Ministério da Integração e do Desenvolvimento Regional - MIDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Administração e Tecnologia

ANEXO I - JUSTIFICATIVAS

Finalidade: Este anexo tem por finalidade incluir exigências e particularidades em função da especificidade dos serviços a serem adquiridos, previstas no Termo de Referência e passam a integrar o TR.

Aprovação do Termo de Referência e Estudo Técnico Preliminar – ETP: O Termo de Referência e o Estudo Técnico Preliminar foram aprovados por ato da autoridade competente, conforme consta do processo, 59500.002004/2024-10-e, peça 10, e-DOC 601022F4.

Justificativas:

Da escolha da solução mais adequada ao atendimento da necessidade:

A contratação de uma solução de Firewall para a Codevasf é fundamental para fortalecer a proteção da infraestrutura de TI, garantindo a segurança das redes e sistemas da organização contra ameaças externas, como ataques cibernéticos, intrusões não autorizadas e tentativas de exploração de vulnerabilidades. Com a implementação de um firewall robusto, a Codevasf poderá monitorar, filtrar e controlar o tráfego de dados, prevenindo acessos indevidos, protegendo dados sensíveis e garantindo a continuidade das operações.

Além disso, a solução de firewall proporcionará um nível de segurança adequado para prevenir ataques como DDoS (negação de serviço), intrusão, malware e outras ameaças em tempo real. A implementação de políticas de segurança personalizadas permitirá um controle granular sobre o tráfego, ajustando as permissões e restrições conforme as necessidades específicas de cada área da empresa.

Com funcionalidades avançadas, como a inspeção profunda de pacotes (DPI), filtragem de conteúdo e bloqueio de IPs maliciosos, a solução de firewall oferecerá uma defesa proativa, evitando custos com recuperação de sistemas, mitigando riscos e assegurando a proteção contra ameaças emergentes, além de permitir o monitoramento contínuo e a geração de relatórios detalhados sobre o desempenho e a segurança da rede.

Do procedimento de pesquisa de preços realizado e dos critérios adotados para a seleção dos orçamentos formadores do valor estimado:

Para a pesquisa de preços, foi utilizada a PORTARIA SGD/ME Nº 6.432, de 15 de junho de 2021. Essa portaria 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. Além disso, foram consideradas pesquisas de mercado e a INSTRUÇÃO NORMATIVA Nº 73, de 5 de agosto de 2020.

Dos requisitos de aceitação e pontuação das propostas:

Serão aceitas propostas que atendam aos critérios e especificações técnicas estabelecidos no Anexo III - Especificações Técnicas para cada item deste Termo de Referência.

Quanto à pontuação das propostas, informa-se que não se aplica, pois essa situação somente é relevante em licitações que adotam o critério de julgamento Técnica e Preço.

Das exigências habilitatórias indispensáveis à garantia do cumprimento das obrigações:

São necessárias as comprovações de qualificação de experiência e econômico-financeira, conforme Resolução DEX nº 821/2023.

Dos critérios de reajustamento e repactuação de preços:

Para contratos de serviços de longo prazo, como aqueles com duração de 36 meses, é crucial estabelecer mecanismos de reajustamento e repactuação de preços para lidar com possíveis variações nos custos ao

longo do tempo. Esses mecanismos visam garantir um equilíbrio financeiro justo para ambas as partes contratantes, considerando as mudanças nas condições econômicas e de mercado.

Ao considerar a utilização do ICTI em contratos de serviços de TI, é importante destacar que esse índice é especialmente projetado para refletir as variações de custos específicas do setor de tecnologia da informação, tornando-o uma escolha adequada e recomendada para contratos desse tipo. Ao incorporar o ICTI como referência para o reajustamento de preços, as partes contratantes podem garantir uma atualização adequada e precisa dos valores do contrato, alinhada com as flutuações de custos no setor de TI.

Da necessidade da contratação:

A contratação de uma solução de **Firewall** para a Codevasf é uma medida essencial para assegurar a proteção e a integridade da infraestrutura de TI, além de garantir a segurança das redes e sistemas da organização contra ameaças cibernéticas. Atualmente, a Codevasf enfrenta um cenário de riscos crescentes provenientes de ataques externos, como tentativas de intrusão, malware e outras vulnerabilidades, que podem comprometer a continuidade dos serviços e a confidencialidade dos dados. Sem uma solução de firewall robusta, a organização fica vulnerável a ataques como DDoS, ransomware e phishing, que podem prejudicar tanto a segurança da informação quanto a produtividade dos colaboradores.

Essa contratação está alinhada ao projeto 2.2.29 do Plano Diretor de Tecnologia da Informação (PDTI) para o período de 2023 a 2027, que visa fortalecer a segurança da informação e proteger o ambiente digital contra ameaças externas.

Da adoção do Pregão Eletrônico:

A escolha do Pregão Eletrônico para esta licitação se justifica pela sua capacidade de promover uma maior competição entre os fornecedores, garantindo a obtenção de melhores propostas e preços mais vantajosos.
A modalidade de Pregão Eletrônico foi adotada em razão do objeto da contratação ser bem comum, cujos padrões de desempenho e qualidade foram objetivamente definidos nas especificações deste Termo de Referência, por meio de padrões usuais de mercado, em conformidade com o disposto no art. 32, inciso IV e § 3º da Lei nº 13.303/2016.

Da adoção do SRP (SISTEMA DE REGISTRO DE PREÇOS):

A adoção do Sistema de Registro de Preços (SRP) para a contratação da solução de firewall é justificada pela sua eficiência na gestão de aquisições recorrentes, permitindo à Codevasf realizar compras de forma ágil e econômica. O SRP proporciona a centralização das demandas, garantindo que a organização possa registrar preços de fornecedores qualificados e adquirir a solução conforme a necessidade, sem a necessidade de novos processos licitatórios. Isso resulta em uma redução significativa do tempo e dos custos administrativos, além de assegurar condições vantajosas nas aquisições ao longo do contrato.

Além disso, o SRP assegura a continuidade dos serviços de suporte, manutenção e atualização da solução de firewall, essenciais para a segurança cibernética da Codevasf. Com a possibilidade de realizar compras por um período pré-estabelecido, a Codevasf ganha flexibilidade para ajustar as aquisições conforme a demanda, garantindo sempre a atualização e evolução da infraestrutura de segurança de forma planejada e controlada. Essa abordagem atende às necessidades da organização, ao mesmo tempo que cumpre as exigências legais e oferece maior previsibilidade orçamentária.

Da não instauração de procedimento de Intenção de Registro de Preços (dispensa de divulgação) e não permissão de participantes na licitação:

Optou-se por não instaurar o procedimento de intenção de registro de preços, devido ao caráter específico e estratégico da contratação. Essa medida visa assegurar agilidade e continuidade operacional, essenciais para a proteção da infraestrutura tecnológica da Codevasf

Da admissão de adesão dos órgãos não participantes:

Sim, será permitida a adesão de órgãos não participantes nesta licitação, pois a adesão a Atas de Registro de Preços traz eficiência às contratações públicas, pois agiliza processos, facilita o planejamento, reduz custos e garante a aquisição pelo melhor preço. Além disso, respeita os princípios da Administração Pública e é uma alternativa útil em casos de urgência ou execução orçamentária, otimizando o serviço público.

Justificativa da adoção do valor estimado público:

Conforme Acórdão nº 1502/2018 – Plenário TCU, nas licitações realizadas pelas empresas estatais, sempre que o orçamento de referência for utilizado como critério de aceitabilidade das propostas, sua divulgação no edital é obrigatória, e não facultativa, em observância ao princípio constitucional da publicidade e, ainda, por não haver no art. 34 da Lei nº 13.303/2016 (Lei das Estatais) proibição absoluta à revelação do orçamento.

Critério de Julgamento:

Menor preço, de acordo com o Art. 67 do Regulamento Interno de Licitações e Contratos da Codevasf. Visa obter a proposta mais vantajosa para a administração, desde que atendidos os parâmetros mínimos de desempenho, de qualidade, as especificações técnicas e requisitos de habilitação estabelecidos no Edital e seus anexos, a fim de proporcionar um julgamento igualitário entre os licitantes, sendo definido o critério de julgamento por grupo.

Dos requisitos de Qualificação Técnica:

A exigência de qualificação técnica para a empresa vencedora da licitação tem caráter de selecionar prestador de serviços com experiência. Essa medida não apenas assegura que a empresa possua o conhecimento e a experiência necessários para executar as tarefas conforme especificado, mas também contribui para a eficiência e a qualidade dos serviços prestados. Além disso, ao garantir a conformidade com os requisitos técnicos e regulamentares, a qualificação técnica protege os interesses das partes envolvidas, mitigando riscos e promovendo a confiança no processo de contratação pública. Ao final, essa exigência visa assegurar que os recursos públicos sejam utilizados de forma eficaz e responsável, resultando em benefícios tangíveis para a sociedade.

Justificativa da vantajosidade da divisão do objeto da licitação em grupos ou parcelas:

A divisão do objeto da licitação em grupos ou parcelas oferece diversas vantagens para a Codevasf, especialmente em um contexto de contratação de soluções complexas, como sistemas de firewall e serviços correlatos. Ao segmentar a licitação em partes, é possível atrair uma gama maior de fornecedores, ampliando a competitividade e aumentando as chances de obter propostas mais vantajosas em termos de custo-benefício. Essa divisão também permite que a Codevasf selecione especialistas para cada componente do projeto, garantindo a contratação de soluções mais adequadas e tecnicamente qualificadas para atender a necessidades específicas.

A adoção de dois grupos também facilita a fiscalização e gestão contratual, o que é fundamental dado o número limitado de empregados disponíveis para essas atividades. Assim, o agrupamento dos elementos em uma única solução representa a melhor estratégia para a Administração, considerando que a adjudicação de itens isolados oneraria a gestão pública com um maior uso de recursos humanos e tornaria o controle mais complexo, ameaçando a economia de escala e a agilidade processual, conforme orientado no ACÓRDÃO Nº5301/2013 – TCU – 2ª Câmara.

Da não exclusividade e/ou cota reservada para ME/EPP: microempresas e empresas de pequeno porte:

A não previsão de exclusividade ou cota reservada para ME/EPP nesta licitação decorre da análise técnica que considerou a indivisibilidade do objeto licitado, que se refere à prestação do serviço em sua totalidade. Segundo o disposto no art. 48 da Lei Complementar nº 123/2006, a exclusividade para ME/EPP é obrigatória apenas quando o valor do item ou grupo é inferior ou igual a R$ 80.000,00 (oitenta mil reais). No presente caso, o valor estimado para o grupo/item licitado supera o referido limite, inviabilizando a adoção do regime exclusivo para ME/EPP.

Permissão para Participação de Consórcios:

A participação de consórcios não será permitida por se tratar de fornecimento de materiais e equipamentos comuns, de baixa complexidade, a logística necessária para cumprimento do objeto não exige o envolvimento de empresas com diferentes especialidades, não sendo consequentemente pertinente a formação de consórcios com intuito de reforçar a capacidade técnica e financeira do licitante. As empresas isoladas podem perfeitamente conseguir preencher os requisitos necessários para tal.

Limite do número de empresas por Consórcio:

Não se aplica

Permissão para Participação de Sociedades Cooperativas:

Não será permitida a participação de pessoas jurídicas organizadas sob a forma de Cooperativas, visto que as características específicas do objeto e da prestação de serviço/operações/atividades requerem uma gestão operacional centralizada e não concedem autonomia aos cooperados, conforme estipulado pela Instrução Normativa MPOG 05/2017. Esta restrição se fundamenta na necessidade de garantir a eficiência e a coerência na execução dos serviços, aspectos que poderiam ser comprometidos pela estrutura descentralizada das cooperativas.

Permissão para Subcontratação:

Não será permitida a subcontratação nesta licitação devido às deficiências na responsabilidade contratual. Ao permitir a subcontratação, a responsabilidade contratual pode se tornar difusa, dificultando a determinação clara de quem é responsável por quais aspectos do projeto em casos de problemas ou disputas. Isso pode complicar a resolução eficaz de questões contratuais e prejudicar a gestão adequada do projeto.

Declaração de compatibilidade com o Plano Plurianual:

Os fornecimentos/serviços a serem contratados serão executados no prazo superior a um ano, conforme consta do Termo de Referência e a previsão de recursos orçamentários é compatível, conforme previsto no Plano Plurianual.

Garantia de Execução (caução):

A exigência de caução nesse edital proporciona segurança para a Administração Pública, garantindo que o contratado cumpra suas obrigações contratuais e protegendo os interesses da CODEVASF. Além disso, a caução atua na mitigação de riscos, servindo como proteção contra inadimplência, insolvência ou incapacidade do contratado, permitindo a cobertura de custos de reparação ou compensação em caso de falha.

Garantia do Objeto:

O prazo de garantia contratual dos bens será de, no mínimo, 36 (trinta e seis) meses, ou conforme o prazo oferecido pelo fabricante, caso seja superior, contando-se a partir do primeiro dia útil após a data de recebimento definitivo do objeto.

Apresentação de amostras:

Não se aplica para essa licitação.

Apresentação de Carta de Solidariedade:

Conforme art. 41, IV, da Lei 14.133/2021, o licitante vencedor deve apresentar carta de solidariedade emitida pelo fabricante, que assegure a execução do contrato, no caso de licitante revendedor ou distribuidor.

Da não exigência de apresentação de capital social mínimo:

O capital social mínimo de 10% (dez por cento) do valor orçado pela Codevasf no grupo da licitação que concorrer, não sendo de forma acumulativa.

Ministério da Integração e do Desenvolvimento Regional - MIDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Administração e Tecnologia

Anexo II

Planilhas de Quantidades e Preços

GRUPO	ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	CATMAT/ CATSER	UNIDADE	QTD	VALOR MÁXIMO UNITÁRIO R$	VALOR MÁXIMO TOTAL R$
GRUPO 1	1	Renovação do suporte premium habilitado pelo parceiro, termo de 3 anos, renovação, PA-3220 | PN: PAN-SVC-BKLN-3220-3YR-R	27502	Unidade	2	R$ 67.575,00	R$ 135.150,00
	2	Renovação da assinatura Advanced Threat Prevention de 3 anos para dispositivo em um par de HA, PA-3220 | PN: PAN-PA-3220-ATP-3YR-HA2	27502	Unidade	2	R$ 103.062,50	R$ 206.125,00
	3	Renovação da assinatura Advanced URL Filtering, 3 anos, PA-3220 HA Pair | PN: PAN-PA-3220-ADVURL-3YR-HA2	27502	Unidade	2	R$ 103.125,00	R$ 206.250,00
	4	Renovação da assinatura GlobalProtect de 3 anos, renovação para dispositivo em um par de HA, PA-3220 | PN: PAN-PA-3220-GP-3YR-HA2-R	27502	Unidade	2	R$ 110.537,00	R$ 221.074,00
	5	Subscrição da licença de uso para DNS Security nos Appliances PA-3220 SN: 016201029545 e SN: 016201029547	27502	Unidade	2	R$ 117.017,00	R$ 234.034,00
	6	Subscrição da Licença WildFire nos Appliances PA-3220 SN: 016201029545 e SN: 016201029547	27502	Unidade	2	R$ 149.010,25	R$ 298.020,50
	7	Subscrição da Licença AIOps nos Appliances PA-3220 SN: 016201029545 e SN: 016201029547	27502	Unidade	2	R$ 115.619,00	R$ 231.238,00
	8	Subscrição da Licença Data Loss Prevention (DLP) nos Appliances PA-3220 SN: 016201029545 e SN: 016201029547	27502	Unidade	2	R$ 240.000,00	R$ 480.000,00
	9	Subscrição de Gerência Centralizada Palo Alto	27502	Mês	36	R$ 2.747,71	R$ 98.917,56
	10	Subscrição da Solução Palo Alto ZTNA	27502	Unidade	500	R$ 406,00	R$ 203.000,00
	11	Serviço de suporte Técnico e Manutenção 24/7 para os itens 1 a 10	26980	Mês	36	R$ 3.601,17	R$ 129.642,12
	12	Treinamento de no mínimo 40h para até 3 pessoas para os itens 1 a 10	3840	Turma	1	R$ 29.800,00	R$ 29.800,00
GRUPO 2	1	Aquisição de Firewall de Aplicação Web (WAF)	27502	Unidade	2	R$ 254.873,70	R$ 509.747,40
	2	Serviço de suporte Técnico e Manutenção 24/7 para o item 1 (WAF)	26980	Mês	36	R$ 2.112,25	R$ 76.041,00
	3	Treinamento de no mínimo 20h para até 3 pessoas (WAF)	3840	Turma	1	R$ 29.997,25	R$ 29.997,25
						Valor total do Grupo 1	**R$ 2.473.251,18**
						Valor total do Grupo 2	**R$ 615.785,65**
						Total do Geral (Grupo 1 + Grupo 2)	**R$ 3.089.036,83**

ANEXO III

ESPECIFICAÇÃO DOS REQUISITOS MÍNIMOS PARA SOLUÇÃO DE FIREWALL

OBJETIVO

Este anexo descreve as especificações técnicas para a contratação de solução de firewall, renovação de assinatura, garantia e suporte para licenças, subscrição de licenças e treinamento; aquisição de firewall de aplicação web (WAF) e treinamento, para Codevasf em Brasília – DF, pelo período de 36 (trinta e seis) meses.

1 – REQUISITOS MINIMOS NECESSARIOS

ITEM 1 - Renovação do Suporte Premium para PA-3220 | PN: PAN-SVC-BKLN-3220-3YR-R

- Descrição: renovação do suporte premium para 2 equipamentos modelo PA-3220 em HA, com acesso direto ao fabricante para assistência e cobertura de incidentes críticos.
- Período: 3 anos de contrato.
- Serviços de atualização:
  - *Patches* e *hotfixes*: inclusão de atualizações de firmware e correções emergenciais de vulnerabilidades.
  - *Release management*: planejamento e consulta para atualizações de software para melhorias contínuas de desempenho.

ITEM 2 - Renovação da Assinatura Advanced Threat Prevention | PN: PAN-PA-3220-ATP-3YR-HA2

- Descrição: renovação da assinatura para prevenção avançada de ameaças, protegendo contra ameaças conhecidas e desconhecidas.
- Período: 3 anos.
- Configuração em alta disponibilidade (HA) para redundância.
- Funcionalidades de segurança:
  - Proteção multicamadas: análise de *malware*, *exploits* e ataques *zero-day*.
  - Análise em tempo real: monitoramento contínuo e detecção de ameaças sem impacto no desempenho.
  - Proteção de tráfego criptografado: inspeção profunda de tráfego HTTPS e SSL, para evitar que ameaças *bypassem* a segurança.
  - Alertas automatizados: notificações em tempo real para ataques e recomendações para remediação.

ITEM 3 - Renovação da Assinatura Advanced URL Filtering | PN: PAN-PA-3220-ADVURL-3YR-HA2

- Descrição: renovação da assinatura para filtragem avançada de URLs, permitindo proteção detalhada contra ameaças veiculadas por links.
- Período: 3 anos.
- Configuração em alta disponibilidade (HA) para redundância.
- Capacidades de filtragem:
  - Detecção e Bloqueio de URLs Maliciosas: monitoramento constante para impedir acesso a URLs maliciosas e sites de phishing.
  - Categorias de Filtragem: 40+ categorias de conteúdo, com opções de bloqueio, alerta ou permissão, conforme as políticas.
  - Identificação de Conteúdo Dinâmico: proteção contra novos domínios e sites criados para ataques de curto prazo.
  - Relatórios de Uso de Web: visualização detalhada do tráfego de URL, categorizando acessos e gerando relatórios para análise de conformidade.

ITEM 4 - Renovação da Assinatura GlobalProtect | PN: PAN-PA-3220-GP-3YR-HA2-R

- Descrição: renovação do serviço de segurança de acesso remoto GlobalProtect.
- Período: 3 anos.
- Configuração em Alta Disponibilidade (HA) para redundância.
- Funcionalidades de Acesso Remoto Seguro:
    - Segmentação e Controle de Aplicativos: controle granular de aplicações acessíveis remotamente.
    - Detecção de Dispositivos e Postura de Segurança: Validação do estado de segurança do dispositivo antes de conceder acesso à rede.
    - Configuração Zero Trust: acesso baseado em princípios de Zero Trust, minimizando riscos de lateralização de ameaças.
    - Logs e Relatórios: monitoramento contínuo do tráfego e relatórios detalhados de acesso para auditoria e conformidade.

ITEM 5 - Subscrição da Licença DNS Security nos Appliances PA-3220

- Descrição: subscrição de segurança DNS, proporcionando proteção contra ataques avançados de DNS.
- Compatibilidade: PA-3220 com SN: 016201029545 e SN: 016201029547.
- Funcionalidades de Proteção de DNS:
    - Mitigação de Ataques DNS: defesa contra ataques de envenenamento de cache, DDoS, e redirecionamentos maliciosos.
    - Consulta Segura de DNS: validação de consultas DNS, garantindo acesso somente a domínios confiáveis.
    - Bloqueio de Domínios Não Confiáveis: identificação de domínios não categorizados e uso de algoritmos para classificação em tempo real.
    - Monitoramento e Visibilidade: relatórios de acessos DNS para análise de segurança e auditorias.

ITEM 6 - Subscrição da Licença WildFire nos Appliances PA-3220

- Descrição: análise avançada de ameaças e prevenção baseada em IA através do serviço WildFire.
- Compatibilidade: PA-3220 com SN: 016201029545 e SN: 016201029547.
- Capacidades de Inteligência e Análise de Malware:
    - Análise de Arquivos Suspeitos: escaneamento de arquivos anexos, executáveis e documentos para detecção de ameaças.
    - Inteligência Artificial para Identificação Proativa: IA para análise comportamental de arquivos e identificação de anomalias.
    - Base de Dados Global: acesso a um banco de dados em constante atualização com informações sobre novas ameaças.
    - Quarentena e Resposta: isolamento automático de arquivos suspeitos, evitando a disseminação de ameaças.

ITEM 7 - Subscrição da Licença AIOps nos Appliances PA-3220

- Descrição: monitoramento e otimização contínua da infraestrutura de TI através de algoritmos de AIOps.
- Compatibilidade: PA-3220 com SN: 016201029545 e SN: 016201029547.
- Recursos de Inteligência Operacional:
    - Análise Preditiva e Detecção de Anomalias: identificação proativa de problemas potenciais antes que afetem a operação.
    - Automação de Respostas a Incidentes: AIOps sugere e aplica respostas automáticas a incidentes, minimizando o tempo de inatividade.
    - Visão Holística da Infraestrutura: integração de dados de várias fontes para monitoramento consolidado e relatórios de desempenho.

ITEM 8 - Subscrição da Licença Data Loss Prevention (DLP) nos Appliances PA-3220

- Descrição: proteção avançada contra vazamento de dados e compliance com a LGPD.
- Compatibilidade: PA-3220 com SN: 016201029545 e SN: 016201029547.
- Funcionalidades de Proteção de Dados:
    - Monitoramento e Controle de Dados Críticos: classificação automática de dados sensíveis e aplicação de políticas de segurança.
    - Prevenção Contra Vazamento de Dados em Trânsito: controle de dados em trânsito para evitar transferências não autorizadas.
    - Auditoria e Conformidade: relatórios detalhados de movimentação de dados para fins de auditoria e conformidade com a LGPD.

ITEM 9 - Subscrição de Gerência Centralizada Palo Alto

- Descrição: plataforma de gerenciamento centralizado para segurança em ambientes de nuvem.
- Compatibilidade: PA-3220 com SN: 016201029545 e SN: 016201029547.
- Funcionalidades de Gestão Centralizada:
    - Monitoramento em Tempo Real: visibilidade em tempo real para ambientes de multi-nuvem.
    - Automação e Implementação de Políticas: definição de políticas de segurança automatizadas em ambientes locais e em nuvem.
    - Conformidade com Normas: ferramentas para garantir *compliance* com LGPD e normas de privacidade.

ITEM 10 - Subscrição da Solução Palo Alto ZTNA

O item consiste na contratação da subscrição de uma solução completa de Secure Access Service Edge (SASE) que integre segurança e conectividade em nuvem para a Codevasf, visando proteção de dados, otimização de performance e conformidade com normas regulatórias, como a LGPD. Este serviço deverá cobrir os seguintes aspectos e funcionalidades:

- **Integração de Segurança e Conectividade em Nuvem**: a solução SASE deve combinar funcionalidades avançadas de segurança de rede, como firewall, VPN, e proteção contra ameaças, com um sistema de conectividade segura e escalável na nuvem. Deve garantir uma experiência de acesso consistente e protegida para colaboradores e dispositivos, independentemente da localização ou do meio de acesso.
- **Segurança em Nuvem para Trabalhos Remotos e Filiais**: a SASE precisa proporcionar uma camada de segurança centralizada que seja facilmente aplicável a ambientes de trabalho remoto e filiais distribuídas. Isso inclui autenticação, verificação de identidade e autorização para acesso seguro a dados e aplicativos corporativos, assegurando a mesma proteção dos ambientes de rede interna.
- **Proteção de Dados Sensíveis e Conformidade com a LGPD**: a solução deve oferecer funcionalidades que ajudem a Codevasf a garantir a privacidade e proteção dos dados em trânsito, em uso e em repouso, atendendo aos requisitos da Lei Geral de Proteção de Dados (LGPD). Este módulo de proteção deve incluir:
    - Controle de acesso e segmentação de rede para dados confidenciais.
    - Monitoramento em tempo real do tráfego de rede para evitar o compartilhamento não autorizado de informações sensíveis.
- **Visibilidade e Controle Centralizado**: o SASE deverá contar com uma plataforma de gerenciamento centralizado, possibilitando:
    - Visibilidade completa sobre o tráfego e a atividade de usuários e dispositivos.
    - Controle em tempo real dos acessos e detecção de anomalias.
    - Análise e criação de relatórios para auditoria e conformidade regulatória.
- **Controle de Acesso *Zero Trust* (ZTNA)**: a solução deve incorporar o princípio de Zero Trust Network Access, onde cada tentativa de acesso é verificada e monitorada. O sistema deverá:
    - Realizar verificações de identidade em cada acesso solicitado.
    - Aplicar políticas de acesso dinâmicas, considerando fatores como localização do usuário, tipo de dispositivo e histórico de acesso.

  - Mitigar riscos de segurança derivados de acessos não autorizados e comportamentos suspeitos.
- **Proteção Contra Ameaças e Inspeção de Tráfego Criptografado**: a solução deverá ter mecanismos de segurança integrados para proteger contra ameaças avançadas, incluindo:
  - Inspeção de tráfego SSL/TLS para identificar e bloquear ameaças escondidas em comunicações criptografadas.
  - Capacidade de identificação de malwares, exploits e ataques de phishing.
- **Desempenho e Otimização de Rede**: o SASE precisa incluir funções de otimização de tráfego e priorização de aplicações para garantir um desempenho eficiente em ambientes de alta demanda. Isso inclui:
  - Balanceamento de carga para distribuir o tráfego de forma otimizada.
  - Redução de latência para conexões remotas por meio de pontos de presença distribuídos globalmente.
- **Escalabilidade e Flexibilidade**: a solução SASE deve ser altamente escalável, adaptando-se ao crescimento da infraestrutura da Codevasf e de fácil integração com soluções existentes. A flexibilidade da solução deve permitir:
  - Adicionar ou remover funcionalidades de acordo com novas demandas.
  - A compatibilidade com diversos dispositivos e ambientes de nuvem pública, privada e híbrida.
- **Suporte e Atualizações Contínuas**: O contrato deve incluir o suporte técnico 24x7, garantindo assistência para instalação, configuração e resolução de problemas. Além disso, a solução deve ser atualizada regularmente para incorporar novas funcionalidades e corrigir vulnerabilidades emergentes.

ITEM 11 - Serviço de Suporte Técnico e Manutenção 24/7 para os Itens 1 a 10

O serviço de suporte técnico para os itens contratados deverá abranger uma série de atividades e compromissos para garantir o pleno funcionamento dos equipamentos e sistemas adquiridos. Os trabalhos realizados não envolverão quaisquer custos adicionais para o CONTRATANTE. Os principais pontos incluem:

- **Melhores Práticas**: o serviço de suporte técnico deve após instalação, realizar a adoção de melhores práticas e *health check* do ambiente com participação do fabricante da solução. Estas práticas envolverão integrante da Codevasf, integrante do CONTRATADO, e, **engenheiro(s) do fabricante para revisar, recomendar e aplicar melhorias nas políticas e regras de proteção no firewall** em todas as funcionalidades e features habilitadas. Ao termino o engenheiro do fabricante, responsável na condução do trabalho, deve entregar documentação das políticas existentes. A periodicidade de revisão de aplicação das melhores práticas deverá, ser realizada regularmente no ambiente da CONTRATADA, em intervalos de tempos não superior a 6 (seis) meses.
- **Alertas Críticos e Violação de Defesa:** o serviço de suporte técnico deve permitir o atendimento com participação de engenheiro(s) do fabricante em caso de atividade(s) de ataque(s) que cause instabilidade ou impacto no ambiente da CONTRATANTE, ou de violação de mecanismos de defesa. A critério da CONTRATANTE poderá solicitar relatório com detalhes da ocorrência, deverão ser elaborados em até 24 (vinte e quatro) horas.
- **Assistência Técnica em Garantia**: o serviço de assistência técnica em garantia deve cobrir todos os procedimentos técnicos destinados ao reparo de falhas nos equipamentos ou sistemas, assegurando o restabelecimento de seu estado normal de operação. Inclui substituição de peças, ajustes e reparos técnicos em conformidade com as especificações dos manuais e normas do fabricante, sem custos adicionais para o CONTRATANTE.
- **Manutenção Preventiva e Corretiva**: os serviços de suporte técnico incluirão manutenção preventiva para evitar falhas, bem como manutenção corretiva para resolver problemas existentes. Abrange esclarecimento de dúvidas e reparo de questões relacionadas ao desempenho e funcionamento da solução contratada.
- **Elaboração de Relatórios e Diagnósticos**: a CONTRATADA deverá fornecer relatórios técnicos detalhados, diagnósticos e estudos sobre o ambiente de operação da solução, permitindo ao CONTRATANTE uma visão precisa sobre o estado atual e eventuais necessidades de aprimoramento.
- **Transferência de Conhecimento**: a CONTRATADA se compromete a compartilhar conhecimento técnico com a equipe do CONTRATANTE, detalhando problemas vivenciados e as soluções aplicadas, por meio de treinamentos ou explicações, conforme acordado entre as partes.

- **Instalação, Atualização e Configuração**: o suporte técnico incluirá a instalação, atualização e configuração de novas versões dos produtos, sempre que o fabricante liberar atualizações tecnológicas. Isso garantirá que a solução esteja atualizada com as melhorias e correções mais recentes.
- **Suporte para Instalação e Configuração**: o suporte técnico deverá fornecer atendimento para esclarecer dúvidas relacionadas à instalação, configuração e uso do software, além de suporte para corrigir problemas como falhas, erros, defeitos ou vícios no funcionamento da solução. Também incluirá suporte para problemas na instalação ou configuração de softwares básicos e de infraestrutura de TIC (ex.: sistemas operacionais, servidores de banco de dados e servidores de aplicação) necessários para o pleno funcionamento da solução.
- **Atualização de Versões e Patches**: o serviço de suporte técnico deverá incluir a atualização de versões do software aplicativo, com incorporação de correções de erros, melhorias implementadas e funcionalidades adicionais. O serviço deverá cobrir:
    - Fornecimento de novas versões e releases durante o período de vigência da garantia.
    - Disponibilização de manuais e documentos técnicos em formato digital para cada atualização, bem como notas informativas sobre as funcionalidades adicionadas.
    - Comunicação imediata ao CONTRATANTE sobre a disponibilização de patches de correção, detalhando os defeitos que serão corrigidos e a forma de obtenção do patch. Essa comunicação deverá ocorrer no prazo máximo de 30 (trinta) dias após o lançamento da atualização ou solução de correção.
- **Implantação de Novas Versões e Patches**: a CONTRATADA será responsável pela implementação de novas versões, releases, e pela aplicação de patches de correção e pacotes de serviço (service packs) para os produtos fornecidos como parte da solução. A implantação deverá ser agendada com os responsáveis pela solução no CONTRATANTE, de acordo com o nível de severidade do chamado técnico.
- **Assistência para Reinstalação de Ferramentas**: a CONTRATADA auxiliará o CONTRATANTE na reinstalação das ferramentas, se necessário, durante o período de garantia da solução.
    - **Canais de Suporte Técnico**: a CONTRATADA deverá disponibilizar múltiplos canais de acesso ao suporte técnico, incluindo: Portal Web, E-mail, Central 0800 e/ou telefone fixo.
- **Atendimento Ininterrupto**: O atendimento deverá estar disponível 24 horas por dia, 7 dias por semana, durante os 365 dias do ano, com atendimento em língua portuguesa.

ITEM 12 - Treinamento de 40 horas para até 3 pessoas (Itens 1 a 10)

Este item detalha as especificações e requisitos para o treinamento técnico de capacitação sobre a solução de firewall adquirida, abrangendo desde a instalação e configuração até a administração e suporte técnico, visando que a equipe da CONTRATANTE adquira conhecimento prático e aprofundado sobre a solução de firewall.

- **Tipo e Objetivo do Treinamento**:
    - O treinamento deverá ser de capacitação técnica oficial, diretamente alinhado com as práticas recomendadas pelo fabricante da solução de firewall adquirida.
    - O curso abordará todos os aspectos fundamentais da solução, incluindo instalação, configuração, administração, monitoramento, e suporte técnico, capacitando a equipe para gerenciar a solução de firewall de forma eficaz.
- **Formato e Local de Treinamento**:
    - O treinamento será realizado online, em uma plataforma de fácil acesso, com recursos que permitam tanto o aprendizado teórico quanto prático (hands-on).
    - A CONTRATADA deverá prover um ambiente virtual que contemple demonstrações ao vivo, sessões interativas e atividades práticas.
- **Carga Horária e Horário**:
    - O treinamento deverá ter uma carga horária mínima de 40 (vinte) horas.
    - Será realizado em dias úteis, conforme a conveniência da CONTRATANTE (matutino ou vespertino).
    - A data e o horário serão acordados entre a CONTRATADA e a CONTRATANTE para maior flexibilidade e adequação à disponibilidade dos participantes.
- **Turma e Participantes**:

- A turma deverá ser composta por até 3 (três) participantes indicados pela CONTRATANTE, que terão acesso completo aos conteúdos e atividades práticas.

- **Pré-requisitos e Condições de Realização**:
  - O treinamento deverá ocorrer após a conclusão da implementação da solução, permitindo que a equipe já esteja familiarizada com o ambiente.
  - O conteúdo programático do curso deverá ser aprovado previamente pela CONTRATANTE, e qualquer alteração deverá ser acordada entre as partes.
  - O curso deve abranger todas as funcionalidades nativas da solução, bem como recursos customizáveis, garantindo um domínio completo das funcionalidades do firewall.
- **Instrutor Certificado**:
  - O treinamento deverá ser ministrado por um instrutor certificado pelo fabricante da solução de firewall, com comprovação de qualificação técnica.
  - A CONTRATADA deverá apresentar o documento de certificação do instrutor em até 5 (cinco) dias antes do início do treinamento, em formato original ou cópia autenticada.
- **Certificação e Capacitação Final dos Participantes**:
  - Ao final do curso, cada participante deverá receber um certificado oficial, contendo a carga horária, o conteúdo programático e demais informações pertinentes.
  - Concluído o treinamento, os participantes deverão estar aptos a realizar as seguintes atividades com autonomia:
    - Instalação, configuração e atualização da solução;
    - Administração e suporte técnico;
    - Monitoramento e ajustes de desempenho;
    - Diagnóstico de problemas;
    - Auditoria de eventos;
    - Geração de relatórios;
    - Execução de backups e restauração, entre outras atividades essenciais para a gestão da solução de firewall na Codevasf.

ITEM 13 - Aquisição de Firewall de Aplicação Web (WAF)

Este item detalha as especificações técnicas para a aquisição de uma solução de Firewall de Aplicação Web (WAF), que visa proteger as aplicações web da Codevasf contra ameaças e vulnerabilidades específicas de camada de aplicação, fortalecendo a segurança e a conformidade com regulamentações como a LGPD.

- **Objetivo e Alcance**:
  - A aquisição do WAF tem como principal objetivo garantir a segurança das aplicações web da Codevasf, protegendo-as contra ataques como injeção de SQL, cross-site scripting (XSS), ataques de negação de serviço distribuídos (DDoS) e outras ameaças que possam comprometer a integridade dos sistemas e a confidencialidade dos dados.
  - A solução deverá proporcionar uma camada de defesa robusta e configurável para mitigar riscos e proteger a experiência dos usuários finais.
- **Requisitos de Proteção e Funcionalidades**:
  - **Proteção contra Vulnerabilidades de Camada de Aplicação**: Identificar e bloquear ameaças específicas de camada de aplicação, incluindo ataques de injeção, manipulação de cookies, e exploração de vulnerabilidades conhecidas.
  - **Filtragem e Análise de Tráfego HTTP/HTTPS**: Monitoramento contínuo do tráfego para detectar e prevenir comportamentos anômalos e maliciosos em tempo real.
  - **Detecção e Mitigação de Ataques DDoS**: A solução deve ter recursos para proteger contra ataques de DDoS, garantindo a disponibilidade das aplicações.
  - **Controle Granular de Políticas de Acesso**: Capacidade de definir e aplicar políticas de acesso e segurança específicas para cada aplicação, com suporte a métodos de autenticação multifatorial.
  - **Proteção Avançada Contra Bots Maliciosos**: Ferramentas de reconhecimento e bloqueio de bots maliciosos que podem explorar as aplicações e sobrecarregar os sistemas.

- **Configurações e Personalização**:
  - **Políticas Customizáveis**: A solução deve permitir a criação e ajuste de regras de segurança específicas para cada aplicação web, alinhando-se às necessidades e especificidades dos serviços da Codevasf.
  - **Aprendizado Automático e Integração com Inteligência Artificial (IA)**: A solução deverá contar com recursos de aprendizado de máquina para identificar padrões suspeitos e ajustar as defesas automaticamente.
  - **Dashboard Centralizado e Relatórios**: Interface de monitoramento centralizada que permita visualização em tempo real do estado das aplicações, ataques detectados e eficácia das medidas de proteção, com a opção de gerar relatórios detalhados.
- **Compatibilidade e Escalabilidade**:
  - **Compatibilidade com Infraestrutura Existente**: A solução de WAF deverá ser compatível com os sistemas e aplicações web da Codevasf, integrando-se aos demais componentes da infraestrutura de segurança.
  - **Escalabilidade**: Deve suportar o crescimento da demanda e da infraestrutura web, permitindo expansões futuras sem a necessidade de troca da solução.
- **Requisitos de Conformidade e Normas de Segurança**:
  - **Compliance com Regulamentações**: Atender às diretrizes e regulamentações nacionais e internacionais, incluindo a LGPD, oferecendo proteção para dados pessoais e garantindo a conformidade com as práticas de segurança da informação.
  - **Certificações de Segurança**: O WAF deve contar com certificações de segurança reconhecidas no mercado, garantindo a confiabilidade e eficácia da solução.
- **Licenciamento**:
  - Fornecimento de licenças permanentes ou por subscrição, conforme especificado pela Codevasf, para garantir a continuidade do funcionamento sem interrupções.

ITEM 14 - Serviço de Suporte Técnico e Manutenção 24/7 para o WAF

Os trabalhos realizados não envolverão quaisquer custos adicionais para o CONTRATANTE. Os principais pontos incluem:

- **Objetivo**:
  - Garantir a operação contínua e eficiente da solução de WAF adquirida, proporcionando suporte técnico especializado para resolver problemas, realizar ajustes e garantir a performance ideal do sistema, 24 horas por dia, 7 dias por semana, durante toda a vigência do contrato.
- **Abrangência dos Serviços**:
  - **Suporte Técnico Remoto**: Disponibilidade de uma equipe especializada para fornecer suporte remoto, por meio de canais como telefone, e-mail e portal de atendimento, para resolução de problemas técnicos, esclarecimento de dúvidas sobre a solução, configuração de regras de segurança e ajustes em tempo real.
  - **Suporte Técnico On-Site**: Caso a solução necessite de intervenção física ou ajustes específicos que não possam ser resolvidos remotamente, o suporte técnico on-site será fornecido. O atendimento no local será realizado dentro do prazo acordado e com a presença de técnicos especializados.
  - **Melhores Práticas**: o serviço de suporte técnico deve após instalação, realizar a adoção de melhores práticas e *health check* do ambiente **com participação do fabricante da solução**. Estas práticas envolverão integrante da Codevasf, integrante do CONTRATADO, e, engenheiro(s) do fabricante para **revisar, recomendar e aplicar melhorias nas políticas e regras de proteção no WAF** em todas as funcionalidades e features habilitadas. Ao termino o engenheiro do fabricante, responsável na condução do trabalho, deve entregar documentação das políticas existentes. A periodicidade de revisão de aplicação das melhores práticas deverá, ser realizada regularmente no ambiente da CONTRATADA, em intervalos de tempos não superior a 6 (seis) meses.
  - **Alertas Críticos e Violação de Defesa**: o serviço de suporte técnico deve permitir o atendimento com participação de engenheiro(s) do fabricante em caso de atividade(s) de ataque(s) que cause instabilidade ou impacto no ambiente da CONTRATANTE, ou de violação de mecanismos de defesa. A critério da CONTRATANTE poderá solicitar relatório com detalhes da ocorrência,

deverão ser elaborados em até 24 (vinte e quatro) horas.

- **Assistência 24/7**: O suporte técnico será disponibilizado ininterruptamente, atendendo em todos os dias do ano (24 horas por dia, 7 dias por semana), garantindo que qualquer incidente seja tratado com a urgência necessária, independentemente da hora ou dia da semana.

- **Manutenção Preventiva e Corretiva**:
  - **Manutenção Preventiva**: A manutenção preventiva será realizada periodicamente, com o objetivo de garantir que a solução de WAF funcione de maneira otimizada, minimizando riscos de falhas e vulnerabilidades. Isso incluirá a análise de performance, verificação de logs e relatórios, ajustes finos em configurações de segurança, bem como recomendações para melhorias.
  - **Manutenção Corretiva**: Caso sejam identificados problemas técnicos ou falhas no sistema, a manutenção corretiva será executada de forma a resolver os incidentes o mais rápido possível. Isso pode incluir a correção de falhas de configuração, problemas com atualizações, ou a implementação de patches de segurança críticos.
- **Gestão de Atualizações e Patches**:
  - **Atualizações de Software**: O serviço de suporte técnico incluirá a instalação e implementação das atualizações de software liberadas pelo fabricante do WAF, garantindo que a solução esteja sempre alinhada com as últimas melhorias de segurança, funcionalidades e correções de bugs.
  - **Patches de Segurança**: A equipe de suporte deverá aplicar todos os patches de segurança fornecidos pelo fabricante de forma proativa e no menor tempo possível, com o objetivo de manter a proteção da solução de WAF contra novas ameaças e vulnerabilidades. A CONTRATADA deverá comunicar ao CONTRATANTE as atualizações e patches disponibilizados, detalhando as melhorias implementadas.
- **Resolução de Incidentes e Análise de Logs**:
  - **Monitoramento e Diagnóstico Proativo**: O suporte incluirá a análise contínua dos logs de tráfego, relatórios de ameaças e alertas para identificar e diagnosticar incidentes de segurança em tempo real. O diagnóstico incluirá a avaliação de tentativas de ataques, falhas de configuração e a análise de eventos críticos.
  - **Escalonamento de Incidentes**: Caso o suporte técnico inicial não consiga resolver um incidente, haverá um escalonamento imediato para especialistas em níveis superiores, garantindo uma resposta ágil e eficaz para resolver problemas complexos ou críticos.
- **Documentação e Relatórios**:
  - **Relatórios de Manutenção e Suporte**: O fornecedor do suporte técnico deverá fornecer relatórios periódicos detalhados sobre as atividades de manutenção realizadas, status da solução de segurança, incidentes resolvidos e atualizações implementadas. Esses relatórios serão entregues ao CONTRATANTE para assegurar a transparência e acompanhamento da performance da solução.
  - **Documentação Técnica**: Em cada intervenção ou atualização realizada, será disponibilizada a documentação técnica pertinente, incluindo guias de configuração, relatórios de incidentes e a descrição detalhada das correções ou melhorias aplicadas.
- **Ferramentas de Suporte**:
  - A CONTRATADA deverá disponibilizar ferramentas de acesso remoto para diagnóstico e resolução de problemas, garantindo que a equipe técnica do CONTRATANTE possa obter assistência imediata e remota para ajustes, atualizações e soluções de incidentes.

Este serviço de suporte técnico e manutenção 24/7 visa assegurar que a solução de Firewall de Aplicação Web (WAF) permaneça sempre operacional e eficaz, com a melhor proteção contra as ameaças cibernéticas, garantindo a continuidade das operações e a segurança das aplicações da Codevasf.

.

ITEM 15 - Treinamento de 20 horas para até 3 pessoas (WAF)

O treinamento visa capacitar os participantes para:

- Instalar e configurar o WAF em ambientes corporativos.
- Administrar e monitorar a solução de WAF para garantir uma defesa efetiva contra ataques de aplicações web.
- Atualizar e otimizar a solução, aplicando patches e novas versões conforme as necessidades.

- Diagnosticar e corrigir falhas, identificando problemas de performance, configuração e segurança.
- Gerenciar políticas de segurança, ajustando regras conforme o tipo de tráfego e as necessidades de proteção.
- Utilizar ferramentas de monitoramento e relatórios para acompanhar a eficácia da solução.

Modalidade e Forma de Execução:

- Treinamento *online*: O treinamento será realizado em ambiente virtual da CONTRATADA, utilizando plataformas de videoconferência e ferramentas de aprendizado interativo. O ambiente de treinamento deve simular ataques diversos sobre a solução WAF, e demonstrar configurações a serem aplicadas de mitigação destes ataques, e até mesmo alternativas de contorno. Observação dos eventos de log e detalhamento das ocorrências. Será ministrado por instrutores certificados e especializados, com experiência comprovada na solução de Firewall de Aplicação Web (WAF).
- Carga Horária:
  - 20 horas de treinamento, distribuídas conforme necessidade, em meio período (matutino ou vespertino), a critério da CONTRATANTE.
- Número de Participantes:
  - O treinamento será destinado a até 3 (três) pessoas da equipe técnica do CONTRATANTE, com foco na capacitação dos profissionais que serão responsáveis pela administração da solução WAF.

Instrutores e Certificação:

- O treinamento será ministrado por profissionais certificados pelo fabricante da solução WAF. Os instrutores terão experiência comprovada na solução e nas práticas de segurança de aplicações web.
- O treinamento será concluído com a emissão de certificado de participação para cada um dos participantes, contendo:
  - Nome dos participantes.
  - Carga horária total (20 horas).
  - Conteúdo programático abordado.
  - Declaração de que os participantes adquiriram as competências necessárias para instalar, configurar, administrar e otimizar a solução WAF.

Ministério da Integração e do Desenvolvimento Regional
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba

Versão 6.0

MATRIZ DE RISCOS

PROCESSO:	59500.002004/2024-10
OBJETO DA CONTRATAÇÃO:	Contratar solução de Firewall para proteção da rede de dados da Codevasf. Monitorar e atuar sobre o tráfego de dados de entrada e saída, permitir ou bloquear passagem de dados e uso de aplicações da Internet com
OBJETIVO DA CONTRATAÇÃO:	Contratar solução de Firewall para proteção da rede de dados da Codevasf. Monitorar e atuar sobre o tráfego de dados de entrada e saída, permitir ou bloquear passagem de dados e uso de aplicações da Internet com base nas
LOCAL DE EXECUÇÃO:	
ÁREA/UNIDADE SUPRIDORA:	
ÁREA/UNIDADE DEMANDANTE:	

Cód*	Etapa de Contratação	Fator de Risco/Causa (devido a...)	Evento de Risco/Incerteza (poderá ocorrer...)	Consequência (Ocasionando)	Responsável pelo Risco (Alocação)	Probabilidade	Impacto	Nível de Risco (Residual)	Resposta - Tipo de Tratamento	Plano de Tratamento
RC006	Gestão contratual	Demora na confeção dos artefatos, demora na análise dos documentos e demora nos trâmites processuais	Poderá acontecer a não contratação de serviços de TI essenciais ao órgão	Atraso e/ou impossibilidade de finalização do processo de contratação; Atraso e/ou impossibilidade de atendimento às necessidades de negócio.	Contratante	2- Baixa	2- Pequeno		0	
RC007	Gestão contratual	Atraso no cronograma previsto - implementação/migração	Poderá ocorrer atraso no início da prestação de serviços contratados	Atraso na disponibilização da solução	Compartilhado	3- Média	2- Pequeno		0	
RC008	Gestão contratual	Não Atendimento aos níveis mínimos de serviço	Poderá acontecer a contratação de serviços que não atendam à necessidade do requisitante	Atraso na prestação do serviço.	Contratante	2- Baixa	2- Pequeno		0	
RC009	Gestão contratual	Interrupção da execução ou rescisão do contrato	Poderá acontecer a ocorrência de muitos ajustes e ao abandono da solução	suporte técnico e manutenção dos equipamentos.	Contratada	2- Baixa	2- Pequeno		0	
RC010	Gestão contratual	Perda de funcionários envolvidos com a implantação da solução.	Poderá acontecer o comprometimento do cronograma e da execução do contrato	Atraso no conogram a da implantação.	Contratante	2- Baixa	2- Pequeno		0	
RC011	Gestão contratual	Variação cambial	Poderá acontecer elevação dos preços praticados pela contratada ou perda de autonomia da contratante em executar serviços essenciais de TI	Aumento no custo do projeto	Contratante	2- Baixa	2- Pequeno		0	

Cód*	Etapa de Contratação	Fator de Risco/Causa (devido a...)	Evento de Risco/Incerteza (poderá ocorrer...)	Consequência (Ocasionando)	Responsável pelo Risco (Alocação)	Probabilidade	Impacto	Nível de Risco (Residual)	Resposta - Tipo de Tratamento	Plano de Tratamento

Cód*	Etapa de Contratação	Fator de Risco/Causa (devido a...)	Evento de Risco/Incerteza (poderá ocorrer...)	Consequência (Ocasionando)	Responsável pelo Risco (Alocação)	Probabilidade	Impacto	Nível de Risco (Residual)	Resposta - Tipo de Tratamento	Plano de Tratamento

Cód*	Etapa de Contratação	Fator de Risco/Causa (devido a...)	Evento de Risco/Incerteza (poderá ocorrer...)	Consequência (Ocasionando)	Responsável pelo Risco (Alocação)	Probabilidade	Impacto	Nível de Risco (Residual)	Resposta - Tipo de Tratamento	Plano de Tratamento

Cód*	Etapa de Contratação	Fator de Risco/Causa (devido a...)	Evento de Risco/Incerteza (poderá ocorrer...)	Consequência (Ocasionando)	Responsável pelo Risco (Alocação)	Probabilidade	Impacto	Nível de Risco (Residual)	Resposta - Tipo de Tratamento	Plano de Tratamento

Cód*	Etapa de Contratação	Fator de Risco/Causa (devido a...)	Evento de Risco/Incerteza (poderá ocorrer...)	Consequência (Ocasionando)	Responsável pelo Risco (Alocação)	Probabilidade	Impacto	Nível de Risco (Residual)	Resposta - Tipo de Tratamento	Plano de Tratamento

* Ocultar as linhas que não forem utilizadas e formatar a altura das linhas.

COORDENADOR DO PROJETO OBJETO DA CONTRATAÇÃO - DEMANDANTE			
No		Lotação:	

ANALISTAS RESPONSÁVEIS PELO MAPEAMENTO DOS RISCOS DA CONTRATAÇÃO - DEMANDANTE			
No		Lotação:	
No		Lotação:	
No		Lotação:	
No		Lotação:	
No		Lotação:	

LOCAL/DATA:	00/01/1900

Obs: Metodologia de Gerenciamento de Riscos em Contratações encontra-se em fase de testes e validação técnica, considerando o Regulamento Interno de Licitação e Contratos (RILC) e a Metodologia de Gerenciamento de Riscos (MGR), com parâmetros metodológicos para identificação, análise, avaliação e tratamento dos riscos.

Ministério da Integração e do Desenvolvimento Regional - MIDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Administração e Tecnologia

Anexo V

MODELO DE PLANILHA DE CUSTOS E FORMAÇÃO DE PREÇOS

DADOS DA PROPONENTE

Razão Social: _____

CNPJ: _____ Inscrição Estadual: _____

Representante(s) legal(is) com poder para assinar contrato _____

CPF: _____ RG: _____ Órgão Expedidor _____ UF ___ Endereço completo: _____

Cidade: _____ CEP: _____ Telefone: (___) _____

E-mail: _____ Contato: _____

Validade da Proposta (mínimo 60 dias): _____

GRUPO	ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	CATMAT/ CATSER	UNIDADE	QTD	VALOR MÁXIMO UNITÁRIO R$	VALOR MÁXIMO TOTAL R$
GRUPO 1	1	Renovação do suporte premium habilitado pelo parceiro, termo de 3 anos, renovação, PA-3220 | PN: PAN-SVC-BKLN-3220-3YR-R	27502	Unidade	2		
	2	Renovação da assinatura Advanced Threat Prevention de 3 anos para dispositivo em um par de HA, PA-3220 | PN: PAN-PA-3220-ATP-3YR-HA2	27502	Unidade	2		
	3	Renovação da assinatura Advanced URL Filtering, 3 anos, PA-3220 HA Pair | PN: PAN-PA-3220-ADVURL-3YR-HA2	27502	Unidade	2		
	4	Renovação da assinatura GlobalProtect de 3 anos, renovação para dispositivo em um par de HA, PA-3220 | PN: PAN-PA-3220-GP-3YR-HA2-R	27502	Unidade	2		
	5	Subscrição da licença de uso para DNS Security nos Appliances PA-3220 SN: 016201029545 e SN: 016201029547	27502	Unidade	2		
	6	Subscrição da Licença WildFire nos Appliances PA-3220 SN: 016201029545 e SN: 016201029547	27502	Unidade	2		
	7	Subscrição da Licença AIOps nos Appliances PA-3220 SN: 016201029545 e SN: 016201029547	27502	Unidade	2		
	8	Subscrição da Licença Data Loss Prevention (DLP) nos Appliances PA-3220 SN: 016201029545 e SN: 016201029547	27502	Unidade	2		
	9	Subscrição de Gerência Centralizada Palo Alto	27502	Mês	1		
	10	Subscrição da Solução Palo Alto ZTNA	27502	Unidade	500		
	11	Serviço de suporte Técnico e Manutenção 24/7 para os itens 1 a 10	26980	Mês	1		
	12	Treinamento de no mínimo 40h para até 3 pessoas para os itens 1 a 10	3840	Turma	1		

Ministério da Integração e do Desenvolvimento Regional - MIDR
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Área de Administração e Tecnologia

GRUPO 2	**1**	Aquisição de Firewall de Aplicação Web (WAF)	27502	Unidade	2		
	2	Serviço de suporte Técnico e Manutenção 24/7 para o item 1 (WAF)	26980	Mês	1		
	3	Treinamento de no mínimo 20h para até 3 pessoas (WAF)	3840	Turma	1		
						Valor total do Grupo 1	**R$**
						Valor total do Grupo 2	**R$**
						Total do Geral (Grupo 1 + Grupo 2)	**R$**

Declaramos que nos preços propostos estão incluídos todos os custos e despesas de qualquer natureza, incidentes sobre os objetos desta proposta.

Declaramos total conhecimento e concordância dos termos do edital do pregão e dos seus anexos. Em anexo documentação complementar com descrição da solução e equipamentos que a compõem.

Cidade (UF), _____ de _____ de 202_____.

_____

Nome Completo Responsável CPF