Ministério do Desenvolvimento Regional
Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba
Secretaria de Licitações – PR/SL

ANEXO I

TERMO DE REFERÊNCIA E SEUS ANEXOS

(GRAVADO EM ARQUIVO SEPARADO)

ANEXO II

CARTA DE APRESENTAÇÃO DE PROPOSTA

OBS.: Deverão ser respeitados os preços máximos, unitários e global orçados pela Codevasf.

MINISTÉRIO DO DESENVOLVIMENTO REGIONAL - MDR
COMPANHIA DE DESENVOLVIMENTO DOS VALES DO SÃO FRANCISCO E DO PARNAÍBA

ANEXO II

CARTA DE APRESENTAÇÃO DE PROPOSTA

DADOS DO PROPONENTE
RAZÃO SOCIAL:
CNPJ:
ENDEREÇO:
FONE:
EMAIL:
SITE:

À
Codevasf
SGA/Norte, Quadra 601, Conjunto I
CEP 70.830.901 – Brasília-DF
Ref.: Edital nº ___/2020.

Prezados Senhores,

Tendo examinado o Edital n.º ___/2020 e seus elementos técnicos constitutivos, nós, abaixo-assinados, oferecemos proposta para contratação de empresa especializada para fornecimento de serviço de suporte técnico 24x7 on-site ou presencial, manutenção técnica, garantia de atualização, garantia de hardware, treinamento e repasse de conhecimento para a solução firewall corporativo e multifuncional marca paloalto modelo 3050 (2 equipamentos em cluster), incluindo assinaturas de filtro url e threat prevention por um período de 48 meses, com repasse de conhecimento da solução, pelo valor global de R$ _____,___ (**VALOR TOTAL POR EXTENSO, EM REAIS),** ordo com a planilha de preços em anexo, que é parte integrante desta proposta.

Comprometendo-nos, se nossa proposta for aceita, a executar os serviços no prazo fixado no Edital e conforme Especificações Técnicas, a contar da data de emissão da(s) Nota(s) de Empenho pela Codevasf. Caso nossa proposta seja aceita, obteremos garantia de um Banco num valor que não exceda 5% (cinco por cento) do valor do Contrato, para a realização do contrato.

Nos preços cotados, deverá estar incluso o transporte (frete) para o material objeto desta licitação.

Comprometendo-nos, se nossa proposta for aceita, a realizar o serviço durante o prazo de 3 (três) anos, a contar da data de assinatura do Contrato.

Concordamos em manter a validade desta proposta por um período de 60 (sessenta) dias desde a data fixada para abertura das propostas (xxxxxxx), representando um compromisso que pode ser aceito a qualquer tempo antes da expiração do prazo.

Até que seja preparado e assinado um contrato formal, esta proposta, será considerada um contrato de obrigação entre as partes.

Na oportunidade, credenciamos junto à Codevasf o(a) Sr.(ª) _____, carteira de Identidade n.º _____, Órgão Expedidor _____, CPF n.º_____,

residente e domiciliado(a) na rua_____, n.º_____, bairro_____, na cidade de_____, Estado de_____, ao(à) qual outorgamos os mais amplos poderes inclusive para interpor recursos, quando cabíveis transigir, desistir, assinar contratos, atas e documentos, enfim, praticar os demais atos no presente processo licitatório.

Declaramos que temos pleno conhecimento de todos os aspectos relativos à licitação em causa e que nossa proposta compreende a integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal e nas leis trabalhistas, normas infralegais, convenções coletivas de trabalho que não serão transferidos à Codevasf a responsabilidade por seu pagamento, bem como dos encargos fiscais e comerciais.

Declaramos, ainda, nossa plena concordância com as condições constantes no presente Edital e seus anexos e que em nossa proposta estão incluídas todas as despesas, inclusive aquelas relativas a taxas, tributos, encargos sociais, ensaios, testes e demais provas exigidas por normas técnicas oficiais e demais e despesas, de qualquer natureza, incidentes sobre o fornecimento.

Atenciosamente,

_____
FIRMA LICITANTE/CNPJ

_____
ASSINATURA DO REPRESENTANTE LEGAL

ANEXO III

MINUTA DE CONTRATO

ANEXO IV
TERMO DE OBSERVÂNCIA AO CÓDIGO DE CONDUTA ÉTICA E INTEGRIDADE DA CODEVASF

MINISTÉRIO DO DESENVOLVIMENTO REGIONAL - MDR
COMPANHIA DE DESENVOLVIMENTO DOS VALES DO SÃO FRANCISCO E DO PARNAÍBA

Termo de Observância ao Código de Conduta Ética e Integridade da Codevasf

Nº do Instrumento: (Informar contrato, convênio ou instrumento congênere.)

Período de Vigência do Instrumento: (Informar Período.)

Finalidade do Instrumento: (Informar finalidade.)

A pessoa física/jurídica , CPF/CNPJ nº , por meio de seu representante legal abaixo subscrito, vem afirmar aderência, ciência e concordância com as normas, políticas e práticas estabelecidas no Código de Conduta Ética e Integridade da Codevasf e compromete-se a respeitá-las e cumpri-las integralmente, bem como fazer com que seus empregados o façam quando no exercício de suas atividades nas dependências da Codevasf ou para a Empresa.

Compreendo que o Código de Conduta Ética e Integridade da Codevasf reflete o compromisso com a dignidade, o decoro, o zelo, a eficácia e a consciência dos princípios morais que devem nortear o serviço público, seja no exercício do cargo em comissão, função de confiança ou gratificada ou emprego, ou fora dele, comprometendo-se a atuar contrariamente a quaisquer manifestações de corrupção e conhecer e cumprir as normas previstas na Lei 12.846/2013 ("Lei Anticorrupção"), regulamentada pelo Decreto 8.420/2015.

Assumo, também, a responsabilidade de denunciar à Ouvidoria e/ou Comissão de Ética da Codevasf sobre qualquer comportamento ou situação que esteja em desacordo com as disposições do Código de Conduta Ética e Integridade da Codevasf, por meio dos seguintes canais:

- Ouvidoria da Codevasf: https://sistema.ouvidorias.gov.br
- Comissão de Ética da Codevasf: etica@codevasf.gov.br.

A assinatura deste Termo é expressão de livre consentimento e concordância do cumprimento das normas, políticas e práticas estabelecidas no Código de Conduta Ética e Integridade da Codevasf.

(Informar o local.) , (Dia.) de (Mês.) de (Ano.)

_____

Assinatura / carimbo do responsável/representante legal

Nome completo:

CPF:

Cargo:

ANEXO V – CÓDIGO DE CONDUTA ÉTICA E INTEGRIDADE DA CODEVASF

(Gravado em arquivo separado)

TERMO DE REFERÊNCIA

CONTRATAÇÃO DE EMPRESA ESPECIALIZADA PARA FORNECIMENTO DE SERVIÇO DE SUPORTE TÉCNICO 24x7 ON-SITE OU PRESENCIAL, MANUTENÇÃO TÉCNICA, GARANTIA DE ATUALIZAÇÃO, GARANTIA DE HARDWARE, TREINAMENTO E REPASSE DE CONHECIMENTO PARA A SOLUÇÃO *FIREWALL* CORPORATIVO E MULTIFUNCIONAL MARCA PALOALTO MODELO 3050. INCLUINDO ASSINATURAS DE FILTRO URL E THREAT PREVENTION POR UM PERÍODO DE 48 MESES.

ÍNDICE

TERMINOLOGIAS E DEFINIÇÕES

Neste Termo de Referência (TR) ou em quaisquer outros documentos relacionados com os serviços acima solicitados, os termos ou expressões têm o seguinte significado e/ou interpretação:

AE/GTI ou GTI – Gerencia de Tecnologia da Informação da Área de Gestão Estratégica da CODEVASF.

AE/GTI/UIT ou UIT – Unidade de Infraestrutura e Tecnologia, subordinada a Gerência de Tecnologia da Informação.

CODEVASF – Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba – Empresa pública vinculada ao Ministério da Integração Nacional, com sede no Setor de Grandes Áreas Norte, Quadra 601 – Lote 1 – Brasília-DF.

CONTRATADA – Empresa licitante selecionada e contratada pela CODEVASF para a execução dos serviços.

CONTRATO – Documento, subscrito pela CODEVASF e a CONTRATADA do certame, que define as obrigações e direitos de ambas com relação à execução dos serviços.

DOCUMENTOS DE CONTRATO – Conjunto de todos os documentos que integram o contrato e regulam a execução dos serviços, compreendendo o Edital, Termo de Referência, especificações técnicas, desenhos e proposta financeira da executante, cronogramas e demais documentos complementares que se façam necessários à execução dos serviços.

DOCUMENTOS COMPLEMENTARES ou SUPLEMENTARES – Documentos que, por força de condições técnicas imprevisíveis, se fizerem necessários para a complementação ou suplementação dos documentos emitidos nos Termo de Referência.

ESPECIFICAÇÃO TÉCNICA – Tipo de norma destinada a fixar as características dos serviços e fornecimentos, condições ou requisitos exigíveis para matérias primas, produtos semifabricados, elementos de construção, materiais ou produtos industriais semifabricados. Conterá a definição do serviço e fornecimentos, descrição do método construtivo, controle tecnológico e geométrico e norma de medição e pagamento.

FISCAL/GESTOR – Técnico(os) responsável(is) da Codevasf atuando sob a autoridade do Diretor da respectiva área e presidente para exercer a gestão e fiscalização do contrato no âmbito administrativo e técnico, bem como manter o contato direto com a CONTRATADA para dirimir dúvidas.

FISCALIZAÇÃO – Equipe da CODEVASF atuando sob a autoridade de um Coordenador/fiscal/gestor, indicada para exercer e auxiliar em sua representação a fiscalização do contrato.

LICITANTE – Empresa habilitada para apresentar proposta.

PDTI: Plano Diretor de Tecnologia da Informação é resultado do detalhamento das ações decorrentes do Planejamento Estratégico da Tecnologia da Informação - PETI, de forma a consolidar todas as iniciativas, metas e os indicadores da área de Tecnologia da Informação, dando visibilidade às ações, prazos e custos necessários para alcance dos objetivos estratégicos definidos e, ainda, assegurando que estas ações agreguem valor ao negócio da Codevasf.

PETI: Plano Estratégico de Tecnologia da Informação é o instrumento que tem por objetivo assegurar que as metas e objetivos da TI estejam fortemente alinhados com o Planejamento Estratégico da Codevasf.

PROPOSTA FINANCEIRA – Documento gerado pelo licitante que estabelece os valores unitário e global dos serviços e fornecimentos, apresentando todo o detalhamento dos custos e preços unitários propostos.

SIASG - é um conjunto informatizado de ferramentas para operacionalizar internamente o funcionamento sistêmico das atividades de gestão de materiais, edificações públicas, veículos oficiais, comunicações administrativas, licitações e contratos. É utilizado por várias entidades da Administração Pública Federal (Ministérios, Secretarias, etc.). Pode ser acessado pelo site do Compras Governamentais: **www.comprasgovernamentais.gov.br**.

TERMO DE REFERÊNCIA – Conjunto de elementos necessários e suficientes, com nível de precisão adequado, para caracterizar os bens a serem fornecidos, capazes de propiciar avaliação do custo pela administração diante de orçamento detalhado, definição dos métodos, estratégia de suprimento, valor estimado em planilhas de acordo com o preço de mercado, cronograma físico-financeiro, se for o caso, critério de aceitação do objeto, deveres do contratado e do contratante, procedimentos de fiscalização e gerenciamento do contrato, prazo de execução e sanções, de forma clara, concisa e objetiva.

1. OBJETO DA CONTRATAÇÃO

O presente Termo de Referência tem por objeto a contratação de empresa especializada para fornecimento de serviço de suporte técnico 24x7 on-site ou presencial, manutenção técnica, garantia de atualização, garantia de hardware, treinamento e repasse de conhecimento para a solução *firewall* corporativo e multifuncional marca paloalto modelo 3050 (2 equipamentos em cluster). incluindo assinaturas de filtro url e threat prevention por um período de 48 meses, com repasse de conhecimento da solução. Conforme condições, quantidades, exigências estabelecidas neste Termo de Referência e seus anexos.

1.1. Grupo 1 - DESCRIÇÃO

Item	DESCRIÇÃO	UN	QT	Valor unit. (R$)	Valor Total (R$)
01	Fornecimento de subscrição para atualização da garantia das licenças de uso – PA-3050 – Threat Prevention e URL Filtering pelo período de 48 (quarenta e oito) meses, válido para 02 (dois) appliances da Palo Alto Networks, incluindo suporte técnico especializado telefônico, remoto e on-site 24x7, de acordo com as especificações. Ver **anexo A**	unit	2	R$ 712.818,08	R$ 1.425.636,16
02	Suporte técnico especializado telefônico, remoto e on-site para os equipamentos e licenças da Palo Alto PA-3050 por um período de **48 meses**. **Ver anexo A**	meses	48	R$ 10.791,27	R$ 517.980,96
03	Treinamento e repasse de conhecimento. **Ver anexo A**	turma	1	R$ 17.329,28	R$ 17.329,28

1.1.1. O custo estimado total informado na tabela acima, R$ 1.960.946,40 (um milhão, novecentos e sessenta mil, novecentos e quarenta e seis reais e quarenta centavos), foi apurado com base em pesquisa de mercado, na Instrução Normativa Nº 73 de 5 de agosto de 2020, e painel de preços do portal de compras do Governo Federal.

1.1.2. Os recursos orçamentários correrão à conta do Programa de Trabalho 04.122.0032.2000.0001 - ADMINISTRAÇÃO DA UNIDADE - NACIONAL, Categorias Econômica 3 sob a gestão das Áreas de Gestão Estratégica da Codevasf – AE.

1.1.3. Os quantitativos foram estimados pela AE/GTI/UGT e estão demonstrados nos autos do processo desta contratação.

1.1.4. O valor corresponde à média dos preços pesquisados e praticados no mercado.

1.1.5. Os elementos técnicos descritos neste instrumento e em seus anexos são os mínimos necessários para assegurar que a contratação se dê de forma satisfatória com as mínimas condições técnicas e de qualidade exigidas, e ainda, assegurar o gasto racional dos recursos públicos.

1.1.6. Por acordo entre as partes, o objeto do Contrato poderá ser suprimido ou aumentado até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado da contratação, facultada a supressão além desse limite, por acordo entre as partes, conforme disposto no art. 81, inciso VI, § 1º, da Lei nº 13.303/16.

2. CRITÉRIO DE JULGAMENTO

2.1. **Critério de Julgamento:** Menor preço por grupo

2.2. **MODO DE DISPUTA: ABERTO,** com intervalo mínimo de diferença entre os lances de 0,5 % (meio por cento), do valor do item pertinente, que incidirá tanto em relação aos lances intermediários quanto e relação ao lance que cobrir a melhor oferta.

2.3. **Valor estimado:** Público.

3. OBJETIVO DA CONTRATAÇÃO

3.1. Garantir o acesso ao ambiente dos recursos de rede e computadores somente a pessoas autorizadas, controlar as aplicações acessadas pelos usuários da rede e manter o acesso à rede de dados da Codevasf por meio da Virtual Private Network (VPN) possibilitando assim o trabalho remoto.

4. CLASSIFICAÇÃO DOS SERVIÇOS

4.1. Nos termos do inciso II, do art. 3º, do Decreto 10.024, de 2019, os serviços objeto deste instrumento são considerados comuns, pois seus padrões de desempenho e qualidade, para efeito de julgamento das propostas, podem ser objetivamente definidos neste Termo de Referência e no Edital, por meio de especificações usuais de mercado.

4.2. 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.

5. FORMA DE PRESTAÇÃO DOS SERVIÇOS

5.1. Os serviços a serem executados são de 3 (três) tipos: “ATUALIZAÇÃO DO LICENCIAMENTO”, “MANUTENÇÃO E SUPORTE” e “TREINAMENTO” conforme detalhado no **Anexo A** – Especificação Técnica dos Serviços.

5.2. LOCAL DE EXECUÇÃO DOS SERVIÇOS

5.2.a.1. Os serviços serão executados preferencialmente remotamente, e só em casos de não solução do problema, serão executados presencialmente.

5.2.a.2. Os serviços presenciais serão executados nas dependências da CONTRATANTE, por decisão unilateral da CONTRATANTE. O endereço para execução dos serviços indicado é:

UNIDADE	Endereço
Sede (Brasília – DF)	SGAN 601, Conj. I – Ed. Manoel Novaes.

5.2.a.3. No caso dos serviços prestados nas dependências da Codevasf e durante sua execução, o prestador de serviço da CONTRATADA deverá estar identificado por crachá da CONTRATADA e acompanhado por empregado da Unidade de Infraestrutura e Tecnologia da CONTRATANTE.

5.2.a.4. Os custos relacionados aos deslocamentos, ocorridos em função de entendimento, validação e/ou aceite dos serviços, serão por conta da CONTRATADA.

6. CONDIÇÕES DE PARTICIPAÇÃO

6.1. Poderão participar da presente licitação empresas do ramo, pertinente e compatível com o objeto desta licitação, nacionais ou estrangeiras, que atendam às exigências do TR e seus anexos.

a. As Empresas estrangeiras poderão participar nas mesmas condições das empresas nacionais.

b. As propostas serão aceitas somente para todos os itens do grupo que a licitante esteja concorrendo, discriminados no item 1.1 - Grupo 1 - DESCRIÇÃO deste Termo de Referência. Não serão aceitas propostas para itens isolados, implicando na desclassificação da proposta.

7. SEGURANÇA DA INFORMAÇÃO

7.1. Os procedimentos mínimos de segurança exigidos da empresa contratada são:

a. Credenciar junto a CONTRATANTE, seus profissionais autorizados a retirar e a entregar documentos, bem como daqueles que venham a ser designados para prestar serviços nas dependências da CODEVASF.

b. Identificar qualquer equipamento das empresas que venha a ser instalado nas dependências da CONTRATANTE, utilizando placas de controle patrimonial, selos de segurança, etc.

c. Manter sigilo absoluto sobre informações, dados e documentos integrantes dos serviços a serem executados na CONTRATANTE.

d. Abster-se, qualquer que seja a hipótese, de veicular publicidade ou qualquer outra informação acerca das atividades objeto do Termo de referência, sem prévia autorização.

e. Observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação - TI da CODEVASF.

f. Adotar critérios adequados para o processo seletivo dos profissionais, com o propósito de evitar a incorporação de pessoas com características e/ou antecedentes que possam comprometer a segurança ou credibilidade da CONTRATANTE.

g. Comunicar com antecedência mínima de 3 (três) dias ao Representante da CONTRATANTE qualquer ocorrência de transferência, remanejamento ou demissão, para que seja providenciada a revogação de todos os privilégios de acesso aos sistemas, informações e recursos da empresa.

h. Manter sigilo sobre todos os ativos de informações e de processos da CONTRATANTE.

7.2. Adotar a Política de Segurança da Informação e Comunicações da Codevasf (Posic), publicada no sítio da empresa, para o exercício de suas atividades no âmbito da Codevasf.

7.3. A Contratada deve firmar aderência, ciência e concordância com as normas, políticas e práticas estabelecidas no Código de Conduta Ética e Integridade da Codevasf e compromete-se a respeitá-las e cumpri-las integralmente, bem como fazer com que seus empregados o façam quando no exercício de suas atividades nas dependências da Codevasf ou para a Empresa.

8. PROPRIEDADE INTELECTUAL

8.1. A CONTRATADA fica proibida de veicular e comercializar os produtos gerados relativos ao objeto da prestação dos serviços, salvo se houver a prévia autorização por escrito da CONTRATANTE.

9. MODELO DE GESTÃO DO CONTRATO E CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

9.1. Garantia e Suporte

9.1.a.1. Os chamados poderão ser abertos diretamente com o fabricante por ligação telefônica, e-mail e/ou site durante a vigência da garantia (48 meses).

9.1.a.2. O suporte deverá ser na modalidade 24x7 (24 horas por dia, 7 dias por semana), com atendimento através de ligações telefônicas para atendimentos emergenciais.

9.1.a.3. A CONTRATADA, a partir da data de formalização de recebimento da abertura do chamado, terá, para o atendimento destes chamados suas regras, prazos e penalidades previstas **no Anexo A itens: 7. SUPORTE TÉCNICO ESPECIALIZADO; e 8. NÍVEIS MÍNIMOS DE SERVIÇO**

b. A CONTRATANTE pode solicitar a presença da CONTRATADA para disponibilizar, instalar e acompanhar os produtos entregue no ambiente de produção.

c. Para os serviços de manutenção corretiva a CONTRATADA deverá atualizar as mudanças efetuadas na documentação existente, não estando obrigada a elaborar novos artefatos de documentação.

d. As não-conformidades identificadas durante a homologação e implantação dos artefatos resultantes do serviço serão corrigidas pela CONTRATADA, sem ônus para a CONTRATANTE.

9.2. Condições de entrega

9.2.1. O prazo de entrega dos produtos deverá ocorrer em até no máximo 90 (noventa) dias corridos a partir da data de assinatura do contrato.

9.2.2. A entrega deve ser agendada com antecedência mínima de 24 horas, sob o risco de não ser autorizada;

9.2.3. Para itens de software, poderá ser fornecido sem mídia de instalação, desde que seja indicado local para download do arquivo de instalação.

9.3. Pagamento

9.3.1. Todos os serviços ora contratados serão cobrados por meio de faturas/notas fiscais emitidas pela CONTRATADA, e pagas em até 30 (trinta) dias, mediante apresentação das faturas/notas fiscais devidamente atestadas pela Fiscalização, conforme disposto no Artigo 9º, do Decreto nº 1.054, de 7 de fevereiro de 1994, sendo efetuada a retenção na fonte dos tributos e contribuições elencados na legislação aplicável.

9.3.2. A fatura só será liberada para pagamento depois de aprovada pelo fiscal do contrato e deverá estar isenta de erros ou omissões, sem o que será, de forma imediata, devolvida à CONTRATADA para correções.

9.3.3. Na hipótese de irregularidade no cadastro ou habilitação no SICAF, o CONTRATADO deverá regularizar a sua situação perante o cadastro no prazo de até 30 (trinta) dias, sob pena de aplicação das penalidades previstas no edital, anexo(s) e rescisão do contrato.

9.3.4. Qualquer atraso acarretado por parte da CONTRATADA na apresentação da fatura ou nota fiscal, ou dos documentos exigidos como condição para pagamento, importará na interrupção da contagem do prazo de vencimento do pagamento, iniciando novo prazo após a regularização da situação

9.3.5. A fatura emitida pela CONTRATADA deverá conter a descrição dos serviços a que se destina e seu valor em moeda corrente (reais) sem indexação ao valor do dólar.

9.3.6. O pagamento será procedido de consulta ao SICAF, para comprovação de cumprimento das obrigações trabalhistas, previdenciárias e as relativas ao FGTS, correspondentes à última nota fiscal ou fatura que tenha sido paga pela CONTRATANTE.

9.3.7. O pagamento será creditado em nome da CONTRATADA, mediante Ordem Bancária em conta corrente por ela indicada ou meio de Ordem Bancária para pagamento de fatura com código de barras, uma vez satisfeitas as condições estabelecidas neste Termo de Referência.

9.3.8. A Nota Fiscal/Fatura deverá destacar o valor do IRPJ e demais contribuições incidentes, para fins de retenção na fonte, de acordo com o art. 2º, § 6º da IN/SRF n.º 1234/2012, ou informar a isenção, não incidência ou alíquota zero, e respectivo enquadramento legal, sob pena de retenção do imposto de renda e das contribuições sobre o valor total do documento fiscal, no percentual correspondente à natureza do bem.

9.3.9. É de inteira responsabilidade da CONTRATADA a entrega à CONTRATANTE dos documentos de cobrança, acompanhados dos seus respectivos anexos, de forma clara, objetiva e ordenada, que se não for atendido, implica desconsideração pela CONTRATANTE dos prazos estabelecidos para conferência e pagamento.

9.3.10. Caso a CONTRATADA seja optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte – SIMPLES, deverá apresentar, juntamente com a Nota Fiscal, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições, conforme legislação em vigor.

9.3.11. Os valores referentes ao licenciamento dos produtos e as aquisições serão pagos em parcela única, após a ativação das licenças, atesto dos serviços, se for o caso, e da fatura pelo representante da CONTRATANTE, em moeda corrente nacional, em até 30 dias após o recebimento da fatura.

9.3.12. É vedado ao contratado transferir a terceiros os direitos ou créditos decorrentes do contrato.

9.3.13. Será considerado em atraso o pagamento efetuado após o prazo estabelecido no subitem 7.3.1, caso em que a CONTRATANTE pagará atualização financeira, aplicando-se a seguinte fórmula:

AM = P x I, onde:

AM = Atualização Monetária

P = Valor da Parcela a ser paga; e

I = Percentual de atualização monetária, assim apurado:

I = $\left(1 + {}^{I_{m1}}/_{100}\right) * d\ x^{1/30}$ * $\left(1 + {}^{I_{m2}}/_{100}\right) * d\ x^{2/30}$ * ... * $\left(1 + {}^{I_{mn}}/_{100}\right) * d\ x^{n/30}$ – 1, onde:

i = Variação do Índice de Custos de Tecnologia da Informação - ICTI no mês "m";

d = Número de dias em atraso no mês "m";

m = Meses considerados para o cálculo da atualização monetária.

9.4. Reajustamento

9.4.1. O preço é fixo e irreajustável pelo período de 12 meses, após a assinatura do instrumento contratual. Após esse prazo, poderá ser reajustado a contar da data de apresentação da proposta, mediante manifestação expressa da CONTRATADA, tendo como limite máximo a variação do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, conforme fórmula abaixo. O reajuste calculado deverá ser encaminhado a CONTRATANTE para análise e posterior aprovação.

$$IR = \frac{I_{1\ \text{mês renovação}} - I_{0\ \text{mês base}}}{I_{0\ \text{mês base}}} \times 100$$, onde:

IR corresponde ao índice de reajustamento;

$I_{1\ \text{mês renovação}}$ corresponde ao valor do ICTI referente ao mês de renovação;

$I_{0\ \text{mês base}}$ corresponde ao valor do ICTI referente a data de apresentação da proposta.

10. VIGÊNCIA DO CONTRATO

10.1. O prazo de vigência do contrato, a ser firmado entre a CONTRATANTE e a CONTRATADA, será de acordo com a proposta vencedora observando o prazo máximo de 48 meses, improrrogáveis, para sua conclusão e terá início na data de sua assinatura.

10.2. Os contratos terão vigência na data de suas assinaturas, com prazo para início da execução dos serviços imediatamente após a assinatura do contrato.

11. VISTORIA

11.1. As empresas interessadas na consecução dos serviços constantes no objeto deste Termo de referência poderão realizar visita técnica na cidade de Brasília/DF, no Edifício Sede da CODEVASF localizado no endereço: SGAN Quadra 601, Conjunto I, Lote 01, Edifício CODEVASF, CEP: 70.830-901, em Brasília-DF;

11.2. O período estabelecido para a visita técnica terá início a partir da data de publicação do edital no Diário Oficial da União - DOU. A visita técnica deverá ser programada com antecedência mínima de 1 (um) dia útil junto à Unidade de Infraestrutura e Tecnologia por meio do e-mail ae.gti.uit@codevasf.gov.br.

11.3. A visita técnica tem a finalidade de prover ao licitante conhecimento das instalações, metodologias, arquiteturas e recursos do ambiente da CONTRATANTE para que o mesmo tenha condições de avaliar o grau de dificuldade existentes na execução dos serviços, constantes no objeto do termo de referência que possam influenciar nos custos envolvidos no fornecimento do serviço;

11.4. Os custos da vistoria são de responsabilidade da licitante, incluindo seu deslocamento ao local vistoriado.

11.5. As licitantes se obrigam a não divulgar, publicar ou fazer uso das informações recebidas durante a vistoria. A simples participação na vistoria caracteriza o compromisso irretratável de guarda do sigilo dos dados colhidos.

11.6. Não tendo realizada a vistoria, a licitante não poderá arguir desconhecimento dos processos, procedimentos, ambientes e das ferramentas utilizadas pela CONTRATANTE para se opor à manutenção dos termos e das condições de sua proposta.

11.7. Nenhuma visita será realizada sem a confirmação de seu agendamento, por e-mail, por parte da CONTRATANTE.

11.8. A vistoria é FACULTATIVA, podendo a licitante realizá-la por intermédio de representante legal.

11.9. Para a vistoria, o licitante, ou o seu representante, deverá estar devidamente identificado, e assinará a declaração de vistoria.

12. QUALIFICAÇÃO TÉCNICA

12.1. Atestado(s) de qualificação técnica emitido em nome da licitante, expedido por pessoa(s) jurídica(s) de direito público ou privado, que comprove que a CONTRATADA presta ou prestou serviços identificados a seguir no item (12.2) para o desempenho de atividade pertinente e compatível em características com o objeto do Termo de Referência, conforme inciso II do art. 58 da Lei nº 13.303/16.

12.2. Atestado(s) de qualificação técnica emitido em nome da licitante, expedido pela fabricante do produto para Manutenção e Suporte Técnico especificamente para esta licitação, que comprove que a CONTRATADA possui capacidade técnica para prestação de serviços no produto licenciado: solução *firewall* corporativo e multifuncional marca paloalto modelo 3050, conforme inciso II do art. 58 da Lei nº 13.303/16.

13. OBRIGAÇÕES DA CONTRATADA

13.1. Executar os serviços conforme especificações deste termo de referência, anexos e de sua proposta;

13.2. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação;

13.3. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

13.4. Prover e gerir infraestrutura própria de hardware e software, bem como recursos físicos necessários à execução dos serviços contratados, no caso em que os serviços sejam prestados nas dependências da CONTRATADA. Entende-se por infraestrutura de hardware e software, todo hardware e licenças dos softwares necessários para a realização do serviço;

13.5. Solicitar autorização prévia da CONTRATANTE antes de utilizar recursos de softwares que necessitem de aquisição de licença de uso;

13.6. Solicitar autorização prévia da CONTRATANTE para incorporar, nos serviços entregues, componentes de software que não sejam de propriedade da CONTRATANTE;

13.7. Utilizar recursos de terceiros somente quando devidamente autorizados ou licenciados pelo detentor dos direitos;

13.8. Garantir que todas as entregas efetuadas estejam compatíveis e totalmente aderentes aos produtos utilizados pela CONTRATANTE, cabendo à CONTRATANTE tomar ciência e autorizar o uso de ferramentas, cuja versão seja diferente daquelas previstas e em uso na empresa;

13.9. Adotar procedimentos no seu ambiente que garantam a segurança das informações e a continuidade das operações, em conformidade com os parâmetros da NBR-ISO/IEC 17.799, e manter documentação atualizada de sua Política de Segurança de Informações.

13.10. Promover o repasse de conhecimento aos novos profissionais da CONTRATADA, em caso de substituição dos responsáveis pela execução de serviços em andamento, evitando o prejuízo à continuidade e qualidade dos serviços;

13.11. Repassar todo o conhecimento adquirido ou produzido na execução dos serviços para os técnicos da CONTRATANTE;

13.12. Assegurar a transferência de conhecimentos adquiridos ou produzidos, relativamente a serviços em andamento, para outra CONTRATADA da CONTRATANTE, nos termos que venham a ser por este definido, no caso em que a CONTRATANTE determine a passagem de serviços em andamento, a fim de garantir a continuidade dos serviços;

13.13. Prestar as informações e esclarecimentos solicitados, em no máximo 2 (dois) dias úteis, a contar da solicitação feita pelo fiscal ou gestor do contrato.

13.14. Selecionar e alocar, na prestação dos serviços contratados, profissionais em conformidade com as exigências dos serviços a serem realizados, e com os perfis adequados.

13.15. Afirmar aderência, ciência e concordância com as normas, políticas e práticas estabelecidas no Código de Conduta Ética e Integridade da Codevasf e compromete-se a respeitá-las e cumpri-las integralmente, bem como fazer com que seus empregados o façam quando no exercício de suas atividades nas dependências da Codevasf ou para a Empresa.

13.16. Reportar à Gerência de Tecnologia da Informação da CONTRATANTE quaisquer anormalidades, erros e irregularidades observados no desenvolvimento dos serviços contratados, causados por ações dos profissionais contratados, de servidores públicos ou de terceiros.

13.17. Responsabilizar-se pelos danos causados diretamente à CONTRATANTE ou a terceiros decorrentes de sua culpa ou dolo quando da execução dos serviços, não excluindo ou reduzindo essa responsabilidade à fiscalização e/ou ao acompanhamento realizados pela CONTRATANTE.

13.18. Indenizar os prejuízos e reparar os danos causados à CONTRATANTE e a terceiros por seus profissionais na execução do contrato.

13.19. Os dados, artefatos, códigos, softwares e informações da organização não poderão ser distribuídos, divulgados e comercializados pela CONTRATADA.

13.20. Todo conhecimento adquirido ou desenvolvido, bem como toda informação produzida e/ou utilizada para a execução dos serviços contratados deverão ser disponibilizados e transferidos à CONTRATANTE.

14. OBRIGAÇÕES DA CONTRATANTE

14.1. Exercer o efetivo acompanhamento da execução do contrato.

14.2. Prestar informações, esclarecimentos necessários e proporcionar condições – no que lhe couber - para que a CONTRATADA possa executar os serviços objeto do Contrato.

14.3. Homologar o serviço prestado, após a aferição da aderência às especificações presentes neste termo de referência, atestando as respectivas faturas.

14.4. Notificar, por escrito, a CONTRATADA a ocorrência de eventuais não conformidades no curso da execução dos serviços, fixando prazo para sua correção.

14.5. Exigir o cumprimento de todas as obrigações assumidas pela CONTRATADA, de acordo com as cláusulas contratuais e os termos de sua proposta.

15. CONSÓRCIO

15.1. Não será permitida a participação de consórcio.

16. SUBCONTRATAÇÃO

16.1. Não será admitida a subcontratação do objeto licitatório.

17. PROPOSTA FINANCEIRA

17.1. As propostas financeiras deverão conter no mínimo o seguinte:

a. Planilha de preços unitários (Proposta) e totais ofertados para os itens, devidamente preenchida, com clareza e sem rasuras, conforme modelo constante do Anexo C, que é parte integrante deste termo de Referência.
b. O prazo de validade da proposta será de 60 (sessenta) dias contados a partir da data estabelecida para entrega das mesmas, sujeita a revalidação por idêntico período.

17.2. Nos preços unitários propostos, deverão estar incluídos todos os custos que venham a incidir, direta ou indiretamente, nos fornecimentos objeto deste Termo de Referência.

17.3. Será considerada a melhor proposta, a que apresentar o menor preço global avaliado para o grupo, conforme critérios acima estabelecidos.

18. ALTERAÇÃO SUBJETIVA

18.1. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

19. CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO

19.1. A execução dos Contratos será fiscalizada por Representante da CODEVASF, especialmente designado, cumprindo-lhe:

a. Registrar as ocorrências relacionadas com a execução dos serviços, determinando junto à empresa CONTRATADA o que for necessário à regularização das falhas ou defeitos observados.

b. Analisar todos os documentos exigidos para o devido atesto das Notas Fiscais de Serviços ou Faturas referente aos serviços realizados pela empresa CONTRATADA.

c. Encaminhar à unidade responsável o(s) eventual(ais) recurso(s) da empresa CONTRATADA, acerca da aplicação de penalidades, com vistas à sua apreciação.

19.2. A CONTRATANTE poderá exigir o afastamento de qualquer profissional ou representante da empresa CONTRATADA que venha causar embaraço à fiscalização do contrato, ou em razão de procedimentos ou atitudes incompatíveis com o exercício de suas funções.

19.3. As atividades de gestão e fiscalização da execução contratual são o conjunto de ações que tem por objetivo aferir o cumprimento dos resultados previstos pela Administração para o serviço contratado, verificar a regularidade das obrigações previdenciárias, fiscais e trabalhistas, bem como prestar apoio à instrução processual e o encaminhamento da documentação pertinente ao setor de contratos para a formalização dos procedimentos relativos a repactuação, alteração, reequilíbrio, prorrogação, pagamento, eventual aplicação de sanções, extinção do contrato, dentre outras, com vista a assegurar o cumprimento das cláusulas avençadas e a solução de problemas relativos ao objeto.

19.4. As atividades de gestão e fiscalização da execução contratual devem 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.

19.5. A fiscalização administrativa poderá ser efetivada com base em critérios estatísticos, levando-se em consideração falhas que impactem o contrato como um todo e não apenas erros e falhas eventuais no pagamento de alguma vantagem a um determinado empregado.

19.6. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da CONTRATANTE ou de seus agentes, gestores e fiscais.

19.7. Fica reservado à fiscalização e à Gerência de Tecnologia da Informação o direito e a autoridade para solucionar todo e qualquer caso singular não previsto neste termo que se relacione com o objeto licitado, desde que não acarrete ônus para a Codevasf ou modificação na contratação.

19.8. A ação e/ou omissão, total ou parcial, da Fiscalização não eximirá a CONTRATADA da integral responsabilidade pela execução do objeto deste contrato.

20. MULTAS

20.1. Por descumprimento das obrigações contratuais ou desrespeito às exigências do Edital a CONTRATANTE aplicará, garantida a prévia defesa, multa e seguintes sanções ao contratado:

a) 0,3% (zero vírgula três por cento) por dia de atraso injustificado na entrega do produto e por descumprimento das obrigações estabelecidas no item 9.2.1, até o máximo de 10% (dez por cento) sobre o valor total do valor a ser contratado;

b) 20% (vinte por cento) sobre o valor total do Contrato, no caso de inexecução total e 10% (dez por cento) sobre o valor total do Contrato, no caso de inexecução parcial do objeto adquirido;

c) Suspensão temporária de participação em licitação e impedimento de contratar com a Administração, por prazo não superior a 02 (dois) anos;

20.2. Se a multa aplicada for superior ao valor da garantia prestada, além da perda desta, responderá o contratado pela sua diferença, que será descontada dos pagamentos eventualmente devidos pela Administração; caso o valor do faturamento seja insuficiente para cobrir a multa, a licitante será convocada para complementar o valor devido no prazo de 05 (cinco) dias úteis a contar da data da convocação ou será cobrada judicialmente;

20.3. A CONTRATADA terá um prazo de 10 (dez) dias corridos, contado a partir da data do conhecimento da aplicação da multa, para defesa prévia e, posteriormente, após eventual decisão que lhe tenha sido desfavorável, mais um prazo de 05 (cinco) dias úteis, para apresentar recurso à CODEVASF. Ouvido o fiscal designado para o acompanhamento do contrato, o recurso será encaminhado à Assessoria Jurídica e apreciado pela autoridade competente, que poderá relevar ou não a multa.

a. Após o procedimento estabelecido no item anterior, o recurso será apreciado pela Diretoria Executiva da CODEVASF, que poderá relevar ou não a multa.

20.4. Em caso de relevação da multa, a CODEVASF se reserva o direito de cobrar perdas e danos porventura cabíveis em razão do inadimplemento de outras obrigações, não constituindo a relevação renovação contratual nem desistência dos direitos que lhe forem assegurados.

Caso a Diretoria Executiva mantenha a multa, não caberá novo recurso administrativo.

21. GARANTIA DE EXECUÇÃO DO CONTRATO

21.1. Para a contratação, será exigida uma prestação de garantia correspondente a 5% (cinco por cento) do valor da contratação, a fim de assegurar a sua execução, em uma das modalidades previstas no art. 70 da Lei nº 13.303/16, à sua escolha.

21.2. A CONTRATANTE poderá utilizar o valor da garantia prestada para descontar os valores referentes a eventuais multas e glosas aplicadas à CONTRATADA, bem como nos casos decorrentes de inadimplemento contratual, e de indenização por danos causados ao Patrimônio da União ou de terceiros, ocorridos nas suas dependências.

21.3. A garantia de execução somente será restituída pela CONTRATANTE após cumprimento integral de todas as obrigações contratuais assumidas.

22. CRITÉRIOS DE SUSTENTABILIDADE AMBIENTAL

22.1. A licitante vencedora deverá observar os seguintes critérios de sustentabilidade ambiental, no que couber, conforme a instrução normativa SLTI/MP nº 01/2010:

a. Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2;
b. Que sejam observados os requisitos ambientais para a obtenção de certificação do Instituto Nacional de Metrologia, Normalização e Qualidade Industrial – INMETRO como produtos sustentáveis ou de menor impacto ambiental em relação aos seus similares;
c. Que os bens devam ser, preferencialmente, acondicionados em embalagem adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento;
d. Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva RoHS (Restriction of Certain Hazardous Substances), tais como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenil-polibromados (PBBs), éteres difenil-polibromados (PBDEs).

A licitante vencedora deverá apresentar certificação emitida por instituição pública oficial ou instituição credenciada, ou por qualquer outro meio de prova que ateste que o bem fornecido cumpre com as exigências supracitadas. Em caso de inexistência de certificação que ateste a adequação, a Codevasf poderá realizar diligências para verificar a adequação do produto às exigências deste TR, antes da assinatura do contrato, correndo as despesas por conta da licitante vencedora. Caso não se confirme a adequação do produto, a proposta vencedora será desclassificada.

22.2. Caso a CONTRATADA deverá comprovar a adoção de práticas de desfazimento sustentável ou reciclagem dos bens que forem inservíveis para o processo de reutilização.

23. ANEXOS

23.1. São ainda, documentos integrantes deste Termo de Referência:

- Anexo A – Especificações Técnicas;

- Anexo B – Justificativas

- Anexo C – Propostas

- Anexo D – Escopo de Fornecimento e planilha de quantidades e preços máximos

ANEXO A - Especificação Técnica dos Serviços e Soluções

1. OBJETO

1.1. Ver objeto da contratação no Termo de Referência

2. CLASSIFICAÇÃO DO SERVIÇO

2.1. Os serviços a serem executados são:

a. Fornecimento de **subscrição para atualização da garantia das licenças de uso** – PA-3050 – Threat Prevention e URL Filtering pelo período de 48 (quarenta e oito) meses, válido para 02 (dois) appliances da Palo Alto Networks, incluindo suporte técnico especializado telefônico, remoto e on-site 24x7, de acordo com as especificações

b. **Suporte técnico especializado** telefônico, remoto e on-site para os equipamentos e licenças da Palo Alto PA-3050 por um período de 48 meses

c. **Treinamento e repasse de conhecimento**;

3. DESCRIÇÃO RESUMIDA DO EQUIPAMENTO

a. 02 equipamentos de firewall de Próxima Geração em cluster ativo-passivo da marca Palo Alto, modelo PA-3050, incluindo: filtro de pacotes; reconhecimento e controle de aplicação; administração de largura de banda (QoS) por aplicação; roteamento dinâmico por aplicação; redes privadas virtuais (VPN) IPSec e SSL; descriptografia de tráfego SSL/TLS; sistema de prevenção a intrusão (IPS) contra ameaças cibernéticas de vírus, spywares e malwares Zero Day ; filtro de URL; autenticação de duplo fator; console de gerenciamento com interface integrada à plataforma de inteligência de ameaças do mesmo fabricante; com suas respectivas licenças e assinaturas pertinentes; módulos das interfaces físicas.

4. GARANTIA TÉCNICA

a. A garantia técnica deverá ser realizada durante todo o período contratual, pelo próprio fabricante ou por Assistência Técnica Autorizada, permitindo cobertura completa e operacional de uso do equipamento em todas as funcionalidades atualmente contratadas.

b. Deve fazer parte da garantia todos os custos operacionais para reprogramações dos sistemas, correções de falhas de software, atualização de versões dos módulos de software, incluindo sistema operacional do equipamento e firmwares, disponibilizados pelo fabricante da solução durante o prazo contratado, sem custo adicional para a CONTRATANTE das novas versões de atualização que por ventura vierem a ser publicadas.

c. A garantia deve contemplar a substituição do todo ou em parte dos equipamentos cobertos quando da necessidade de manutenções corretivas e, ou, manutenções evolutivas do hardware.

d. Durante a vigência do contrato, todas as funcionalidades dos 2 (dois) equipamentos PA modelo 3050, hora em produção, deverão ser atualizadas a medida do lançamento de novas versões sem custos para a CONTRATADA.

e. Todas as instalações de novas versões, atualizações, correções sejam do próprio PaloAlto, sejam de *features* instaladas devem ser executadas pela CONTRATADA.

f. Segue a lista de funcionalidades (features) habilitadas e disponíveis nos 2 (dois) equipamentos PA-3050. Cabe ressaltar que os part numbers apresentados é referente

a contratação atual de 3 anos, sendo que na nova contratação as features serão as mesmas, mas considerando o período de 4 anos:

Part Number Fabricante	Descrição do Produto
PAN-SVC-PREM-3020-3YR	Premium Support 3-Year Prepaid, Pa-3050
PAN-PA-3050-URL4-3YR-HA2	PANDB URL Filtering Subscription 3-Year Pre
PAN-PA-3050-TP-3YR-HA2	Threat Prevention Subscription 3-Year Pre
PAN-PA-3050-GP-3YR-HA2	Global Protection Subscription 3-Year Pre

5. SUBSCRIÇÃO PARA ATUALIZAÇÃO DA GARANTIA DAS LICENÇAS DE USO

5.1. O serviço de atualização de licenciamento consiste na atualização da versão atual para versões mais novas, bem como as atualizações de novas versões que forem lançadas durante a vigência do contrato. As atualizações são para os itens abaixo:

5.1.1. Atualização de licenças e versões do PA-3050 e todos os seus componentes e partes (features), já em produção.

5.1.2. Atualização do URL Filtering Version;

5.1.3. Atualização do Antivírus;

5.1.4. Atualização do Threat Version;

5.1.5. GlobalProtect Clientless VPN Version;

5.2. No caso de a solução contratada passar a constar em listas de End-of-Support, End-of-Sales ou End-of-Life do fabricante a CONTRATADA deverá substituir a solução por uma outra com características técnicas iguais ou superiores.

6. TREINAMENTO E REPASSE DE CONHECIMENTO

6.1. O repasse de conhecimento diz respeito ao curso de operação, configuração e utilização de todas as funcionalidades do firewall PA-3050, para o total de 3 pessoas, a serem indicados pela CONTRATANTE dos serviços. Toda e qualquer despesa, instalações necessárias, local e o que for necessário para a realização deste curso correrá por conta da CONTRATADA.

6.2. A carga horária mínima deverá ser de 40 horas.

6.3. Deve ser emitido certificado de conclusão do curso, sendo um para cada participante.

6.4. O curso deverá ser preferencialmente presencial. Este não podendo ocorrer devido a restrições da pandemia de Covid 19 poderá ser ministrado remotamente com a presença de instrutor.

6.5. Disponibilização de material impresso ou para download durante o curso.

7. SUPORTE TÉCNICO ESPECIALIZADO

a. O serviço de manutenção e suporte consiste na desinstalação, reconfiguração ou reinstalação decorrentes de falhas no software/hadware, adequação dos softwares às melhores práticas, atualização da versão de software, correção de defeitos, ajustes e reparos necessários, de acordo com os manuais e as normas técnicas específicas para os recursos utilizados. Quanto às atualizações pertinentes aos softwares, entende-se como “atualização” o provimento de toda e qualquer evolução de software, incluindo correções, “patches”, “fixes”, “updates”, “service-packs”, novas “releases”, “versions”, “builds”, “upgrades”, durante a vigência do contrato.

b. O suporte técnico deve compreender procedimentos destinados a manter os equipamentos em perfeito estado de uso, nos casos de inoperância total ou parcial, defeito ou mau funcionamento, incluindo substituições ou reposições, inclusive de peças, ajustes e reparos, de acordo com os manuais e normas técnicas adotadas e recomendadas pelo fabricante.

c. Todo o hardware e software que for empregado para garantir o perfeito funcionamento das funcionalidades dos produtos, em qualidade, quantidade e desempenho requeridos, deverão ser assegurados durante todo o período de garantia.

a. Toda nova implementação/criação de serviços, configurações e outros, que surjam durante a vigência do contrato, e que a equipe interna da CONTRATANTE não esteja apta para a sua execução, será aberto um chamado junto a CONTRATADA para prover o suporte técnico especializado e acompanhamento do mesmo. Não incorrendo em custas ou pagamentos extras ao valor contratado.

b. Toda e qualquer manutenção de hardware, no equipamento acima descrito, suas despesas, correrá por parte da CONTRATADA sendo as mais variadas. Em caso de troca ou substituição do equipamento deverá ser por uma igual ou superior ao que está instalado nas dependências da CONTRATADA.

7.1. As atividades de manutenção e suporte técnico corretivo serão realizadas sempre que solicitadas pela Codevasf por meio da abertura de chamado diretamente à CONTRATADA via telefone, e-mail e/ou site.

7.2. Um chamado somente poderá ser fechado após o aceite do fiscal técnico responsável pelo contrato na Codevasf e o término de atendimento se dará com a disponibilidade do recurso para uso em perfeitas condições de funcionamento no local onde o mesmo está instalado.

7.3. Todas as solicitações feitas pela Codevasf deverão ser registradas pela CONTRATADA para acompanhamento e controle da execução dos serviços. Após a realização dos serviços, a CONTRATADA deverá apresentar um Relatório de Atividades, contendo no mínimo as informações descritas no item a seguir, e este relatório deverá ser homologado pelo Fiscal Técnico responsável pelo contrato na Codevasf.

7.3.1. O relatório de atividades deverá ser emitido pelo Gerente de Suporte encarregado pelo contrato na CONTRATADA e será preenchido pelo técnico da CONTRATADA encarregado de prestar os serviços, contendo no mínimo:

a) Identificação do Relatório de Atividades;
b) data da emissão;
c) data e hora de início e término do atendimento;
d) número do contrato;
e) identificação do requisitante do serviço;
f) descrição da atividade realizada e detalhamento da solução aplicada;
g) identificação do fiscal técnico da Codevasf que validou o serviço; e
h) identificação do técnico da CONTRATADA responsável pela execução do serviço.

7.3.2. A CONTRATADA, a partir da data de formalização de recebimento da abertura do chamado, terá os prazo estipulados para atendimento segundo TABELA I para iniciar o atendimento presencial caso seja necessário.

7.3.3. Os chamados serão categorizados conforme a sua Severidade pela equipe da CONTRATANTE no momento de abertura do chamado conforme TABELA I;

Severidade	Descrição	Atendimento Técnico (em até)	Solução
1 – Crítica	Situação emergencial ou problema crítico que cause a indisponibilidade do ambiente ou da solução contratada.	2 horas	4 horas
2 – Alta	Impacto de alta significância relacionado à utilização e/ou aplicação da remediação orientada pela solução contratada.	4horas	8 horas
3 – Média	Impacto de baixa significância relacionado à utilização e/ou aplicação da remediação orientada pela solução contratada.	8 horas	12 horas
4 – Baixa	Questionamentos necessários para sanar dúvidas acerca da utilização da solução contratada.	24 horas	72 horas

7.3.4. A CONTRATADA deverá informar aos responsáveis da Codevasf qualquer situação que possa ensejar em uso inadequado dos recursos.

8. NÍVEIS MÍNIMOS DE SERVIÇO

8.1. O nível de serviço mínimo, para este certame para os chamados abertos será dado pela TABELA II, a seguir:

Percentual dos chamados com atraso	Tempo de atraso para resolução dos chamados em horas úteis	Medidas corretivas
Até 5%	Tempo de atraso ≤ 12h	Aceito
	12h < tempo de atraso ≤ 28h	Advertência
	28h < tempo de atraso ≤ 40h	Glosa de 1% do valor do serviço referente ao mês de encerramento do chamado
	Tempo de atraso > 40h	Multa de 2% sobre o valor do Contrato pelo descumprimento dos limites máximos estabelecidos para o Nível de Serviço Mínimo, assegurada à administração o direito de aplicar a Glosa aferida no instrumento, aplicada em dobro na sua reincidência.
≤ 10%	Tempo de atraso ≤ 12h	Advertência
	12h < tempo de atraso ≤ 28h	Glosa de 1% do valor do serviço referente ao mês de encerramento do chamado
	28h < tempo de atraso ≤ 40h	Glosa de 3% do valor do serviço referente ao mês de encerramento do chamado
	Tempo de atraso > 40h	Multa de 2% sobre o valor do Contrato pelo

		descumprimento dos limites máximos estabelecidos para o Nível de Serviço Mínimo, assegurada à administração o direito de aplicar a Glosa aferida no instrumento, aplicada em dobro na sua reincidência.
10%<chamados com atraso ≤ 20%	Tempo de atraso ≤ 12h	Glosa de 1% do valor do serviço referente ao mês de encerramento do chamado
	12h < tempo de atraso ≤ 28h	Glosa de 3% do valor do serviço referente ao mês de encerramento do chamado
	28h < tempo de atraso ≤ 40h	Glosa de 5% do valor do serviço referente ao mês de encerramento do chamado
	Tempo de atraso > 40h	Multa de 2% sobre o valor do Contrato pelo descumprimento dos limites máximos estabelecidos para o Nível de Serviço Mínimo, assegurada à administração o direito de aplicar a Glosa aferida no instrumento, aplicada em dobro na sua reincidência.
20%<chamados com atraso ≤ 30%	Tempo de atraso ≤ 12h	Glosa de 3% do valor do serviço referente ao mês de encerramento do chamado
	12h < tempo de atraso ≤ 28h	Glosa de 5% do valor do serviço referente ao mês de encerramento do chamado
	28h < tempo de atraso ≤ 40h	Glosa de 8% do valor do serviço referente ao mês de encerramento do chamado
	Tempo de atraso > 40h	Multa de 2% sobre o valor do Contrato pelo descumprimento dos limites máximos estabelecidos para o Nível de Serviço Mínimo, assegurada à administração o direito de aplicar a Glosa aferida no instrumento, aplicada em dobro na sua reincidência.
> 30%		Multa de 2% sobre o valor do Contrato pelo descumprimento dos limites máximos estabelecidos para o Nível de Serviço Mínimo, assegurada à administração o direito de aplicar a Glosa aferida no instrumento, aplicada em dobro na sua reincidência.

9. ESPECIFICAÇÃO TÉCNICA DA SOLUÇÃO DE FIREWALL PA-3050

9.1. DA DESCRIÇÃO DOS ITENS

9.1.1. A plataforma de segurança possui a capacidade e as características abaixo, por equipamento:

9.1.2. Throughput de 4 Gbps com a funcionalidade de controle de aplicação habilitada para todas as assinaturas que o fabricante possuir;

9.1.3. Throughput de 2 Gbps com as seguintes funcionalidades habilitadas simultaneamente para todas as assinaturas que a plataforma de segurança possuir devidamente ativadas e atuantes: controle de aplicação IPS, Antivírus e Antispyware. Caso o fabricante divulgue múltiplos números de desempenho para qualquer uma destas funcionalidades, somente o de menor valor será aceito;

9.1.4. Os throughputs devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, serão considerados inabilitados e sujeitos as sanções previstas em lei;

9.1.5. Suporte a, no mínimo, 500.000 conexões simultâneas;

9.1.6. Suporte a, no mínimo, 50.000 novas conexões por segundo;

9.1.7. Fonte de 400W AC;

9.1.8. Disco Solid State Drive (SSD) de, no mínimo, 100 GB;

9.1.9. 12 (doze) interfaces de rede 10/100/1000 base-TX;

9.1.10. 8 (oito) interfaces de rede 1 Gbps SFP;

9.1.11. 2 (duas) Gbps interfaces dedicadas para alta disponibilidade;

9.1.12. 1 (uma) interface de rede 1 Gbps dedicada para gerenciamento;

9.1.13. 1 (uma) interface do tipo console ou similar;

9.1.14. Suporte a, no mínimo, 10 (dez) roteadores virtuais;

9.1.15. Suporte a, no mínimo, 30 (trinta) zonas de segurança;

9.1.16. Estar licenciada para ou suportar sem o uso de licença, 1.000 (mil) clientes de VPN SSL simultâneos;

9.1.17. Estar licenciada para ou suportar sem o uso de licença, 1.000 (mil) túneis de VPN IPSEC simultâneos;

9.1.18. Suporta, no mínimo, 5 sistemas virtuais lógicos (Contextos) no firewall Físico;

9.1.19. Os contextos virtuais suportam funcionalidades nativas do gateway de proteção incluindo: Firewall, IPS, Antivírus, Anti-Spyware, Filtro de URL, Filtro de Dados, VPN, Controle de Aplicações, QOS, NAT e Identificação de usuários;

9.1.20. Por cada equipamento que compõe a plataforma de segurança, entende-se o hardware e as licenças de softwares necessárias para o seu funcionamento;

9.1.21. Por console de gerência e monitoração, entende-se as licenças de software necessárias para as duas funcionalidades, bem como hardware dedicado para o funcionamento das mesmas;

9.1.22. A console de gerência e monitoração podem residir no mesmo appliance de proteção de rede, desde que possuam recurso de CPU, memória, interface de rede e sistema operacional dedicados para esta função;

9.1.23. A solução consiste de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

9.1.24. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;

9.1.25. As funcionalidades de proteção de rede que compõe a plataforma de segurança, funciona em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação;

9.1.26. A plataforma é otimizada para análise de conteúdo de aplicações em camada 7;

9.1.27. O hardware e software que executem as funcionalidades de proteção de rede, bem como a console de gerência e monitoração, é do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

9.1.28. A solução suporta montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

9.1.29. O software deverá ser fornecido em sua versão mais atualizada;

9.1.30. Os dispositivos de proteção de rede possuem pelo menos as seguintes funcionalidades:

9.1.30.1. Suporte a 4094 VLAN Tags 802.1q;
9.1.30.2. Agregação de links 802.3ad e LACP;
9.1.30.3. Policy based routing ou policy based forwarding;
9.1.30.4. Roteamento multicast (PIM-SM);
9.1.30.5. DHCP Relay;
9.1.30.6. DHCP Server;
9.1.30.7. Jumbo Frames;
9.1.30.8. Suporte a criação de objetos de rede que possam ser utilizados como endereço IP de interfaces L3;
9.1.30.9. Suportar sub-interfaces ethernet logicas.
9.1.30.10. suporta os seguintes tipos de NAT:
9.1.30.10.1. Nat dinâmico (Many-to-1);
9.1.30.10.2. Nat dinâmico (Many-to-Many);
9.1.30.10.3. Nat estático (1-to-1);
9.1.30.10.4. NAT estático (Many-to-Many);
9.1.30.10.5. Nat estático bidirecional 1-to-1;
9.1.30.10.6. Tradução de porta (PAT);
9.1.30.10.7. NAT de Origem;
9.1.30.10.8. NAT de Destino;
9.1.30.10.9. Suportar NAT de Origem e NAT de Destino simultaneamente;
9.1.30.10.10. Implanta Network Prefix Translation (NPTv6), prevenindo problemas de roteamento assimétrico;
9.1.30.10.11. Implementa o protocolo ECMP;
9.1.30.10.12. Implementa balanceamento de link por hash do IP de origem;
9.1.30.10.13. Implementa balanceamento de link por hash do IP de origem e destino;
9.1.30.10.14. Implementa balanceamento de link através do método round-robin;
9.1.30.10.15. Implementa balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Suporta o balanceamento de, no mínimo, quarto links;
9.1.30.10.16. Implementa balanceamento de link através de políticas por usuário e grupos de usuários do LDAP/AD;
9.1.30.10.17. Implementa balanceamento de link através de políticas por aplicação e porta de destino;
9.1.30.10.18. Implementa o protocolo Link Layer Dicovery (LLDP), permitindo que o appliance e outros ativos da rede se comuniquem para identificação da topologia da rede em que estão conectados e a função dos mesmos facilitando o processo de throubleshooting. As informações aprendidas e armazenadas pelo appliance devem ser acessíveis via SNMP;
9.1.30.10.19. Enviar log para sistemas de monitoração externos, simultaneamente;

9.1.30.10.20. Há a opção de enviar logs para os sistemas de monitoração externos via protocolo TCP e SSL;
9.1.30.10.21. Permite configurar certificado caso necessário para autenticação no sistema de monitoração externo de logs;
9.1.30.10.22. Proteção contra anti-spoofing;
9.1.30.10.23. Permite bloquear sessões TCP que usarem variações do 3-way hand-shake, como 4 way e 5 way split hand-shake, prevenindo desta forma possíveis tráfegos maliciosos;
9.1.30.10.24. Para IPv4, suporta roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);
9.1.30.10.25. Para IPv6, suporta roteamento estático e dinâmico (OSPFv3);
9.1.30.10.26. Suportar a OSPF graceful restart;
9.1.30.10.27. Suportar no mínimo as seguintes funcionalidades em IPv6: SLAAC (address auto configuration), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, Regras de proteção contra DoS (Denial of Service), De-criptografia SSL e SSH, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, IPSEc, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS e controle de aplicação;
9.1.30.10.28. Os dispositivos de proteção possuem ter a capacidade de operar de forma simultânea em uma única instância de firewall, mediante o uso de suas interfaces físicas nos seguintes modos: Modo sniffer (monitoramento e análise do tráfego de rede), camada 2 (l2) e camada 3 (l3);
9.1.30.10.29. Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
9.1.30.10.30. Modo Camada – 2 (L2), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação;
9.1.30.10.31. Modo Camada – 3 (L3), para inspeção de dados em linha e ter visibilidade e controle do tráfego em nível de aplicação operando como default gateway das redes protegidas;
9.1.30.10.32. Modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

9.1.30.11. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo:
9.1.30.11.1. Em modo transparente;
9.1.30.11.2. Em layer 3;
9.1.30.11.3. A configuração em alta disponibilidade deve sincronizar:
9.1.30.11.4. Sessões;
9.1.30.11.5. Configurações, incluindo, mas não limitado a políticas de Firewall, NAT, QOS e objetos de rede;
9.1.30.11.6. Certificados de-criptografados;
9.1.30.11.7. Associações de Segurança das VPNs;
9.1.30.11.8. Tabelas FIB;
9.1.30.11.9. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link.

9.1.30.12. As funcionalidades de controle de aplicações, VPN IPSec e SSL, QOS, SSL e SSH Decryption e protocolos de roteamento dinâmico devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

9.1.30.13. Deverá suportar controles por zona de segurança.

9.2. CONTROLE POR POLÍTICA DE FIREWALL

9.2.1. Controles de políticas por porta e protocolo.

9.2.2. Controle de políticas por aplicações grupos estáticos de aplicações, grupos dinâmicos de aplicações (baseados em características e comportamento das aplicações) e categorias de aplicações.
9.2.3. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança.
9.2.4. Controle de políticas por código de País (Por exemplo: BR, USA, UK, RUS).

9.2.5. Controle, inspeção e de-criptografia de SSL por política para tráfego de entrada (Inbound) e Saída (Outbound).
9.2.6. Deve suportar offload de certificado em inspeção de conexões SSL de entrada (Inbound);
9.2.7. Deve de-criptografar tráfego Inbound e Outbound em conexões negociadas com TLS 1.2;
9.2.8. Controle de inspeção e de-criptografia de SSH por política;
9.2.9. A de-criptografia de SSH deve possibilitar a identificação e bloqueio de tráfego caso o protocolo esteja sendo usado para tunelar aplicações como técnica evasiva para burlar os controles de segurança;
9.2.10. A plataforma de segurança deve implementar espelhamento de tráfego de-criptografado (SSL e TLS) para soluções externas de análise (Forense de rede, DLP, Análise de Ameaças, entre outras);
9.2.11. É permitido uso de appliance externo, específico para a de-criptografia de (SSL e TLS), com espelhamento de cópia do tráfego de-criptografado tanto para o firewall, quanto para as soluções de análise.
9.2.12. Bloqueios dos seguintes tipos de arquivos: bat, cab, dll, exe, pif, e reg
9.2.13. Traffic shaping QoS baseado em Políticas (Prioridade, Garantia e Máximo)
9.2.14. QoS baseado em políticas para marcação de pacotes (diffserv marking), inclusive por aplicações.
9.2.15. Suporte a objetos e regras IPV6.
9.2.16. Suporte a objetos e regras multicast.
9.2.17. Suporta no mínimo três tipos de negação de tráfego nas políticas de firewall: Drop sem notificação do bloqueio ao usuário, Drop com opção de envio de ICMP Unreachable para máquina de origem do tráfego, TCP-Reset para o client, TCP-Reset para o server ou para os dois lados da conexão;
9.2.18. Suportar a atribuição de agendamento as políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

9.3. CONTROLE DE APLICAÇÕES

9.3.1. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

9.3.2. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos.

9.3.3. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

9.3.4. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs, etc;

9.3.5. Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante

independente de porta e protocolo. A checagem de assinaturas também deve determinar se uma aplicação está utilizando a porta default ou não, incluindo, mas não limitado a RDP na porta 80 ao invés de 389;

9.3.6. Deve aplicar heurística a fim de detectar aplicações através de análise comportamental do tráfego observado, incluindo, mas não limitado a Encrypted Bittorrent e aplicações VOIP que utilizam criptografia proprietária;

9.3.7. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e ataques mediante a porta 443.

9.3.8. Para tráfego criptografado SSL, deve de-criptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;

9.3.9. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo, incluindo, mas não limitado a Yahoo Instant Messenger usando HTTP. A decodificação de protocolo também deve identificar funcionalidades especificas dentro de uma aplicação, incluindo, mas não limitado a compartilhamento de arquivo dentro do Webex. Além de detectar arquivos e outros conteúdos que devem ser inspecionados de acordo as regras de segurança implementadas;

9.3.10. Deve permitir a utilização de aplicativos para um determinado grupo de usuário e bloquear para o restante, incluindo, mas não limitado a Skype. Deve permitir também a criação de políticas de exceção concedendo o acesso a aplicativos como Skype apenas para alguns usuários;

9.3.11. Identificar o uso de táticas evasivas via comunicações criptografadas;

9.3.12. Atualizar a base de assinaturas de aplicações automaticamente;

9.3.13. Reconhecer aplicações em IPv6;

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

9.3.15. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

9.3.16. Deve ser possível adicionar controle de aplicações em todas as regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

9.3.17. Deve suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos e análise heurística;

9.3.18. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;

9.3.19. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

9.3.20. A criação de assinaturas personalizadas deve permitir o uso de expressões regulares, contexto (sessões ou transações), usando posição no payload dos pacotes TCP e UDP e usando decoders de pelo menos os seguintes protocolos:

9.3.21. HTTP, FTP, SMB, SMTP, Telnet, SSH, MS-SQL, IMAP, IMAP, MS-RPC, RTSP e File body.

9.3.22. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;

9.3.23. Deve alertar o usuário quando uma aplicação for bloqueada;

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

9.3.25. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, neonet, etc.) possuindo granularidade de controle/politicas para os mesmos;

9.3.26. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Gtalk, Facebook Chat, etc.) possuindo granularidade de controle/politicas para os mesmos;

9.3.27. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Gtalk chat e bloquear a transferência de arquivos;

9.3.28. Deve possibilitar a diferenciação de aplicações Proxies (ghostsurf, freegate, etc.) possuindo granularidade de controle/politicas para os mesmos;

9.3.29. Deve ser possível a criação de grupos estáticos de aplicações e grupos dinâmicos de aplicações baseados em características das aplicações como:

9.3.30. Tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc).

9.3.31. Nível de risco da aplicação.

9.3.32. Categoria e sub-categoria de aplicações.

9.3.33. Aplicações que usem técnicas evasivas, utilizadas por malwares, como transferência de arquivos e/ou uso excessivo de banda etc.

9.4. PREVENÇÃO DE AMEAÇAS

9.4.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de Firewall ou entregue através de composição com outro equipamento ou fabricante.

9.4.2. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware); As funcionalidades de IPS, Antivírus e Anti-Spyware devem operar em caráter permanente, podendo ser utilizadas por tempo indeterminado, mesmo que não subsista o direito de receber atualizações ou que não haja contrato de garantia de software com o fabricante.

9.4.3. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade ativo/ativo e ativo/passivo;

9.4.4. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS, Antipyware e Antivirus: permitir, permitir e gerar log, bloquear, bloquear IP do atacante por um intervalo de tempo e enviar tcp-reset;

9.4.5. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
9.4.6. Exceções por IP de origem ou de destino devem ser possíveis nas regras, de forma geral e assinatura a assinatura;
9.4.7. Deve suportar granularidade nas políticas de IPS Antivírus e Anti-Spyware , possibilitando a criação de diferentes politicas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens.
9.4.8. Deve permitir o bloqueio de vulnerabilidades.
9.4.9. Deve permitir o bloqueio de exploits conhecidos.
9.4.10. Deve incluir proteção contra ataques de negação de serviços.
9.4.11. Deverá possuir os seguintes mecanismos de inspeção de IPS:

9.4.11.1. Análise de padrões de estado de conexões;
9.4.11.2. Análise de decodificação de protocolo;
9.4.11.3. Análise para detecção de anomalias de protocolo;
9.4.11.4. Análise heurística;
9.4.11.5. IP Defragmentation;
9.4.11.6. Remontagem de pacotes de TCP;
9.4.11.7. Bloqueio de pacotes malformados.

9.4.12. Ser imune e capaz de impedir ataques básicos como: Synflood, ICMPflood, UDPfloof, etc;
9.4.13. Detectar e bloquear a origem de portscans;
9.4.14. Bloquear ataques efetuados por worms conhecidos, permitindo ao administrador acrescentar novos padrões;
9.4.15. Suportar os seguintes mecanismos de inspeção contra ameaças de rede: análise de padrões de estado de conexões, análise de decodificação de protocolo, análise para detecção de anomalias de protocolo, análise heurística, IP Defragmentation, remontagem de pacotes de TCP e bloqueio de pacotes malformados;
9.4.16. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
9.4.17. Possuir assinaturas para bloqueio de ataques de buffer overflow;
9.4.18. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
9.4.19. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS e anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
9.4.20. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
9.4.21. É permitido uso de appliance externo (antivírus de rede), para o bloqueio de vírus e spywares em protocolo SMB de forma a conter malwares se espalhando horizontalmente pela rede;
9.4.22. Suportar bloqueio de arquivos por tipo;
9.4.23. Identificar e bloquear comunicação com botnets;
9.4.24. Deve suportar várias técnicas de prevenção, incluindo Drop e tcp-rst (Cliente, Servidor e ambos);

9.4.25. Deve suportar referência cruzada com CVE;
9.4.26. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:
9.4.27. O nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo;
9.4.28. Deve suportar a captura de pacotes (PCAP), por assinatura de IPS e Antyspyware;
9.4.29. Deve permitir que na captura de pacotes por assinaturas de IPS e Antispyware seja definido o número de pacotes a serem capturados. Esta captura deve permitir selecionar, no mínimo, 50 pacotes;

9.4.30. Deve possuir a função resolução de endereços via DNS, para que conexões com destino a domínios maliciosos sejam resolvidas pelo Firewall com endereços (IPv4 e IPv6), previamente definidos;
9.4.31. Permitir o bloqueio de vírus, pelo menos, nos seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
9.4.32. Os eventos devem identificar o país de onde partiu a ameaça;
9.4.33. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms.
9.4.34. Proteção contra downloads involuntários usando HTTP de arquivos executáveis. maliciosos.
9.4.35. Rastreamento de vírus em pdf.
9.4.36. Deve permitir a inspeção em arquivos comprimidos que utilizam o algoritmo deflate (zip, gzip, etc.)
9.4.37. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando Usuários, Grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferentes de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança.

9.5. ANÁLISE DE MALWARES MODERNOS

9.5.1. Devido aos Malwares hoje em dia serem muito dinâmicos e um antivírus comum reativo não ser capaz de detectar os mesmos com a mesma velocidade que suas variações são criadas, a solução ofertada dever possuir funcionalidades para análise de Malwares não conhecidos incluídas na própria ferramenta ou entregue com composição com outro fabricante;
9.5.2. O dispositivo de proteção deve ser capaz de enviar arquivos trafegados de forma automática para análise "In Cloud" ou local, onde o arquivo será executado e simulado em ambiente controlado;
9.5.3. Selecionar através de políticas granulares quais tipos de arquivos sofrerão esta análise incluindo, mas não limitado a: endereço IP de origem/destino, usuário/grupo do AD/LDAP, aplicação, porta, URL/categoria de URL de destino, tipo de arquivo e todas estas opções simultaneamente;
9.5.4. Deve possuir a capacidade de diferenciar arquivos analisados em pelo menos três categorias: malicioso, não malicioso e arquivos não maliciosos, mas com características indesejáveis como softwares que deixa o sistema operacional lento, que alteram parâmetros do sistema, etc.;
9.5.5. Suportar a análise com pelo menos 100 (cem) tipos de comportamentos maliciosos para a análise da ameaça não conhecida;
9.5.6. Suportar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows XP, Windows 7 (32 bits) e Windows 7 (64 bits);
9.5.7. Deve suportar a monitoração de arquivos trafegados na internet (HTTPs, FTP, HTTP, SMTP) como também arquivos trafegados internamente entre servidores de arquivos usando SMB em todos os modos de implementação: sniffer, transparente e L3;
9.5.8. A solução deve possuir a capacidade de analisar em sand-box links (http e https) presentes no corpo de e-mails trafegados em SMTP e POP3. Deve ser gerado um relatório caso a abertura do link pela sand-box o identifique como site hospedeiro de exploits;
9.5.9. Para ameaças trafegadas em protocolo SMTP e POP3, a solução deve ter a capacidade de mostrar nos relatórios o remetente, destinatário e assunto dos e-mails permitindo identificação ágil do usuário vítima do ataque;
9.5.10. O sistema de análise “In Cloud” ou local deve prover informações sobre as ações do Malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo Malware, gerar assinaturas de Antivírus e Anti-spyware

automaticamente, definir URLs não confiáveis utilizadas pelo novo Malware e prover informações sobre o usuário infectado (seu endereço ip e seu login de rede);

9.5.11. O sistema automático de análise "In Cloud" ou local deve emitir relatório com identificação de quais soluções de antivírus existentes no mercado possuem assinaturas para bloquear o malware;

9.5.12. Deve permitir exportar o resultado das análises de malwares de dia Zero em PDF e CSV a partir da própria interface de gerência;

9.5.13. Deve permitir o download dos malwares identificados a partir da própria interface de gerência;

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

9.5.15. Deve permitir informar ao fabricante quanto a suspeita de ocorrências de falso-positivo e falso-negativo na análise de malwares de dia zero a partir da própria interface de gerência.

9.5.16. Caso a solução seja fornecida em appliance local, deve possuir, no mínimo, 28 ambientes controlados (sand-box) independentes para execução simultânea de arquivos suspeitos;

9.5.17. Caso seja necessário licenças de sistemas operacional e softwares para execução de arquivos no ambiente controlado (sand-box), as mesmas devem ser fornecidas em sua totalidade, sem custos adicionais para a contratante;

9.5.18. Suportar a análise de arquivos executáveis, DLLs, ZIP e criptografados em SSL no ambiente controlado;

9.5.19. Permitir o envio de arquivos para análise no ambiente controlado via de forma automática via API.

9.6. FILTRO DE URL

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

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

9.6.1.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, Ips, Redes e Zonas de segurança.

9.6.1.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local.

9.6.1.4. Permite popular todos os logs de URL com as informações dos usuários conforme descrito na integração com serviços de diretório;

9.6.1.5. Suporta a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

9.6.1.6. Deve bloquear o acesso a sites de busca (Google, Bing e Yahoo), caso a opção Safe Search esteja desabilitada. Deve ainda exibir página de bloqueio fornecendo instruções ao usuário de como habilitar a função;

9.6.1.7. Suporta base ou cache de URLs local no appliance, evitando delay de comunicação/validação das URLs;

9.6.1.8. Possui pelo menos 60 categorias de URLs;

9.6.1.9. A categorização de URL deve analisar toda a URL e não somente até o nível de diretório;

9.6.1.10. Suporta a criação categorias de URLs customizadas;

9.6.1.11. Suporta a exclusão de URLs do bloqueio, por categoria;

9.6.1.12. Permite a customização de página de bloqueio;

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

9.6.1.14. Suporta a inclusão nos logs do produto de informações das atividades dos usuários;

9.6.1.15. Deve salvar nos logs as informações dos seguintes campos do cabeçalho HTTP nos acessos a URLs: UserAgent, Referer, e X-Forwarded For;

9.7. IDENTIFICAÇÃO DE USUÁRIOS

9.7.1. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via ldap, Active Directory, E-directory e base de dados local;

9.7.2. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

9.7.3. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

9.7.4. Deve implementar a criação de políticas de segurança baseada em atributos específicos do Radius, incluindo, mas não limitado a: baseado no sistema operacional do usuário remoto exigir autenticação padrão Windows e on-time password (OTP) para usuários Android;

9.7.5. Deve possuir integração com Ldap para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

9.7.6. Deve suportar o recebimento eventos de autenticação de controladoras wireless, dispositivos 802.1x e soluções NAC via syslog, para a identificação de endereços IP e usuários;

9.7.7. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

9.7.8. Suporte a autenticação Kerberos;

9.7.9. Deve suportar autenticação via Kerberos para administradores da plataforma de segurança, captive portal e usuário de VPN SSL;

9.7.10. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

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

9.7.12. Deve permitir a criação de políticas de segurança baseadas em usuários de rede com reconhecimento dos mesmos através de leitura do campo x-fowarded-for;

9.7.13. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD;

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

9.8. QOS

9.8.1. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, ustream, etc) e ter um alto consumo de largura de banda, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de máximo de largura de banda quando forem solicitadas por diferentes usuários ou aplicações, tanto de áudio como de vídeo streaming.

9.8.2. Suportar a criação de políticas de QoS por:

9.8.2.1. Endereço de origem
9.8.2.2. Endereço de destino
9.8.2.3. Por usuário e grupo do LDAP/AD.
9.8.2.4. Por aplicações, incluindo, mas não limitado a Skype, Bittorrent, YouTube e Azureus;
9.8.2.5. Por porta;

9.8.3. O QoS deve possibilitar a definição de classes por:

9.8.3.1. Banda Garantida
9.8.3.2. Banda Máxima
9.8.3.3. Fila de Prioridade.

9.8.4. Suportar priorização RealTime de protocolos de voz (VOIP) como H.323, SIP, SCCP, MGCP e aplicações como Skype.
9.8.5. Suportar marcação de pacotes Diffserv, inclusive por aplicação
9.8.6. Deve implemetar QOS (traffic-shapping), para pacotes marcados por outros ativos na rede (DSCP). A priorização e limitação do tráfego deve ser efetuada nos dois sentidos da conexão (inboud e outbound);
9.8.7. Disponibilizar estatísticas RealTime para classes de QoS.
9.8.8. Deve suportar QOS (traffic-shapping), em interface agregadas;
9.8.9. Deverá permitir o monitoramento do uso que as aplicações fazem por bytes, sessões e por usuário.

9.9. FILTRO DE DADOS

9.9.1. Permite a criação de filtros para arquivos e dados pré-definidos;
9.9.2. Os arquivos devem ser identificados por extensão e assinaturas;
9.9.3. Permite identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (P2P, InstantMessaging, SMB, etc);
9.9.4. Suportar identificação de arquivos compactados e a aplicação de politicas sobre o conteúdo desses tipos de arquivos;
9.9.5. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular;
9.9.6. Permitir listar o número de aplicações suportadas para controle de dados;
9.9.7. Permitir listar o número de tipos de arquivos suportados para controle de dados;

9.10. GEOLOCALIZAÇÃO

9.10.1. Suportar a criação de políticas por Geolocalização, permitindo o tráfego de determinado Pais/Países sejam bloqueados.
9.10.2. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.
9.10.3. Deve possibilitar a criação de regiões geográficas pela interface gráfica e criar políticas utilizando as mesmas.

9.11. VPN

9.11.1. Suportar VPN Site-to-Site e Cliente-To-Site;
9.11.2. Suportar IPSec VPN;
9.11.3. Suportar SSL VPN

9.11.4. A VPN IPSEc deve suportar:

9.11.4.1. 3DES;
9.11.4.2. Autenticação MD5 e SHA-1;
9.11.4.3. Diffie-Hellman Group 1 , Group 2, Group 5 e Group 14;
9.11.4.4. Algoritmo Internet Key Exchange (IKEv1 e v2);
9.11.4.5. AES 128, 192 e 256 (Advanced Encryption Standard)
9.11.4.6. Autenticação via certificado IKE PKI.

9.11.5. Deve possuir interoperabilidade com os seguintes fabricantes:

9.11.5.1. Cisco;
9.11.5.2. Checkpoint;
9.11.5.3. Juniper;
9.11.5.4. Palo Alto Networks;
9.11.5.5. Fortinet;
9.11.5.6. Sonic Wall;

9.11.6. Deve permitir habilitar, desabilitar, reiniciar e atualizar IKE gateways e túneis de VPN IPSEc a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

9.11.7. A VPN SSL deve suportar:

9.11.8. O usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
9.11.9. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
9.11.10. Atribuição de endereço IP nos clientes remotos de VPN SSL;
9.11.11. Deve permitir a atribuição de IPs fixos nos usuários remotos de VPN SSL;
9.11.12. Deve permitir a criação de rotas de acesso e faixas de endereços IP atribuídas a clientes remotos de VPN de forma customizada por usuário AD/LDAP e grupo de usuário AD/LDAP;
9.11.13. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
9.11.14. Atribuição de DNS nos clientes remotos de VPN;

9.11.15. Deve haver a opção de ocultar o agente de VPN instalado no cliente remoto, tornando o mesmo invisível para o usuário;
9.11.16. Deve exibir mensagens de notificação customizada toda vez que um usuário remoto se conectar a VPN. Deve permitir que o usuário desabilite a exibição da mensagem nas conexões seguintes;
9.11.17. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
9.11.18. A VPN SSL deve suportar proxy arp e uso de interfaces PPPOE;
9.11.19. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;
9.11.20. Permite estabelecer um túnel VPN client-to-site do cliente a plataforma de segurança, fornecendo uma solução de single-sign-on aos usuários, integrando-se com as ferramentas de Windows-logon;
9.11.21. Suporta leitura e verificação de CRL (certificate revocation list);
9.11.22. Permite a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;
9.11.23. O agente de VPN a ser instalado nos equipamentos desktop e laptops, dever ser capaz de ser distribuído de maneira automática via Microsoft SMS, Active

Directory e ser descarregado diretamente desde o seu próprio portal, o qual residirá no centralizador de VPN;

9.11.24. O agente deverá comunicar-se com o portal para determinar as políticas de segurança do usuário, Deve permitir que a conexão com a VPN SSL seja estabelecida das seguintes formas:

9.11.24.1. Antes do usuário autenticar na estação;
9.11.24.2. Após autenticação do usuário na estação;
9.11.24.3. Sob demanda do usuário;
9.11.24.4. Deverá manter uma conexão segura com o portal durante a sessão.

9.11.25. O agente de VPN SSL client-to-site deve ser compatível com pelo menos: Windows XP, Vista Windows 7, Windows 8 e Mac OSx;

9.12. CONSOLE DE GERÊNCIA E MONITORAÇÃO

9.12.1. Centralizar a administração de regras e políticas do cluster, usando uma única interface de gerenciamento;
9.12.2. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
9.12.3. Caso haja a necessidade de instalação de cliente para administração da solução o mesmo deve ser compatível com sistemas operacionais Windows e Linux;

9.12.4. O gerenciamento deve permitir/possuir:

9.12.4.1. Criação e administração de políticas de firewall e controle de aplicação;
9.12.4.2. Criação e administração de políticas de IPS, Antivírus e Anti-Spyware;
9.12.4.3. Criação e administração de políticas de Filtro de URL;
9.12.4.4. Monitoração de logs;
9.12.4.5. Ferramentas de investigação de logs;
9.12.4.6. Debugging;
9.12.4.7. Captura de pacotes.

9.12.5. Acesso concorrente de administradores;
9.12.6. Deve possuir mecanismo busca global na solução onde possa se consultar por uma string tais como: nome de objetos, ID ou nome de ameaças, nome de aplicações, nome de políticas, endereços IPs, permitindo a localização e uso deles na configuração do dispositivo;
9.12.7. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;
9.12.8. Deve permitir usar palavras chaves e cores para facilitar identificação de regras;
9.12.9. Deve permitir monitorar via SNMP falhas de hardware, inserção ou remoção de fontes, discos e coolers, uso de recursos por número elevado de sessões, número de túneis estabelecidos na VPN cliente-to-site, porcentagem de utilização em referência ao número total suportado/licenciado e número de sessões estabelecidas;
9.12.10. Deve suportar também o monitoramento dos seguintes recursos via SNMP: IP fragmentation, TCP state e dropped packets;
9.12.11. Bloqueio de alterações, no caso acesso simultâneo de dois ou mais administradores;
9.12.12. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
9.12.13. Autenticação integrada ao Microsoft Active Directory e servidor Radius;
9.12.14. Localização de em quais regras um endereço IP, IP Range, subnet ou objetos estão sendo utilizados;
9.12.15. Deve atribuir sequencialmente um número a cada regra de firewall, NAT, QOS e regras de DOS;

9.12.16. Criação de regras que fiquem ativas em horário definido;
9.12.17. Criação de regras com data de expiração;
9.12.18.
9.12.19. Backup das configurações e rollback de configuração para a última configuração salva;
9.12.20. Suportar Rollback de Sistema Operacional para a última versão local;
9.12.21. Habilidade de upgrade via SCP, TFTP e interface de gerenciamento;
9.12.22. Deve possuir mecanismo de análise de impacto na política de segurança antes de atualizar a base com novas aplicações disponibilizadas pelo fabricante;
9.12.23. Validação de regras antes da aplicação;
9.12.24. Deve implementar mecanismo de validação de configurações antes da aplicação delas permitindo identificar erros, tais como: rota de destino inválida, regras em shadowing etc.
9.12.25. É permitido o uso de appliance externo para permitir a validação de regras antes da aplicação.
9.12.26. Validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
9.12.27. É permitido o uso de appliance externo para permitir a validação de políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);
9.12.28. Deve possibilitar a visualização e comparação de configurações Atuais, configuração anterior e configurações antigas.
9.12.29. Deve possibilitar a integração com outras soluções de SIEM de mercado (third-party SIEM vendors)
9.12.30. Geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;
9.12.31. Deverá ter a capacidade de gerar um relatório gráfico que permita visualizar as mudanças na utilização de aplicações na rede no que se refere a um período de tempo anterior, para permitir comparar os diferentes consumos realizados pelas aplicações no tempo presente com relação ao passado;
9.12.32. Geração de relatórios com mapas geográficos gerados em tempo real para a visualização de origens e destinos do tráfego gerado na instituição;
9.12.33. Deve prover relatórios com visão correlacionada de aplicações, ameaças (IPS, Antivírus e Anti-Spware), URLs e filtro de arquivos, para melhor diagnóstico e resposta a incidentes;
9.12.34. Deve permitir a criação de Dash-Boards customizados para visibilidades do tráfego de aplicativos, usuários, categorias de URL, ameaças identificadas pelo IPS, antivírus, anti-spyware, malwares "Zero Day"detectados em sand-box e tráfego bloqueado;
9.12.35. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos dispositivos de segurança;
9.12.36. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Spware), etc;
9.12.37. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus e Anti-Spware), e URLs que passaram pela solução;
9.12.38. Deve possuir mecanismo "Drill-Down" para navegação nos relatórios em RealTime;

9.12.39. Nas opções de "Drill-Down", ser possível identificar o usuário que fez determinado acesso;
9.12.40. Deve possuir relatório de visibilidade e uso sobre aplicativos (SaaS). O relatório também deve mostrar os riscos para a segurança do ambiente, tais como a entrega de malwares através de aplicativos SaaS com a informação do usuário responsável pelo acesso;
9.12.41. Deve ser possível exportar os logs em CSV;
9.12.42. Deverá ser possível acessar o equipamento a aplicar configurações durante momentos onde o trafego é muito alto e a CPU e memória do equipamento estiver totalmente utilizada.

9.12.43. Rotação do log;
9.12.44. Deve permitir que os logs e relatórios sejam rotacionados automaticamente baseado no tempo em que estão armazenados na solução, assim como no espaço em disco usado;
9.12.45. Exibição das seguintes informações, de forma histórica e em tempo real (atualizado de forma automática e contínua a cada 1 minuto):
9.12.46. Situação do dispositivo e do cluster;
9.12.47. Principais aplicações;
9.12.48. Principais aplicações por risco;
9.12.49. Administradores autenticados na gerência da plataforma de segurança;
9.12.50. Número de sessões simultâneas;
9.12.51. Status das interfaces;
9.12.52. Uso de CPU;

9.12.53. Geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

9.12.53.1. Resumo gráfico de aplicações utilizadas;
9.12.53.2. Principais aplicações por utilização de largura de banda de entrada e saída;
9.12.53.3. Principais aplicações por taxa de transferência de bytes;
9.12.53.4. Principais hosts por número de ameaças identificadas;
9.12.53.5. Atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Spware), de rede vinculadas a este tráfego;
9.12.53.6. Deve permitir a criação de relatórios personalizados;
9.12.53.7. Em cada critério de pesquisa do log deve ser possível incluir múltiplas entradas (ex. 10 redes e IP's distintos; serviços HTTP, HTTPS e SMTP), exceto no campo horário, onde deve ser possível definir um faixa de tempo como critério de pesquisa;

9.12.54. Gerar alertas automáticos via:

9.12.54.1. Email;
9.12.54.2. SNMP;
9.12.54.3. Syslog;

9.12.55. A plataforma de segurança deve permitir através de API-XML (Application Program Interface) a integração com sistemas existentes no ambiente da contratante de forma a possibilitar que aplicações desenvolvidas na contratante possam interagir em RealTime com a solução possibilitando assim que regras e políticas de segurança de possam ser modificadas por estas aplicações com a utilização de scripts em linguagens de programação como Perl ou PHP.

ANEXO B - Justificativas

Justificativas:
Da necessidade da contratação

A Codevasf adota desde 2017 a solução de segurança de rede composta por firewall corporativo e multifuncional da marcao PaloAlto, modelo PA-3050, para prover segurança e proteção da rede de computadores, contemplando gerência unificada, com segurança no tráfego dos dados digitais, análise em tempo real das ameaças externas, das tentativas de invasões e das quebras de segurança, das tentativas de injeção de malwares, ransomwares ou vírus e manter o acesso à rede de dados da Codevasf por meio da Virtual Private Network (VPN) possibilitando assim o trabalho remoto.

Devido ao encerramento do contrato, ao final de 2020, e a necessidade de prover a empresa de infraestrutura de segurança de rede ao ambiente de tecnologia da informação que permita o acesso remoto e garanta a segurança das informações digitais, além de manutenção do investimento já realizado, se faz imprescindível realizar uma nova contratação de solução de firewall corporativo e multifuncional, conforme apontado no documento de Análise de Viabilidade, constantes como parte deste processo, com a finalidade de mantermos os serviços hoje prestados pelo firewall existente, com garantia de funcionamento e atualizações dos equipamentos por 48 meses.

Da adoção pelo uso do PREGÃO ELETRÔNICO

A adoção do Pregão Eletrônico visa ampliar a eficiência nesta contratação, a competitividade entre os licitantes, assegurar o tratamento isonômico, buscar maior simplificação, celeridade, transparência e eficiência nos procedimentos para dispêndio de recursos públicos e a seleção da proposta mais vantajosa para a administração pública. Os bens objeto desta contratação se classificam como bens comuns para fins de Pregão Eletrônico, não havendo nenhuma complexidade neles.

Permite Participação de Consórcios: Não - Por se tratar de prestação de serviços comuns, 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.

Critério de Julgamento: Menor preço – Justifica-se pela maior economicidade e vantajosidade para a administração pública.

Sustentabilidade Ambiental: Serão atendidos os requisitos previstos na legislação aplicável.

Garantia do Objeto: A garantia do objeto deverá obedecer ao prazo definido na legislação mais atual e ao que consta no Anexo A - Especificações Técnicas, parte integrante deste Termo de Referência.

Justificativa de não reserva de cota de até 25% (vinte e cinco) por cento – Considerando que o objeto da presente licitação não é divido em itens não haverá reserva de cota de 25%.

Da composição de preços – cotações - Para composição dos preços máximos estimados para os itens da licitação, foram feitas cotações junto a várias atas de registro de preços vigentes e a diversos fornecedores regionais e nacionais.

Da Fonte de Recursos: A fonte orçamentária será informada no momento da emissão da Ordem de Fornecimento ou contrato.

Permite Subcontratação: Não será aceito a subcontratação devido a impossibilidade de

parcelamento do item contratado.

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.

ANEXO C - Propostas

Item	DESCRIÇÃO	UN	QT	Valor unit. (R$)	Valor Total (R$)
01	Fornecimento de subscrição para atualização da garantia das licenças de uso – PA-3050 Ver **anexo A**	unit	2		
02	Serviço de suporte técnico 24x7 on-site ou presencial, manutenção técnica, garantia de atualização, garantia de hardware, para a solução *firewall* corporativo e multifuncional marca paloalto modelo 3050. incluindo assinaturas de filtro url e threat prevention por um período de **48 meses**. **Ver anexo A**	meses	48		
03	Treinamento e repasse de conhecimento. **Ver anexo A**	turma	1		
Valor Global R$					

ANEXO D - ESCOPO DE FORNECIMENTO E PLANILHA DE QUANTIDADES E PREÇOS MÁXIMOS

Item	DESCRIÇÃO	UN	QT	Valor unit. (R$)	Valor Total (R$)
01	Fornecimento de subscrição para atualização da garantia das licenças de uso – PA-3050 Ver **anexo A**	unit	2	R$ 712.818,08	R$ 1.425.636,16
02	Serviço de suporte técnico 24x7 on-site ou presencial, manutenção técnica, garantia de atualização, garantia de hardware, para a solução *firewall* corporativo e multifuncional marca paloalto modelo 3050. incluindo assinaturas de filtro url e threat prevention por um período de **48 meses**. **Ver anexo A**	meses	48	R$ 10.791,27	R$ 517.980,96
03	Treinamento e repasse de conhecimento. **Ver anexo A**	turma	1	R$ 17.329,28	R$ 17.329,28
Valor Total					R$ 1.960.946,40

COMPANHIA DE DESENVOLVIMENTO DOS VALES
DO SÃO FRANCISCO E DO PARNAÍBA

MINISTÉRIO DO DESENVOLVIMENTO REGIONAL - MDR

CÓDIGO DE CONDUTA ÉTICA E INTEGRIDADE DA CODEVASF

Deliberação nº 35, de 28 de setembro de 2020

2020

SUMÁRIO

APRESENTAÇÃO

A responsabilidade social de uma empresa pública exige a incorporação, às suas práticas comerciais e organizacionais, de princípios e valores éticos essenciais ao cumprimento da missão institucional que lhe é confiada pela sociedade.

O presente Código de Conduta Ética e Integridade apresenta as condutas a serem adotadas pelos agentes públicos que exercem cargo em comissão, emprego ou função de confiança na Codevasf, que devem ser orientadas pelos princípios de respeito, de honestidade e de responsabilidade, compondo as regras básicas para o agir ético.

As condutas aqui descritas deverão ser observadas como orientações de comportamento em situações da vida profissional ou de atos que dela decorrem.

A Codevasf, com este Código, visa à prevenção de desvios de conduta, promovendo a defesa da dignidade humana, a proteção ao interesse público, a promoção do bem comum e a disseminação de orientações e atividades educativas, sem prejuízo da aplicação de medidas disciplinares cabíveis, quando tais desvios forem constatados.

O compromisso de todos com o cumprimento das disposições presentes neste Código é fundamental para que a Codevasf alcance suas metas, seus objetivos e sua missão de forma ética e transparente.

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º A Companhia de Desenvolvimento dos Vales do São Francisco e do Parnaíba - Codevasf tem por finalidade o aproveitamento, para fins agrícolas, agropecuários e agroindustriais, dos recursos de água e solo das bacias hidrográficas que compõem sua área de atuação, diretamente ou por intermédio de entidades públicas e privadas, com a promoção do desenvolvimento integrado de áreas prioritárias e a implantação de distritos agroindustriais e agropecuários, com possibilidade, para esse efeito, de coordenar ou executar, diretamente ou mediante contratação, obras de infraestrutura, particularmente de captação de água, para fins de irrigação, de construção de canais primários ou secundários, e também obras de saneamento básico, eletrificação e transportes, conforme plano diretor, em articulação com os órgãos federais competentes.

Art. 2º A conduta dos agentes públicos da Codevasf será orientada pelo Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, aprovado pelo Decreto nº 1.171, de 22 de junho de 1994, pelo Código de Conduta da Alta Administração Federal, pelas resoluções expedidas pela Comissão de Ética Pública da Presidência da República - CEP e por este Código, sem prejuízo de outras normas aplicáveis.

Art. 3º Este Código de Conduta Ética e Integridade tem por finalidade orientar os agentes públicos da Codevasf sobre as normas gerais de conduta, com o objetivo de:

I - fortalecer a imagem institucional;

II - criar ambiente adequado ao convívio social;

III - promover a prática e a conscientização quanto aos princípios de conduta;

IV - instituir instrumento referencial de apoio à decisão ética cotidiana; e

V - fortalecer o agir ético.

CAPÍTULO II
DA CONCEITUAÇÃO

Art. 4º Para fins deste Código, entende-se:

I - Agente Público: todo aquele que, por força de lei, contrato ou qualquer outro ato jurídico, preste serviços de natureza permanente, temporária, excepcional ou eventual à Codevasf, ainda que não remunerado, inclusive os ocupantes de cargos em comissão, funções de confiança ou gratificada e membros dos órgãos estatutários, ainda que estejam em gozo de licença ou em período de afastamento ou cedidos temporariamente para outros órgãos;

II - Atividade de cunho político-partidário: a atividade cujo objetivo, ainda que indireto, seja a promoção de uma pessoa, um partido político ou uma ideologia partidária;

III - Assédio moral: consiste na repetição deliberada de gestos, palavras (orais ou escritas) e/ou comportamentos, os quais expõem o agente público a situações humilhantes e

constrangedoras, capazes de lhes causar ofensa à personalidade, à dignidade ou à integridade psíquica ou física, com o objetivo de excluí-lo das suas funções ou de deteriorar o ambiente de trabalho;

IV - Assédio sexual: o ato de constranger alguém, com o intuito de obter vantagem ou favorecimento sexual, prevalecendo-se o agente público da sua condição de superior hierárquico ou ascendência inerentes ao exercício de emprego, cargo ou função;

V - Clientes: pessoas físicas ou jurídicas que adquirem ou possam adquirir bens, serviços ou informações produzidas pela Codevasf;

VI - Conflito de interesses: qualquer situação gerada pelo confronto entre os interesses da Codevasf e os interesses particulares de seus agentes públicos, que possa vir a comprometer os interesses da Empresa ou influenciar de maneira imprópria o desempenho das atividades de seus agentes públicos;

VII - Consciência cidadã: atuação com responsabilidade ambiental, econômica, social e cultural, de forma equilibrada, respeitando o direito à vida plena das gerações atuais e contribuindo para a preservação das futuras;

VIII - Corrupção: qualquer ação, direta ou indireta, que consiste em autorização, oferecimento, promessa, solicitação, aceitação, exigência, entrega ou recebimento de vantagem indevida, de natureza econômica ou não, envolvendo pessoas físicas ou jurídicas, agentes públicos ou não, com o objetivo de que se pratique ou deixe de se praticar determinado ato;

IX - Denúncia anônima: manifestação que chega aos canais de denúncia sem identificação;

X - Dignidade humana e respeito às pessoas: valorização da vida e afirmação da cidadania, respeitando a integridade física e moral de todas as pessoas, as diferenças individuais, sociais e econômicas e a diversidade de grupos sociais, com igualdade, equidade e justiça;

XI - Eficiência: executar as atividade da Empresa com presteza e rendimento funcional, exigindo a concretização de resultados positivos para a administração pública e o atendimento satisfatório das necessidades da comunidade;

XII - Ética: valor que norteia a conduta humana no que se refere ao seu caráter, altruísmo e virtudes, tanto no meio social quanto institucional, de modo a determinar a melhor forma de agir e se comportar em sociedade;

XIII - Fornecedores: pessoas físicas ou jurídicas que forneçam bens e serviços à Codevasf;

XIV - Fraude: qualquer ação ou omissão intencional, com o objetivo de lesar ou ludibriar outra pessoa, capaz de resultar em perda para a vítima e/ou vantagem indevida, patrimonial ou não, para o autor ou terceiros, pela declaração falsa ou omissão de circunstâncias materiais com o intuito de levar ou induzir terceiros a erro;

XV - Impessoalidade: prevalência do interesse público sobre os interesses particulares, com objetividade e imparcialidade nas decisões, ações e no uso dos recursos da Empresa;

XVI - Informação privilegiada: a que diz respeito a assuntos sigilosos ou aquela relevante ao processo de decisão no âmbito da Codevasf, que tenha repercussão econômica ou financeira e que não seja de amplo conhecimento público;

XVII - Integridade: honestidade, moralidade e probidade na realização dos compromissos assumidos, repudiando toda a forma de fraude e corrupção, com postura ativa diante de situações que não estejam de acordo com os princípios éticos assumidos;

XVIII - Legalidade: respeito à legislação e às normas internas da Empresa;

XIX - Moralidade: dever de não apenas cumprir a lei formalmente, mas cumprir substancialmente, procurando sempre o melhor resultado para a Empresa;

XX - Nepotismo: o favorecimento de parentes em linha reta ou colateral por consanguinidade ou afinidade até o terceiro grau, nas relações de trabalho ou emprego, para privilegiar os laços de parentesco em detrimento da avaliação de mérito, conforme explicitado na tabela abaixo:

FORMAS DE PARENTESCO			**GRAU DE PARENTESCO**		
			1º grau	2º grau	3º grau
Parentes Consanquíneos	Em linha reta	Ascendentes	Pais (inclusive madastra e padastro)	Avós	Bisavós
		Descendetes	Filhos	Netos	Bisnetos
	Em linha colateral			Irmãos	Tios e Sobrinhos (e seus cônjuges)
Parentes por afinidade	Em linha reta	Ascendente	Sogros (inclusive madastra e padastro do cônjuge ou companheiro)	Avós do cônjuge ou companheiro	Bisavós do cônjuge ou companheiro
		Descendente	Enteados, genros e noras (inclusive do cônjuge ou companheiro)	Netos (exclusivo do cônjuge ou companheiro)	Bisnetos (exclusivo do cônjuge ou companheiro)
	Em linha colateral			Cunhados (irmãos do cônjuge ou companheiro)	Tios e sobrinhos do cônjuge ou companheiro (e seus cônjuges)

Obs: O Cônjuge ou Companheiro, embora não seja considerado parente, encontra-se sujeito às vedações contidas na súmula vinculante nº 13 do Supremo Tribunal Federal.

XXI - Profissionalismo: desempenho profissional íntegro, assíduo, eficiente, com responsabilidade e zelo, comprometido com a busca da excelência no desempenho de suas atividades na Codevasf;

XXII - Publicidade: trata-se da divulgação oficial do ato para o conhecimento público;

XXIII - Reserva de identidade: a ocultação da identificação do denunciante, a pedido ou de ofício; e

XXIV - Transparência: visibilidade dos critérios que norteiam as decisões e as ações da Empresa, nos termos da legislação vigente, mediante comunicação clara, exata, ágil e acessível, observando os limites do direito à confidencialidade.

CAPÍTULO III
DOS PRINCÍPIOS E VALORES ÉTICOS

Art. 5º A conduta dos agentes públicos da Codevasf será orientada por este Código, pelo cumprimento dos normativos vigentes, da lei de criação da Empresa, do seu Estatuto Social e Regimento Interno, e da legislação aplicável, observados princípios e valores essenciais na atuação da Empresa.

Art. 6º São Princípios Éticos na Codevasf:

I - a legalidade, impessoalidade, moralidade, publicidade e eficiência;

II - o reconhecimento da probidade, da integridade corporativa e da lealdade como valores intrínsecos ao exercício das atividades profissional e organizacional;

III - a garantia da liberdade de expressão e de acesso à informação;

IV - o respeito às diferenças individuais e consequente eliminação de qualquer forma de discriminação em função de etnia, nacionalidade, gênero, crença religiosa, convicção política, origem, classe social, linguística, orientação sexual, idade ou capacidade física;

V - a proteção ao meio ambiente, a otimização do trabalho, a cooperação e o combate ao desperdício dos recursos públicos; e

VI - a defesa da dignidade humana, a proteção ao interesse público e a promoção do bem comum.

Art. 7º São Valores Éticos na Codevasf:

I - a ética;

II - a dignidade humana e o respeito às pessoas;

III - a integridade;

IV - a consciência cidadã;

V - a transparência;

VI - a honestidade;

VII - a discrição;

VIII - a cordialidade e urbanidade;

IX - a boa-fé e o decoro; e

X - o zelo permanente pela imagem e integridade institucional.

CAPÍTULO IV
DA CONDUTA ÉTICA

Art. 8º A Codevasf possuirá Comissão de Ética encarregada de orientar e aconselhar quanto a ética profissional de seus agentes públicos, no tratamento com as pessoas e com o patrimônio público, competindo-lhe conhecer as condutas e procedimentos passíveis de censura.

Art. 9º Os princípios e valores éticos contidos neste Código, em leis, decretos, políticas e normativos internos deverão ser considerados no exercício das atividades profissionais.

Seção I
Do Ambiente de Trabalho

Art. 10. Pelas características das atividades realizadas pela Empresa, exige-se prontidão e atenção especial em relação às condições do ambiente de trabalho em que são desenvolvidas, sendo necessário aos agentes públicos da Codevasf:

I - zelar pela defesa da vida, pela integridade física e segurança própria, das pessoas com quem se relacionam e das instalações utilizadas;

II - não movimentar ou retirar do lugar próprio qualquer documento ou objeto pertencente a Empresa, sem prévia autorização da autoridade competente;

III - respeitar as normas de segurança do trabalho na realização das atividades diárias, fazendo o uso de uniformes e Equipamentos de Proteção Individual – EPI disponibilizados pela Empresa, quando necessário;

IV - respeitar e zelar pelo fiel cumprimento das normas legais e regulamentares, internas e externas;

V - preservar o meio ambiente, observando e difundindo os normativos ambientais;

VI - não portar armas nos locais de trabalho, quando estas não forem necessárias para as atividades que executa;

VII - não praticar atividades comerciais de compra e venda, oferta de serviços ou propaganda nas dependências da Empresa, ainda que fora do horário de expediente, sem prévia autorização;

VIII - não praticar jogos de azar nas dependências da Empresa;

IX - não consumir, distribuir, comprar ou vender substâncias entorpecentes, mesmo que lícitas, nas dependências da Codevasf ou estar sob o efeito destas substâncias durante a jornada de trabalho; e

X - não fumar no ambiente de trabalho, exceto nas áreas definidas para este fim, quando houver.

Parágrafo único. O consumo moderado de bebidas alcóolicas é permitido em ocasiões oficiais de festividades e comemorações realizadas pela Codevasf.

Seção II
Do Convívio no Ambiente de Trabalho

Art. 11. O convívio no ambiente de trabalho deverá ser alicerçado na cordialidade, no respeito mútuo, na equidade, no bem-estar, na segurança de todos, na colaboração, no espírito de equipe e na busca de um objetivo comum, independentemente da posição hierárquica, emprego, cargo em comissão ou função de confiança.

Art. 12. Constituem condutas a serem observadas pelo agente público da Codevasf:

I - contribuir para um ambiente de trabalho livre de ofensas, difamação, exploração, discriminação, repressão, intimidação, assédio e todo e qualquer tipo de violência;

II - compartilhar com os demais colegas os conhecimentos e as informações necessárias ao exercício das atividades próprias da Empresa, respeitadas as normas relativas ao sigilo;

III - dispensar a outros agentes públicos, ainda que licenciados ou aposentados, assim como os de outros órgãos públicos, o mesmo tratamento conferido ao público em geral, quando estes demandarem serviços da Codevasf;

IV - não permitir que interesses de ordem pessoal, simpatias ou antipatias interfiram no trato com colegas, público em geral e no andamento dos trabalhos;

V - não prejudicar deliberadamente, no ambiente de trabalho ou fora dele, por qualquer meio, a imagem da Empresa ou a reputação de seus agentes públicos;

VI - zelar pela correta utilização de recursos materiais, equipamentos, serviços contratados e veículos oficiais, da Empresa ou de prestadores de serviço, colocados à sua disposição;

VII - respeitar a hierarquia, porém sem nenhum temor de denunciar qualquer ilegalidade ou abuso de poder;

VIII - resistir às pressões de superiores hierárquicos, de contratantes, interessados e outros que visem obter quaisquer favores ou vantagens indevidas;

IX - denunciar atos decorrentes de ações imorais, ilegais ou antiéticas;

X - ser assíduo e se apresentar com vestimentas adequadas ao local de trabalho;

XI - solicitar autorização prévia a chefia imediata para ausentar-se durante o expediente e evitar faltar ao trabalho sem motivo que o justifique; e

XII - promover o Código de Conduta Ética e Integridade, com ampla divulgação aos empregados e demais agentes públicos e privados com quem a Empresa mantém relações de negócio, mediante ações de comunicação e educação.

Art. 13. O agente público que coordenar, supervisionar ou chefiar outros agentes públicos na Codevasf deverá:

I - agir de forma clara e inequívoca, primando pela moralidade e pelo profissionalismo;

II - promover ambiente de trabalho harmonioso, cooperativo, participativo, motivador e produtivo;

III - agir com urbanidade e respeito, tratando as questões individuais com discrição; e

IV - abster-se de conduta que possa caracterizar preconceito, discriminação, constrangimento, assédio de qualquer natureza, desqualificação pública ou pessoal, ofensa ou ameaça, a terceiros ou a outros agentes públicos.

Art. 14. Será vedado ao agente público da Codevasf praticar ou compactuar com atos de assédio moral ou sexual na Empresa.

Seção III
Da Execução das Atividades

Art. 15. O agente público da Codevasf deverá agir de forma objetiva e técnica, com urbanidade e clareza, mantendo conduta moderada e independência profissional, aplicando a legislação em vigor e os normativos internos, em todo seu conjunto, sem se deixar intimidar por interferências ou pressões de qualquer ordem na execução das atividades que lhe forem atribuídas.

Parágrafo único. As decisões estratégicas tomadas pelos agentes públicos deverão se basear em análise de risco, quando disponível, visando a sustentabilidade e a viabilidade das ações da Empresa.

Art. 16. É dever do agente público da Codevasf abster-se de atuar em processos administrativos, participar de comissão de licitação, comissão ou banca de concurso ou da tomada de decisão, quando haja interesse próprio ou de seu cônjuge ou companheiro, parente consanguíneo ou afim, em linha reta ou colateral, até o terceiro grau, amigo íntimo, inimigo notório, credor ou devedor.

Art. 17. Na análise de processos administrativos de qualquer natureza, o agente público da Codevasf deverá agir de forma imparcial, diligente e tempestivo, buscando a veracidade dos fatos, controlando e cumprindo os prazos.

Art. 18. Quando participar de procedimentos correcionais, o agente público da Codevasf deverá agir de forma objetiva e imparcial, com discrição e cordialidade, buscando a veracidade dos fatos, assegurando aos envolvidos o direito ao contraditório e à ampla defesa e resguardando o sigilo das informações.

Seção IV
Do Uso da Autoridade do Cargo, Função ou Emprego

Art. 19. É vedado ao agente público da Codevasf:

I - exercer ou permitir o uso de seu cargo em comissão, função de confiança ou gratificada, e emprego com finalidade estranha ao interesse público, ainda que observadas as formalidades legais.

II - utilizar ou permitir o uso do seu cargo em comissão, função de confiança ou gratificada, emprego, ou do nome da Codevasf para a promoção de opinião, produto, serviço ou empresa própria ou de terceiros;

Parágrafo único. A citação do cargo em comissão, função de confiança ou gratificada, emprego e a emissão de opiniões somente serão permitidas em documentos curriculares, em aulas, palestras e livros, ou em qualquer outra forma de publicação, desde que fique registrado que não refletem o posicionamento da Empresa.

Seção V
Da Promoção da Igualdade e Respeito à Diversidade

Art. 20. Os agentes públicos da Codevasf, a fim de promover a igualdade e o respeito à diversidade, deverão:

I - abster-se de emitir opinião ou de adotar práticas que demonstrem preconceito de origem, raça, sexo, cor, idade, gênero, credo e quaisquer outras formas de discriminação ou que possam perturbar o ambiente de trabalho ou causar constrangimento aos demais agentes públicos; e

II - repudiar toda e qualquer forma de preconceito e discriminação, denunciando os eventuais casos vivenciados ou testemunhados.

Seção VI
Do Relacionamento com o Público

Art. 21. Nas relações estabelecidas com públicos diversos, o agente público da Codevasf deverá apresentar conduta equilibrada e isenta, não participando de transações ou atividades que possam comprometer a sua dignidade profissional ou desabonar a sua imagem pública, bem como a da Empresa.

Parágrafo único. O exercício da função pública deverá ser profissional e se integrar à vida particular de cada agente público, de forma que os fatos e atos verificados na conduta cotidiana da vida privada do agente público poderão influenciar no conceito de sua vida funcional, desde que tenham correlação com sua atividade profissional.

Art. 22. O agente público da Codevasf deverá pautar o seu comportamento consoante as seguintes diretrizes:

I - respeito aos valores, às necessidades públicas e às boas práticas da comunidade, contribuindo para a construção e consolidação de consciência cidadã no relacionamento com a sociedade em geral;

II - respeito às regras protocolares, às competências e à coordenação estabelecida em operação ou evento no relacionamento com autoridades públicas nacionais e estrangeiras;

III - observância às normas e à posição oficial da Empresa no relacionamento com a imprensa, quando se manifestar em nome da Codevasf, tendo o cuidado de não expressar opiniões contra a honra e o desempenho funcional de outro agente público;

IV - comunicação entre agentes públicos da Codevasf e a imprensa, mediante prévia autorização da Empresa;

V - portar-se com urbanidade e cortesia; e

VI - profissionalismo, impessoalidade, publicidade e transparência, com atenção especial quanto aos aspectos legais e contratuais envolvidos, resguardando-se de eventuais práticas desleais ou ilegais de terceiros ao relacionar-se com fornecedores ou prestadores de serviços.

Art. 23. O atendimento ao público deverá ser realizado com agilidade, presteza, qualidade, urbanidade e respeito, fornecendo informações claras e confiáveis, devendo o agente público atuar de modo a harmonizar as relações entre o cidadão e a Codevasf.

Parágrafo único. Durante o atendimento, o agente público da Codevasf deverá adotar, entre outras, as seguintes condutas:

I - evitar interrupções por razões alheias ao atendimento;

II - ser claro em seus posicionamentos e opiniões, mantendo a discrição, com vistas a motivar respeito e confiança do público em geral;

III - agir com profissionalismo em situações de conflito, procurando manter o controle emocional; e

IV - orientar e encaminhar corretamente o cidadão quando o atendimento precisar ser realizado por outra unidade ou órgão.

Seção VII
Do Relacionamento com Clientes e Fornecedores

Art. 24. No relacionamento com clientes e fornecedores, são condutas esperadas dos agentes públicos da Codevasf:

I - colaborar com as condições adequadas para que fornecedores desempenhem suas atividades de forma apropriada;

II - visitar ou reunir-se com clientes ou fornecedores, mediante autorização do superior hierárquico, seja por motivos de ordem técnica ou comercial, acompanhados de pelo menos mais um empregado da Empresa;

III - conduzir as reuniões do processo de contratação ou negociação, formalmente, com registro em ata e sempre na presença de, no mínimo, 2 (dois) agentes públicos da Codevasf;

IV - não prestar qualquer tipo de assessoramento ou auxílio profissional a clientes ou fornecedores, exceto quando previsto em contrato ou expressamente autorizado pela autoridade competente;

V - comunicar ao superior hierárquico condutas ou comportamentos inadequados por parte de clientes ou fornecedores;

VI - observar estritamente as condições contratuais; e

VII - orientar clientes e fornecedores em relação à observância deste Código e demais normativos internos, no que for aplicável.

Art. 25. Nos processos de contratação de bens e serviços, o agente público da Codevasf deve atuar com isonomia, cumprindo as normas internas e externas, sem favorecer ou prejudicar qualquer concorrente.

Seção VIII
Das Publicações e Autoria de Iniciativas e Trabalhos

Art. 26. O agente público deverá assumir a execução e autoria de seus trabalhos.

Art. 27. A divulgação ou publicação de dados, programas de computador, metodologias de trabalho ou informações produzidas no exercício das atividades da Empresa ou na participação em projetos institucionais, inclusive aqueles desenvolvidos em parceria com outros órgãos, deverão ser previamente autorizadas, ressalvadas as situações de interesse institucional.

Art. 28. O agente público da Codevasf, que na elaboração de documentos citar trechos de obras protegidas por leis de direitos autorais ou de propriedade intelectual, deverá indicar a sua autoria e origem.

Art. 29. O agente público da Codevasf deverá respeitar a autoria de iniciativas, trabalhos ou soluções de problemas apresentados por outros agentes públicos, conferindo-lhes os respectivos créditos.

Parágrafo único. O disposto no caput não se aplica à reprodução parcial ou integral de textos produzidos para a Codevasf em despachos, processos administrativos, pareceres e documentos assemelhados.

Seção IX
Do Sigilo das Informações

Art. 30. O agente público da Codevasf deverá adotar as seguintes condutas:

I - guardar sigilo sobre as informações a que tiver acesso ou conhecimento em função de suas atribuições, preservando o sigilo de acordo com as normas vigentes na Empresa;

II - não divulgar, repassar ou comentar informações privilegiadas ou relativas a atos ou fatos relevantes, com repercussão econômica e/ou financeira e que não tenham sido tornados públicos;

III - respeitar o sigilo profissional; e

IV - guardar segredo sobre as informações pessoais de qualquer outro agente público da Codevasf às quais tenham acesso em razão de cargo em comissão, função de confiança ou gratificada e/ou atividade desenvolvida, excetuando-se as situações previstas em lei.

Seção X
Da Segurança das Informações

Art. 31. Constituem condutas a serem adotadas pelo agente público da Codevasf:

I - observar os protocolos de segurança relacionados com a utilização de sistemas de Tecnologia da Informação - TI e equipamentos;

II - não compartilhar senhas, ou permitir o acesso ou uso não autorizado dos sistemas de TI;

III - comunicar ao seu superior hierárquico ou à autoridade competente:

a) o desaparecimento ou a suspeita de perda de informação e/ou de equipamentos que contenham informações pessoais ou privilegiadas;

b) qualquer forma de manipulação indevida ou desvio do uso de informação por outro agente público; e

c) situações de vulnerabilidade ou fragilidade de seu conhecimento e que coloque as informações sob o risco de serem violadas ou acessadas por pessoas não autorizadas.

IV - não alterar ou destruir documentos originais de valor probatório, mantendo-os em arquivo pelos prazos definidos por normativo interno e pela legislação aplicada.

Seção XI
Do Uso da Rede Corporativa e dos Meios Digitais

Art. 32. Será vedado aos agentes públicos da Codevasf o uso dos recursos de hardware e software disponibilizados pela Empresa para:

I - fazer uso particular em atividades comerciais de compra e venda, oferta de serviços ou propaganda;

II - obter, armazenar, utilizar ou repassar material que viole leis de direitos autorais ou de propriedade intelectual;

III - obter, armazenar, utilizar ou repassar material que tenha conteúdo pornográfico, de exploração sexual, racista, homofóbico, sexista, político-partidário, contra a liberdade religiosa ou que atente contra a diversidade;

IV - usar do anonimato para envio de mensagens ou postagem de conteúdos que contrariem os interesses da Empresa, resguardados os casos previstos neste Código;

V - enviar mensagens ofensivas por meio de correio eletrônico corporativo;

VI - obter ou propagar intencionalmente vírus e similares;

VII - tentar invadir, violar sistemas ou controles de segurança;

VIII - fornecer ou utilizar senhas de terceiros para obter acesso a sistemas ou computadores;

IX - enviar, transmitir, distribuir, disponibilizar ou armazenar na internet ou em outros meios digitais, informações, dados, segredos comerciais, financeiros ou tecnológicos ou quaisquer outras informações pertencentes à Codevasf, salvo se expressamente autorizado pelo gestor da respectiva informação;

X - utilizar a rede corporativa e os meios digitais disponibilizados pela Empresa para acessar serviços de telefonia via internet que não sejam autorizados pela Codevasf; e

XI - praticar atividades de caráter político-partidário, religioso, de autoajuda e para a propagação de “correntes”.

Art. 33. O uso dos recursos de hardware e software disponibilizados pela Empresa poderá ocorrer para fins particulares, desde que não prejudique ou atente contra:

I - a legislação;

II - a imagem e reputação da Empresa ou de sua força de trabalho;

III - a imagem de terceiros;

IV - as atividades ou processos de trabalho da Empresa; e

V - a segurança das informações e dos recursos corporativos.

Seção XII
Da Participação em Eventos

Art. 34. As despesas relacionadas à participação de agente público da Codevasf em eventos como seminários, congressos, palestras, visitas e reuniões técnicas, no Brasil ou no exterior, que guardem correlação com as atribuições de seu cargo em comissão, emprego ou função de confiança ou gratificada, ou que sejam de interesse da Codevasf deverão ser custeadas, preferencialmente, pela Empresa.

§1º As despesas relativas a transporte, alimentação, hospedagem e inscrição do agente público, excepcionalmente, poderão ser custeadas pela instituição promotora do evento, no todo ou em parte, sendo vedado o recebimento de remuneração, se esta for:

a) organismo internacional do qual o Brasil faça parte;

b) governo estrangeiro e suas instituições;

c) instituição acadêmica, científica e cultural; ou

d) empresa, entidade ou associação de classe que não esteja sob a jurisdição regulatória da Codevasf, ou que possa ser beneficiária de decisão da qual participe o agente público, seja individual ou coletivamente.

§2º O agente público da Codevasf poderá aceitar descontos de transporte, hospedagem e refeição, bem como de taxas de inscrição, desde que não sejam em benefício pessoal.

Art. 35. A prestação de contas de afastamentos custeados com recursos públicos (passagens, diárias, hospedagem, dentre outros) será, obrigatoriamente, realizada pelo agente público da Codevasf nos prazos e formas determinados pelos normativos vigentes.

Seção XIII
Do Recebimento de Presentes e Outros Benefícios

Art. 36. O agente público da Codevasf não poderá exigir, aceitar, solicitar ou receber presente de qualquer valor ou qualquer tipo de ajuda financeira, gratificação, prêmio, comissão,

doação ou vantagem de qualquer espécie, para si, familiares ou qualquer pessoa, quando o ofertante for pessoa, empresa ou entidade que:

I - tiver interesse pessoal, profissional ou empresarial em decisão que possa ser tomada pelo agente público, individual ou coletivamente;

II - mantiver relação comercial com a Codevasf; ou

III - representar o interesse de terceiros, como procurador ou preposto, de pessoas, empresas ou entidades compreendidas nos incisos I e II.

§1º O recebimento de presentes será permitido nas seguintes situações:

I - em razão de laços de parentesco ou amizade, desde que o seu custo seja arcado pelo próprio ofertante, e não por pessoa, empresa ou entidade que se enquadre em qualquer das hipóteses previstas nos incisos de I a III do art. 36; e

II - quando ofertados por autoridades estrangeiras, nos casos protocolares em que houver reciprocidade ou em razão do exercício de funções diplomáticas.

§2º Nos casos em que o presente não possa, por qualquer razão, ser recusado ou devolvido sem ônus para o agente público, o fato deverá ser comunicado por escrito à chefia da unidade orgânica de sua lotação e o material entregue à unidade responsável pelas atividades de patrimônio e almoxarifado que providenciará a emissão de recibo e os devidos registros e destinações legais.

§3º Para fins deste Código, não são caracterizados como presente:

I - prêmio em dinheiro ou bens concedidos ao agente público por entidade acadêmica, científica ou cultural, em reconhecimento por sua contribuição de caráter intelectual;

II - prêmio concedido em razão de concurso de acesso público a trabalho de natureza acadêmica, científica, tecnológica ou cultural; e

III - bolsa de estudos vinculada ao aperfeiçoamento profissional ou técnico do agente público, desde que o patrocinador não tenha interesse em decisão que possa ser tomada pelo agente público, em razão do cargo em comissão, função de confiança ou gratificada ou emprego que exerce.

Art. 37. O agente público da Codevasf poderá aceitar brindes desde que:

I - não tenham valor comercial ou sejam distribuídos por entidade de qualquer natureza a título de cortesia, propaganda, divulgação habitual ou por ocasião de eventos ou datas comemorativas de caráter histórico ou cultural, desde que não ultrapassem o valor unitário de R$ 100,00 (cem reais), conforme estabelecido na Resolução nº 3, de 23/11/2000, elaborada pela Comissão de Ética Pública, da Casa Civil, Subchefia para Assuntos Jurídicos, que trata das regras sobre o tratamento de presentes e brindes aplicáveis às autoridades públicas abrangidas pelo Código de Conduta da Alta Administração Federal;

II - tenham periodicidade de distribuição não inferior a 12 (doze) meses; e

III - sejam de caráter geral ou que não se destinem exclusivamente a um determinado agente público da Codevasf.

§1º Caso o valor do brinde ultrapasse o valor previsto no inciso I do art. 37, ele será tratado como presente, e será aplicado o disposto no artigo 36.

§2º O agente público não deverá vincular o uso do brinde, ainda que recebido a título de propaganda, à imagem institucional da Codevasf e de seus agentes públicos no exercício de suas atribuições.

Seção XIV
Do Conflito de Interesses

Art. 38. Com vistas a prevenir ou impedir possível conflito de interesses, o agente público da Codevasf não deverá:

I - envolver-se direta ou indiretamente em qualquer atividade que seja conflitante com os interesses da Codevasf;

II - divulgar ou fazer uso de informação privilegiada, em proveito próprio ou de terceiros, obtida em razão das atividades exercidas;

III - exercer atividade que implique na prestação de serviços ou na manutenção da relação de negócio com pessoa física ou jurídica, que tenha interesse em decisão da qual participa, seja individual ou coletivamente, ou da unidade orgânica de sua lotação;

IV - desempenhar, direta ou indiretamente, atividade que em razão da sua natureza seja incompatível com as atribuições do cargo em comissão, da função de confiança ou gratificada, ou do emprego que exerce;

V - atuar, ainda que informalmente, como procurador, consultor, assessor ou intermediário de interesses privados na Codevasf;

VI - praticar ato em benefício de pessoa jurídica da qual ele participe, ou seu cônjuge, companheiro ou parentes, consanguíneos ou afins, em linha reta ou colateral, até o terceiro grau, e que possa ser por ele beneficiada ou influenciada em seus atos de gestão; e

VII - prestar serviços, ainda que eventuais, à empresa cuja atividade seja controlada ou fiscalizada pela Codevasf.

Art. 39. O agente público da Codevasf, em casos de dúvidas, deverá consultar a Comissão de Ética da Codevasf ou a Comissão de Ética Pública sobre a existência de conflito de interesses e pedido de autorização para o exercício de atividade privada, observada a legislação vigente

Parágrafo único. A consulta citada no caput também será aplicada aos agentes públicos da Codevasf em gozo de licença para tratar de interesses particulares.

Seção XV
Da Fraude e Corrupção

Art. 40. Com vistas a evitar a ocorrência de fraude e/ou corrupção, é vedado aos agentes públicos da Codevasf:

I - insinuar, prometer, oferecer, pagar ou dar, direta ou indiretamente, vantagem a agente público, nacional ou estrangeiro, ou a pessoa a ele relacionada;

II - solicitar, aceitar ou receber, direta ou indiretamente, suborno, propina ou qualquer vantagem indevida ou promessa de tal vantagem em razão de função pública exercida; e

III - aceitar qualquer tipo de cortesia, transporte ou hospedagem de empresa que possa participar de processo licitatório ou de outra forma de aquisição de bens e serviços, exceto quando legalmente previsto;

Art. 41. Os agentes públicos da Codevasf deverão denunciar qualquer situação de fraude ou corrupção que tiverem conhecimento, sob qualquer forma, direta ou indiretamente, que envolva ou não valores monetários.

Parágrafo único. Os agentes públicos deverão estabelecer diligências administrativas com vistas à prevenção de fraude e corrupção nos acordos e contratos firmados com terceiros, sendo, ainda, que resultados e constatações em desvio aos ditames deste código e ao cumprimento de normativos da Empresa deverão ser encaminhados para conhecimento da Secretaria de Integridade, Riscos e Controles Internos – PR/SRC.

Seção XVI
Do Nepotismo

Art. 42. Será vedado aos agentes públicos da Codevasf:

I - nomear, designar, contratar ou influenciar, direta ou indiretamente, na contratação de pessoa física ou jurídica cujo administrador ou sócio com poder de direção seja parente consanguíneo ou por afinidade de:

a) qualquer agente público que exerça função de confiança em unidade orgânica da Empresa responsável por demandar aquisições ou contratações e realizar procedimentos licitatórios, inclusive de dispensa ou inexigibilidade de licitação; e

b) agente público da Codevasf responsável pela autorização da contratação e/ou pela assinatura do contrato.

II - realizar nomeações ou designações recíprocas entre as unidades orgânicas da Codevasf, mediante ajustes recíprocos caracterizando tal prática como nepotismo cruzado.

Seção XVII
Das Atividades Políticas e Religiosas

Art. 43. Em relação às atividades políticas e religiosas será vedado aos agentes públicos da Codevasf:

I - promover ou participar de atividades político-partidárias ou religiosas durante o expediente e no local de trabalho ou fazer uso dos recursos da Codevasf com esta finalidade, ou mesmo associá-la à sua imagem;

II - realizar qualquer tipo de propaganda político-partidária ou religiosa nas dependências da Codevasf.

Parágrafo único. Em casos excepcionais, a realização de atividades religiosas poderão ser autorizadas pela Empresa.

CAPÍTULO V
DAS VIOLAÇÕES AO CÓDIGO DE CONDUTA ÉTICA E INTEGRIDADE

Art. 44. As condutas que possam configurar violação a este Código serão apuradas, de ofício ou em razão de denúncia fundamentada, pela Comissão de Ética Codevasf, nos termos do seu Regimento Interno, que poderá ensejar:

I - na aplicação da pena de censura ética; ou

II - na recomendação para se adotar a conduta adequada.

Parágrafo único. Se a conclusão for pela existência de falta ética, além das providências previstas neste Código, no Código de Conduta da Alta Administração Federal e no Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal, a Comissão de Ética da Codevasf tomará as seguintes providências, no que couber:

I - sugerir à autoridade hierarquicamente superior ao agente público na Codevasf a sua exoneração, se ocupante de cargo em comissão ou função de confiança ou gratificada, ou a devolução ao órgão de origem, se agente público cedido de outro órgão;

II - encaminhar o processo de apuração a Controladoria-Geral da União - CGU ou, conforme o caso, a outra unidade do Sistema de Correição do Poder Executivo Federal, para exame de eventuais transgressões disciplinares; e

III - recomendar a abertura de processo administrativo próprio, em caso de indícios de infração disciplinar.

Art. 45. As condutas que possam configurar violações disciplinares, ou a este Código, serão encaminhadas à Ouvidoria da Codevasf – CONSAD/OUV, para fins de registro, e à Corregedoria da Codevasf - PR/COR para providências quanto à apuração disciplinar.

Art. 46. A Comissão de Ética da Codevasf não poderá deixar de proferir decisão sobre matéria de sua competência, alegando omissão por parte deste Código, do Código de Conduta da Alta Administração Federal ou do Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal.

Parágrafo único. Caso ocorra a omissão prevista no art. 46, esta será resolvida por analogia e invocação aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência.

Art. 47. A Comissão de Ética da Codevasf em casos de dúvida quanto à legalidade de suas decisões deverá ouvir, previamente, a Assessoria Jurídica da Codevasf.

Art. 48. A Comissão de Ética de Codevasf comunicará à Comissão de Ética Pública as situações que possam configurar descumprimento do Código de Conduta da Alta Administração Federal.

CAPÍTULO VI
DAS DENÚNCIAS

Seção I
Dos Canais de Comunicação e Denúncia

Art. 49. Os agentes públicos da Codevasf que testemunharem, tomarem conhecimento ou sofrerem com alguma conduta que configure descumprimento às orientações deste Código deverão comunicar ou denunciar o fato aos superiores hierárquicos, à Ouvidoria e/ou à Comissão de Ética da Codevasf, com a utilização dos seguintes canais:

I - Ouvidoria da Codevasf: https://sistema.ouvidorias.gov.br; e

II - Comissão de Ética da Codevasf: etica@codevasf.gov.br ou pela intranet http://srv122/etica/.

Parágrafo único. Ao comunicante ou denunciante será assegurado a confidencialidade do fato relatado.

Art. 50. A Codevasf acolherá a comunicação ou denúncia de desvio de conduta ou de indícios de desvio de conduta feita de boa-fé, e não admitirá retaliações ou punições contra quaisquer pessoas que apresentem essa comunicação ou denúncia.

§1º Os empregados que causarem retaliações ou punições ao comunicante ou denunciante, se identificados, poderão sofrer sanção disciplinar.

§2º Qualquer pessoa física ou entidade regularmente constituída é parte legítima para formular denúncia sobre violações a este Código à Ouvidoria e/ou à Comissão de Ética da Codevasf.

Seção II
Do Tratamento das Denúncias

Art. 51. A Codevasf garantirá o anonimato do denunciante por prazo indeterminado e a confidencialidade do processo de investigação e de apuração de responsabilidades, até a publicação da decisão administrativa definitiva.

§1º Os processos instaurados para apuração de prática em desrespeito ao presente Código e às normas éticas serão considerados “reservados”, conforme legislação específica, até que sejam concluídos.

§2º A Ouvidoria e/ou Comissão de Ética da Codevasf, depois de concluído o processo apuratório, providenciará(ão) o desentranhamento dos documentos dos autos, mantendo-os lacrados e protegidos de forma a resguardar o devido sigilo.

§3º A qualquer pessoa que esteja sendo investigada será assegurado o direito de saber o que lhe está sendo imputado, de conhecer o teor da acusação e de ter vista aos autos, no recinto da Comissão de Ética da Codevasf, mesmo que ainda não tenha sido notificada da existência do procedimento investigatório, como também de obter cópia dos autos e de certidão do seu teor, ressalvado o disposto no artigo 52.

Art. 52. Ao denunciante, sempre que solicitado, será garantido o acesso restrito à sua identidade e às demais informações pessoais constantes das denúncias.

§1º Nos casos em que for adotado reserva de identidade, a Codevasf deverá encaminhar a denúncia aos órgãos de apuração sem o nome do denunciante.

§2º Nos casos de adoção de reserva de identidade em que a identificação do denunciante for indispensável à apuração dos fatos e houver justificativa formal, o nome do denunciante será encaminhado ao órgão de apuração, que ficará responsável por restringir o acesso à identidade do denunciante a terceiros.

§3º A restrição de acesso estabelecida no caput deste dispositivo não se aplica caso se configure denúncia caluniosa ou flagrante má-fé por parte do denunciante.

CAPÍTULO VII
DAS DISPOSIÇÕES GERAIS

Art. 53. O agente público da Codevasf poderá consultar a Comissão de Ética da Codevasf, em caso de dúvida quanto à aplicação deste Código e em situações que possam configurar desvio de conduta.

Art. 54. A Comissão de Ética da Codevasf será responsável por garantir a aplicação deste Código.

Art. 55. A Comissão de Ética da Codevasf deverá propor atualizações a este Código, a cada 3 (três) anos, devendo ser aprovado pelo Conselho de Administração da Codevasf – Consad.

Parágrafo único. Após a revisão do Código, deverá ser dada ampla publicidade aos empregados e demais agentes públicos e privados que mantêm relações de negócio com a Empresa.

Art. 56. Os agentes públicos da Codevasf deverão cumprir o estabelecido neste Código, consoante a assinatura do “Termo de Adesão ao Código de Ética e Integridade da Codevasf” - Anexo I, que poderá ser realizada eletronicamente, por meio de link disponibilizado na intranet da Codevasf no ato de posse, investidura em função pública ou celebração de contrato de trabalho, devendo a renovação do temo de ciência ocorrer a cada alteração deste Código.

§1º A posse em cargo ou função pública que submeta o agente público da Codevasf às normas do Código de Conduta da Alta Administração Federal deverá ser precedida de consulta à Comissão de Ética Pública, acerca de alguma situação que possa suscitar conflito de interesses.

§2º A Área de Gestão Administrativa e Suporte Logístico – AA, com o auxílio da Comissão de Ética da Codevasf, adotará as medidas necessárias ao cumprimento do disposto no §2º.

Art. 57. A Área de Gestão Administrativa e Suporte Logístico – AA, com o auxílio da Comissão de Ética da Codevasf, será responsável pela promoção de treinamento, no mínimo uma vez ao ano, sobre o Código de Conduta Ética e Integridade para todos os agentes públicos da Codevasf, conforme disposto na legislação.

Art. 58. Os contratos, convênios e instrumentos congêneres conterão cláusulas específicas que imponham a obrigação aos contratados/convenentes e assemelhados de assinarem o "Termo de Observância ao Código de Conduta Ética e Integridade da Codevasf" – Anexo II.

§1º O Termo previsto no caput deste artigo deverá ser anexado ao processo relativo ao instrumento firmado.

§2º Os termos aditivos dos contratos, convênios e instrumentos congêneres, celebrados após a aprovação deste Código, deverão incluir cláusulas específicas que contenham as obrigações a que se refere o caput.

§3º O descumprimento deste Código por empregado de empresa contratada pela Codevasf deverá ser comunicado formalmente ao representante legal da contratada.

Art. 59. Os editais de concursos ou de processos seletivos para contratação de empregados pela Codevasf deverão fazer expressa referência a este Código como conteúdo programático do concurso ou do processo seletivo.

Art. 60. No processo de ambientação de novos empregados, a Codevasf promoverá ampla divulgação deste Código.

Art. 61. Os processos de apuração de violações a este Código estão sujeitos à Lei nº 12.527, de 18 de novembro de 2011, e ao Decreto nº 7.724, de 16 de maio de 2012, quanto ao acesso das informações neles contidas, e observarão as formalidades exigidas pelo Decreto nº 6.029, de 1º fevereiro de 2007, e pela Lei nº 8.429, de 2 de junho de 1992, Lei nº 9.784, de 29 de janeiro de 1999, Lei nº 13.303 de 30 de junho de 2016 e pela Constituição da República Federativa do Brasil de 1988.

Art. 62. O presente Código de Conduta Ética e Integridade entra em vigor na data de sua aprovação pelo Conselho de Administração.

Art. 63. As dúvidas de interpretação quanto ao mérito técnico e operacional serão dirimidas pela Comissão de Ética da Codevasf e pela Secretaria de Gestão de Integridade,

Riscos e Controles Internos – PR/SRC de acordo com a sua competência, quanto ao mérito redacional pela Área de Gestão Estratégica - AE e quanto ao mérito jurídico pela Assessoria Jurídica - PR/AJ.

Art. 64. Orientações técnicas quanto à condução do Programa e do Plano de Integridade da Codevasf poderão ser obtidas na Secretaria de Gestão de Integridade, Riscos e Controles Internos – PR/SRC.

Art. 65. Os casos omissos serão dirimidos pela Comissão de Ética de Codevasf.

ANEXO I - Termo de Adesão ao Código de Conduta Ética e Integridade da Codevasf

Nome do agente público:

Cargo/ Emprego/ Função:

Cadastro nº:

Área ou Superintendência Regional/Unidade de Lotação:

Declaro que li e estou ciente e de acordo com as normas, políticas e práticas estabelecidas no Código de Conduta Ética e Integridade da Codevasf e comprometo-me a respeitá-las e cumpri-las integralmente.

Compreendo que o presente Código de Conduta Ética e Integridade da Codevasf reflete o compromisso com a dignidade, o decoro, o zelo, a eficácia e a consciência dos princípios morais que devem nortear o agente público, seja no exercício do cargo em comissão, função de confiança ou gratificada ou emprego, ou fora dele. E, ainda, que seus atos, comportamentos e atitudes devem ser direcionados para a preservação da honra e da tradição dos serviços públicos.

Assumo, também, a responsabilidade de denunciar à Ouvidoria e/ou Comissão de Ética da Codevasf, qualquer comportamento ou situação que esteja em desacordo com as disposições estabelecidas no Código de Conduta Ética e Integridade da Codevasf, por meio dos seguintes canais:

- Ouvidoria da Codevasf: https://sistema.ouvidorias.gov.br
- Comissão de Ética da Codevasf: etica@codevasf.gov.br ou pela intranet: http://srv122/etica/.

A assinatura deste Termo é expressão de livre consentimento e concordância quanto ao cumprimento das normas, políticas e práticas estabelecidas no Código de Conduta e Integridade da Codevasf.

Brasília, XX de XX 20XX.

Assinatura do agente público

Nome completo

ANEXO II - Termo de Observância ao Código de Conduta Ética e Integridade da Codevasf

Nº do Instrumento (contrato, convênio ou instrumento congênere):

Período de Vigência do Instrumento:

Finalidade do Instrumento:

A pessoa física/jurídica _____, CPF/CNPJ nº _____, por meio de seu representante legal abaixo subscrito, vem afirmar aderência, ciência e concordância com as normas, políticas e práticas estabelecidas no Código de Conduta Ética e Integridade da Codevasf e compromete-se a respeitá-las e cumpri-las integralmente, bem como fazer com que seus empregados o façam quando no exercício de suas atividades nas dependências da Codevasf ou para a Empresa.

Compreendo que o Código de Conduta Ética e Integridade da Codevasf reflete o compromisso com a dignidade, o decoro, o zelo, a eficácia e a consciência dos princípios morais que devem nortear o serviço público, seja no exercício do cargo em comissão, função de confiança ou gratificada ou emprego, ou fora dele, comprometendo-se a atuar contrariamente a quaisquer manifestações de corrupção e conhecer e cumprir as normas previstas na Lei 12.846/2013 ("Lei Anticorrupção"), regulamentada pelo Decreto nº 8.420/2015.

Assumo, também, a responsabilidade de denunciar à Ouvidoria e/ou Comissão de Ética da Codevasf sobre qualquer comportamento ou situação que esteja em desacordo com as disposições do Código de Conduta Ética e Integridade da Codevasf, por meio dos seguintes canais:

- Ouvidoria da Codevasf: https://sistema.ouvidorias.gov.br
- Comissão de Ética da Codevasf: etica@codevasf.gov.br ou pela intranet: http://srv122/etica/.

A assinatura deste Termo é expressão de livre consentimento e concordância do cumprimento das normas, políticas e práticas estabelecidas no Código de Conduta Ética e Integridade da Codevasf.

Brasília, _____ de _____ de _____.

_____

Assinatura do responsável/representante legal

Nome completo: XXXXXXXXXXXX

CPF: XX.XXX.XXX-XX

Cargo: XXXXXXXXXXXXXXXXXXXXX