as estritamente fornecidas são de responsabilidade da CONTRATANTE, ou seja, cabe a CONTRATADA interligar os equipamentos fornecidos;

9.12.5. Upgrade ou Downgrade do firmware;

9.12.6. A realização dos ajustes de hardware e software necessários ao funcionamento do ambiente e a instalação da solução de gerenciamento;

9.12.7. Conexão das interfaces de gerenciamento a nova rede out-of-band e testes de acesso a ferramenta de gerência para administração;

9.12.8. Configuração e teste de envio de Traps SNMP. Verificações dos recursos e o seu perfeito funcionamento e integração com os demais, conforme as melhores práticas indicadas pelo fabricante;

9.12.9. A identificação dos equipamentos e de todas as suas conexões.

9.13. Todos os parâmetros a serem configurados deverão ser alinhados entre as partes em reuniões de pré-projeto, podendo estas ser realizadas presencialmente, por telefone ou via conferência web, devendo a futura CONTRATADA sugerir as configurações de acordo com

normas e boas práticas, cabendo à CONTRATANTE a sua aceitação expressa ou recusa nos casos de não atendimento das condições estabelecidas.

9.14. A Contratada deverá configurar todas as funcionalidades do produto licenciadas e solicitadas pela Contratante.

9.15. As configurações deverão seguir fielmente a padronização previamente estabelecida pela CONTRATANTE.

9.16. Durante o processo de instalação e configuração deverá ser realizada transferência de conhecimento para a equipe da Contratante.

9.17. A futura CONTRATADA deverá fazer análise do ambiente tecnológico atual, devendo a CONTRATANTE fornecer todas as informações necessárias sobre a infraestrutura instalada, de modo que se possa garantir a continuidade dos serviços prestados pelo órgão durante a migração, mantendo a disponibilidade dos serviços básicos de rede (resolução de nomes, endereçamento dinâmico, autenticação dos usuários, etc.) e dos demais serviços de retaguarda (aplicativos, correio eletrônico, banco de dados, Internet, etc.).

9.18. A substituição da infraestrutura atual deve ser planejada e executada de modo que não cause interrupções e paralisações não programadas, ou qualquer outro tipo de transtorno ao correto funcionamento do ambiente operacional da CONTRATANTE; caso não seja possível manter a disponibilidade dos serviços básicos no momento da instalação, as manobras de implantação deverão ser realizadas durante janela de manutenção agendada previamente, em horários que não comprometam o funcionamento das atividades do órgão, inclusive aos sábados, domingos e feriados.

9.19. Ao término do serviço deve ser fornecido um relatório detalhado (as-built) contendo todas as configurações realizadas, com comentários sobre os principais comandos e as justificativas das opções de parametrização de modo a facilitar a posterior administração da solução e a continuidade de seu funcionamento.

9.20. O relatório deve conter, no mínimo, as seguintes informações:

9.20.1. Diagrama de arquitetura da solução;

9.20.2. Procedimento operacional detalhado com as etapas de instalação e configuração;

9.20.3. Informações de monitoramento da solução;

9.20.4. Informações pertinentes a posterior continuidade e manutenção da solução;

9.20.5. Referências da documentação oficial do produto.

9.21. A critério da CONTRATANTE, poderá ser elaborado um único as-built contendo todas as informações de todos os equipamentos e softwares instalados/configurados.

9.22. O serviço de instalação e configuração somente será concluído após a apresentação pela contratada do projeto executivo, as-built e o recebimento definitivo do serviço pela contratante.

9.23. A contratada deverá monitorar o ambiente da contratante por ao menos 15 dias após o final e aprovação da instalação e configuração pela contratante e atuar imediatamente no caso de evento ou falha das configurações ou equipamentos.

10. GERENCIAMENTO CENTRALIZADO

10.1. A solução de gerenciamento deve fornecer um ponto de controle unificado para todo o cluster de equipamentos da solução.

10.2. A solução de gerenciamento centralizada deve ser capaz de armazenar logs, eventos.

10.3. Seja capaz de realizar operações de backup;

10.4. Deve ser capaz de realizar o licenciamento dos componentes do cluster;

10.5. Deve ser capaz de realizar monitoramento e gerenciamento do cluster;

10.6. Ser capaz de gerenciar usuários, limitando os acessos dos usuários de acordo com seus níveis de acesso;

10.7. Deve realizar coleta de dados do cluster com objetivo de armazenar e gerenciar os dados;

10.8. Deve ser capaz de armazenar backups de eventos, alertas e dados estatísticos para requisitos de recuperação de desastres do cluster;

10.9. Realizar backups automático de imagens e configurações;

10.10. Monitoramento por meio de painéis, relatórios e alertas;

10.11. Deve ser capaz de permitir realização de análises detalhadas por aplicativo;

10.12. Gerenciar licenças do cluster;

10.13. Garantir políticas consistentes de segurança e gerenciamento de tráfego em toda a sua infraestrutura;

10.14. Criar, provisionar e implantar novos dispositivos e serviços de aplicativos;

10.15. Caso a solução de gerenciamento centralizado ofertada seja virtualizado, a solução deve ser compatível com as plataformas vmware;

10.16. Deve fornecer controle de acesso baseado em função (RBAC);

10.17. Ser capaz de associar funções a usuários e grupos locais ou a outros usuários e grupos de servidores remotos do Active Directory (AD), TACACS+, RADIUS ou LDAP;

- 10.18. Deve permitir o gerenciamento de solicitações de certificados Let's Encrypt;
- 10.19. Deve ser capaz de gerar relatórios de alertas de segurança;
- 10.20. Permitir geração de relatórios de segurança por tipo de dispositivo, aplicativo, anomalias, DDoS, atividade de bot, políticas de segurança diferenciais e políticas não utilizadas;
- 10.21. Deve ser capaz de agendar e gerar automaticamente relatórios;

11. SUPORTE TÉCNICO

11.1. O serviço de suporte técnico deve ser prestado conforme especificação a seguir:

11.1.1. O licitante vencedor deverá fornecer serviço de suporte técnico on-site e remotamente, sempre que for necessário à Presidência da República para solucionar problemas, instalar, configurar e reconfigurar o software ou dirimir dúvidas técnicas relacionadas as soluções ofertadas.

11.1.2. A escolha entre o suporte técnico on-site ou remoto será realizada pela contratante e ocorrerá na ocasião da abertura de cada ordem de serviços.

11.1.3. O licitante vencedor deverá iniciar o atendimento de acordo com os prazos definidos no Instrumento de Medição de Resultado, a contar da abertura da Ordem de Serviço e esse prazo para o início do atendimento para ambos os tipos de suporte On-site, e remoto é o mesmo.

11.1.4. O suporte técnico será realizado 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana, incluindo feriados, conforme Instrumento de Medição de Resultado.

11.1.5. O término do atendimento não poderá ultrapassar o prazo estipulado no Instrumento de Medição de Resultado.

11.1.6. Os serviços de suporte técnico, a serem prestados, abrangem atividades que não são cobertas pela garantia ou pelo suporte técnico do fornecedor/fabricante, que garante a resolução de problemas referentes a falhas e defeitos.

11.1.7. O serviço será remunerado mensalmente.

11.1.8. A Ordem de Serviço poderá ser aberta por e-mail e telefone, e na ocasião da assinatura do contrato, o licitante vencedor deverá fornecer as informações para a abertura de Ordens de Serviço.

11.1.9. A empresa deverá possuir no mínimo 2 (dois) técnicos certificados pelo fabricante da solução.

11.1.10. O suporte técnico iniciará a partir da data de recebimento definitivo da solução.

11.2. Instrumento de Medição de Resultado:

11.2.1. As soluções ofertadas devem estar cobertas por garantia total fornecida pelo fabricante.

11.2.2. Durante o período de suporte, o licitante vencedor deverá atender às solicitações da PR, feitas por meio da Coordenação-Geral de Infraestrutura Tecnológica, em qualquer horário, respeitando as condições e níveis de serviço especificados a seguir.

11.2.3. O Instrumento de Medição de Resultado (IMR) será contado a partir da abertura de ordem de serviço e será classificado conforme as severidades especificadas a seguir.

11.2.4. Severidade ALTA: Esse nível de severidade é aplicado quando há indisponibilidade de componentes da solução ou as aplicações que são acessadas por meio da solução estão indisponíveis:

Dias Úteis		Sábados, Domingos e Feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
04 horas	04 horas	04 horas	04 horas

11.2.5. Severidade MÉDIA: Esse nível de severidade é aplicado quando há falha no uso da solução, estando ainda disponível, porém apresentando problemas ou instabilidade:

Dias Úteis		Sábados, Domingos e Feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
08 horas	24 horas	08 horas	24 horas

11.2.6. Severidade BAIXA: Esse nível de severidade é aplicado para a instalação, configuração, manutenções preventivas, aplicações de firmwares e esclarecimento técnico relativo ao uso da solução. Não haverá abertura de chamados de suporte técnico com esta severidade em sábados, domingos e feriados:

Dias Úteis		Sábados, Domingos e Feriados	
Prazo de atendimento	Prazo de solução definitiva	Prazo de atendimento	Prazo de solução definitiva
24 horas	72 horas	Não se aplica	Não se aplica

11.2.7. Haverá multa em caso de atraso na prestação dos serviços de acordo com a seguinte tabela:

Multa	Classificação IMR	Limite da Incidência
Para infração descrita na alínea “b” do subitem 13.1 do Termo de Referência, a multa será de 5% (cinco por cento) a 10% (dez por cento), do valor do Contrato	Severidade Crítica	180 dias

Compensatória, para a inexecução total do contrato prevista na alínea “c” do subitem 13.1 do Termo de Referência, a multa será de 1% (um por cento) a 5% (cinco por cento), do valor do Contrato	Severidade Alta	180 dias
Para infração descrita na alínea “d” do subitem 13.1 do Termo de Referência, a multa será de 0,5% (cinco décimos por cento) a 1% (um por cento), do valor do Contrato	Severidade Média	90 dias
Moratória de 0,5% (cinco décimos por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida	Severidade Baixa	15 dias
Referência: Item “13. Infrações e Sanções Administrativas” do Termo de Referência.		

11.2.8. Serão considerados para efeitos dos níveis exigidos:

11.2.8.1. Prazo de Atendimento: Tempo decorrido entre a solicitação efetuada pela Equipe Técnica da PR à Prestadora de Serviço e o efetivo início dos trabalhos de manutenção;

11.2.8.2. Prazo de Solução Definitiva: Tempo decorrido entre a solicitação efetuada pela Equipe Técnica do PR à Prestadora de Serviço e a efetiva colocação dos equipamentos em seu pleno estado de funcionamento e operação normais.

11.2.9. A contagem do prazo de atendimento e solução definitiva de cada solicitação será a partir da notificação ao licitante vencedor, até o momento da comunicação da solução definitiva do problema e aceite pela equipe técnica da PR.

11.2.10. O atendimento às solicitações de severidade ALTA deverá ser realizado nas instalações da PR (on-site) e não poderá ser interrompido até o completo restabelecimento do serviço, mesmo que se estenda para períodos noturnos, sábados, domingos e feriados. Nesse caso, não poderá implicar em custos adicionais à PR. A interrupção do suporte técnico de uma solicitação desse tipo de severidade por parte do licitante vencedor e que não tenha sido previamente autorizado pela PR, poderá ensejar em aplicação de glosas previstas.

11.2.11. As ordens de serviços classificadas com severidade MÉDIA, quando não solucionados no prazo definido, poderão ser automaticamente escaladas para a severidade ALTA, sendo que os prazos de atendimento e solução definitiva do problema, bem como glosas previstas, serão automaticamente ajustados para o novo nível. A interrupção do suporte técnico de uma solicitação desse tipo de severidade por parte do licitante vencedor e que não tenha sido previamente autorizado pela PR, poderá ensejar em aplicação de glosas previstas.

11.2.12. Depois de concluído o suporte técnico, o licitante vencedor comunicará o fato à Equipe Técnica da PR e solicitará autorização para o fechamento do chamado. Caso a PR não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pelo licitante vencedor. Nesse caso, a PR fornecerá as pendências relativas à solicitação em aberto.

11.2.13. A PR encaminhará ao licitante vencedor, quando da reunião de apresentação inicial, relação nominal da equipe técnica autorizada a abrir e fechar solicitações de suporte técnico.

11.2.14. Por necessidade excepcional de serviço, a PR também poderá solicitar a escalção de chamado para níveis superiores de severidade. Nesse caso, a escalção deverá ser justificada e os prazos dos chamados passarão a contar do início novamente.

11.2.15. O pagamento das faturas estará sujeito à glosa quando não houver cumprimento dos níveis de serviço exigidos ou quaisquer outras que impliquem em glosas previstas.

12. CAPACITAÇÃO

12.1. A capacitação deverá ser realizada no idioma português do Brasil.

12.2. O material didático utilizado na capacitação deve estar no idioma inglês ou português do Brasil.

12.3. O instrutor que ministrará a capacitação da solução deve possuir certificação do fabricante da solução ofertada.

12.4. A documentação exigida em relação ao instrutor deverá ser apresentada na assinatura do contrato.

12.5. A capacitação deverá possuir uma carga horária mínima de 40 horas.

12.6. A capacitação deverá abordar no mínimo sobre a instalação, configuração, administração e resolução de problemas da solução ofertada.

12.7. Deve ser emitido um certificado para cada servidor que participar da capacitação e tiver frequência mínima de 70% (setenta por cento).

12.8. A capacitação será realizada DE FORMA ON-LINE OU PRESENCIAL em Brasília em local definido pelo licitante vencedor.

12.9. O licitante vencedor irá capacitar 8 (oito) servidores da PR.

12.10. A capacitação deve ser realizada em até 90 (noventa) dias corridos, contados a partir da solicitação oficial deste serviço.

12.11. É permitida a subcontratação desse item.