

ANEXO III

ESPECIFICAÇÃO DOS REQUISITOS MÍNIMOS PARA SOLUÇÃO DE FIREWALL

OBJETIVO

Este anexo descreve as especificações técnicas para a aquisição de solução de *firewall* (gerência, prevenção avançada de ameaças, sistema de detecção e prevenção de intrusões – IDS/IPS, filtro avançado de URL, filtro avançado de DNS, acesso remoto/VPN, com suporte, manutenção e treinamento em Brasília-DF.

1 – REQUISITOS MÍNIMOS NECESSARIOS

ITEM 1 - Fornecimento de solução de *firewall* (gerência, sistema de detecção e prevenção de intrusões – IDS/IPS, prevenção avançada de ameaças, filtro avançado de URL, filtro avançado de DNS, acesso remoto/VPN, por 5 anos.

Este item contempla a aquisição de uma solução unificada de segurança de perímetro (Firewall de Próxima Geração - NGFW), fornecida como um serviço contínuo pelo período de 5 (cinco) anos. O objetivo é consolidar múltiplas funções de segurança em uma única plataforma, garantindo a proteção robusta da infraestrutura de rede da CONTRATANTE contra um amplo espectro de ameaças cibernéticas, tanto conhecidas quanto desconhecidas. A solução deverá integrar os seguintes componentes, que serão detalhados subsequentemente:

Característica/Recurso	Capacidade Mínima
<i>Throughput</i> de prevenção de ameaças <i>firewall</i>	2.5 Gbps
VPN <i>throughput</i>	3.0 Gbps
IPS <i>throughput</i>	4.0 Gbps
Sessões simultâneas (TCP) (conexões concorrentes TCP)	900.000
Novas Sessões/Segundo (TCP)	90.000
Usuários VPN	1.000
Portas (interfaces)	8×GE RJ-45 (incluindo gestão/HA), 2×GE SFP, 4×10 GE SFP+ ou 12×GE RJ-45 (incluindo gestão/HA), 4×10 GE SFP+
Armazenamento	SSD 120 GB

Tabela 1

1.1. Gerência e Monitoramento

- 1.1.1. **Descrição:** plataforma de gerenciamento para gestão de políticas e regras, monitoramento de logs.
- 1.1.2. **Monitoramento em Tempo Real:** visibilidade em tempo real do tráfego de rede.
- 1.1.3. **Envio de Logs:** envio de logs para outras soluções, como repositórios de logs ou soluções *SIEM*, usando protocolos padrão de mercado para isso, como *Syslog*.
- 1.1.4. **Alertas:** deve ser possível configurar o envio de alertas do sistema via e-mail;
- 1.1.5. **Monitoramento de Performance:** a máquina deve permitir seu monitoramento através do protocolo *SNMP* (versão 2 e 3), enviando informações de performance da máquina como:

1.1.5.1. Tráfego em cada uma de suas interfaces de rede.

1.1.5.2. Uso de todas as unidades de processamento (CPUs, NPUs, ASICs e similares).

1.1.5.3. Uso de armazenamento.

1.1.5.4. Número de sessões correntes.

1.1.6. **Gerência:** os *appliances* devem permitir acesso ao equipamento via interface de linha de comando (CLI), console, SSH além de interface web HTTPS.

1.1.6.1. A solução de firewall deve ser gerenciada por uma console gráfica web (GUI) que permita a configuração completa do equipamento. As funções devem incluir a criação e administração de políticas (*firewall*, aplicações, IPS, antivírus, *anti-spyware*, filtro URL), além do monitoramento, investigação de logs e demais configurações.

1.1.6.2. O firewall deve permitir autenticação via *Active Directory*, *LDAP*, e *SAML*.

1.1.6.3. O firewall deve armazenar registros das alterações de configurações e outras ações dos administradores da solução.

1.1.6.4. A interface de gerenciamento deve permitir a criação de perfis de acesso com permissões granulares. Isso deve possibilitar a definição de papéis distintos, como "somente leitura", "leitura e escrita", ou permissões específicas para tarefas como "criação de usuários" e "alteração de configurações".

1.1.6.5. A interface de gerenciamento do equipamento deve permitir a geração de relatórios, como resumos gráficos de aplicações e ameaças, principais aplicações por uso de banda e atividades de usuários (incluindo aplicações e URLs). Além disso, deve ser possível criar relatórios personalizados.

1.1.6.6. A interface gráfica de gerenciamento deve exibir, em tempo real, as principais aplicações acessadas, o risco associado a elas, o número de sessões simultâneas, o *status* das interfaces de rede e o uso de CPU. Essas informações devem ser atualizadas automaticamente a cada 1 (um) minuto.

1.1.6.7. A solução deve permitir o armazenamento de logs e registros (de controle de acesso, de prevenção de ameaças e de auditoria) por, no mínimo, 365 dias, de maneira nativa ou integrada a partir de solução do mesmo fabricante. Os relatórios gerados pela ferramenta devem ter como insumo registros dos últimos 365 dias de funcionamento da solução.

1.2. Sistema de Detecção e Prevenção de Intrusões – IDS/IPS

1.2.1. **Descrição:** assinatura do serviço de Sistema de Prevenção de Intrusões (IPS) para inspeção de tráfego em linha e em tempo real, projetada para identificar, registrar e bloquear assinaturas de ataques, *exploits* de vulnerabilidades conhecidas, varreduras de rede e anomalias de protocolo.

1.2.2. Funcionalidades de Prevenção de Intrusões

1.2.2.1. **Proteção Baseada em Assinaturas:** detecção e bloqueio de uma biblioteca abrangente de assinaturas de ameaças conhecidas, incluindo *exploits* de sistemas operacionais e aplicações, *malware* de rede e tráfego de comando e controle (C2).

1.2.2.2. **Análise de Anomalia de Protocolo:** capacidade de identificar tráfego que não está em conformidade com os padrões de protocolo RFC como uso de portas não padrão e comandos de protocolo malformados, indicando tentativas de evasão.

1.2.2.3. **Proteção Baseada em Vulnerabilidades:** as assinaturas devem ser capazes de bloquear ameaças com base na vulnerabilidade-alvo (identificador CVE), e não apenas em uma variante específica, protegendo contra futuras variações do mesmo ataque.

1.2.2.4. Proteção contra Negação de Serviço (DoS): capacidade de detectar e mitigar ataques de negação de serviço em nível de rede e aplicação, como inundações SYN (*SYN floods*), UDP *floods* e varreduras de porta (*port scans*).

1.2.2.5. Atualizações Automáticas de Assinaturas: a solução deve receber atualizações de assinaturas de ameaças de forma automática, regular, garantindo proteção contra os ataques mais recentes sem intervenção manual.

1.2.2.6. Aplicação Granular de Políticas: permissão para aplicar perfis de IPS distintos por regra de firewall, zona de segurança, origem, destino ou aplicação, e capacidade de configurar exceções e ações (bloquear, alertar, redefinir conexão).

1.2.2.7. Registro e Alertas: Geração de logs detalhados e alertas em tempo real para todas as ameaças detectadas e bloqueadas, com integração à plataforma de gerenciamento.

1.3. Prevenção avançada de ameaças

1.3.1. Descrição: assinatura para prevenção avançada de ameaças, protegendo contra ameaças conhecidas e desconhecidas.

1.3.2. Funcionalidades de segurança

1.3.2.1. Proteção multicamadas: análise de *malware*, *exploits* e ataques *zero-day*.

1.3.2.2. Análise em tempo real: monitoramento contínuo e detecção de ameaças sem impacto no desempenho.

1.3.2.3. Análise em Sandbox: realiza a execução e observação de arquivos em um ambiente virtual isolado na nuvem, projetado para resistir a técnicas de evasão e identificar ameaças desconhecidas e *malware zero-day*.

1.3.2.4. Proteção de tráfego criptografado: inspeção profunda de tráfego HTTPS e TLS/SSL, para evitar que ameaças *bypass*em a segurança.

1.3.2.5. Alertas automatizados: notificações de alertas de detecção de ameaças.

1.3.2.6. Proteção contra botnets: o firewall deve ter inteligência para identificar e bloquear ataques provenientes de bots/botnets.

1.3.2.7. Proteção de downloads: o firewall deve implementar um controle de arquivos baseado em políticas que considere tanto a aplicação quanto a extensão do arquivo. A solução deve permitir, por exemplo, o bloqueio de transferências de *.exe* via navegador web, ao mesmo tempo que suporta o bloqueio de extensões como: *.exe*, *.com*, *.bat*, *.cmd*, *.msi*, *.dll*, *.pdf*, *.pif*, *.jar*, *.js*, *.jsp*, *.vbs*, *.ps1*, *.sh*, *.rar*, *.zip*, *.7z*, *.gz*, *.tar* e *.torrent*.

1.4. Filtro avançado de URL

1.4.1. Descrição: assinatura para filtragem avançada de URLs, permitindo proteção detalhada contra ameaças veiculadas por links. Identifica, categoriza e bloqueia em tempo real URLs maliciosas ou indesejadas.

1.4.2. Capacidades de filtragem

1.4.2.1. Detecção e Bloqueio de URLs Maliciosas: monitoramento constante para impedir acesso a URLs maliciosas e sites de *phishing*.

1.4.2.2. Categorias de Filtragem: 60+ categorias de conteúdo, com opções de bloqueio, alerta ou permissão, conforme as políticas.

1.4.2.3. Identificação de Conteúdo Dinâmico: proteção contra novos domínios e sites criados para ataques de curto prazo.

1.4.3. Relatórios de Uso de Web: visualização detalhada do tráfego de URL, categorizando acessos e gerando relatórios para análise de conformidade.

1.5. Filtro avançado de DNS

1.5.1. **Descrição:** assinatura de filtro DNS, proporcionando proteção contra o acesso a domínios maliciosos, interrompendo ataques ainda na fase de resolução de nomes.

1.5.2. Funcionalidades de Proteção de DNS

1.5.2.1. **Consulta Segura de DNS:** validação de consultas DNS, garantindo acesso somente a domínios confiáveis.

1.5.2.2. **Bloqueio de Domínios Não Confiáveis:** identificação de domínios não categorizados e uso de algoritmos para classificação em tempo real.

1.5.2.3. **Análise preditiva:** identificação de domínios suspeitos inéditos com base na análise de suas características.

1.5.2.4. **Monitoramento e Visibilidade:** relatórios de acessos DNS para análise de segurança e auditorias.

1.6. Acesso remoto/VPN

1.6.1. **Descrição:** permite que usuários externos (remotos) se conectem com segurança à rede interna da empresa, utilizando software cliente de VPN instalado no dispositivo do usuário.

1.6.2. Funcionalidade de proteção

1.6.2.1. **Criptografia de tráfego:** o túnel VPN utiliza protocolos seguros (como IPsec ou SSL/TLS) para proteger os dados transmitidos pela Internet.

1.6.2.2. **Autenticação de usuário:** permite verificar a identidade do usuário com base em credenciais, certificados digitais, e autenticação multifator (MFA). E integrando com autenticação centralizada via *Active Directory*, *LDAP*, e *SAML*.

1.6.2.3. **Controle de acesso:** o *firewall* aplica políticas definindo quais recursos internos cada usuário ou grupo pode acessar.

1.6.2.4. **Compatibilidade com múltiplas plataformas de dispositivos:** suporte para Windows, macOS, Linux, Android, iOS.

1.6.2.5. **Split tunneling:** permitir que apenas o tráfego destinado à rede corporativa siga pelo túnel VPN, enquanto o restante usa a Internet local.

1.6.2.6. **Full tunnel:** permitir que todo o tráfego do usuário siga pelo túnel VPN.

1.6.3. **Registro e monitoramento:** o *firewall* registra conexões, tentativas de acesso, duração de sessão e uso de banda.

1.7. Funcionalidades na camada de aplicação

1.7.1. **Descrição:** a solução deve ser capaz de inspecionar tráfego a nível de aplicação.

1.7.2. **Controle de aplicativos:** deve ser possível identificar a aplicação está sendo acessada em uma conexão, e bloqueá-la, se necessário.

1.7.3. **Identificação de usuários:** o firewall deve possuir mecanismo de mapeamento dinâmico entre endereços de IP e identidades de usuários autenticados.

1.7.3.1. Esse mapeamento deve ser obtido através de integração com:

1.7.3.1.1. Controladores de domínio.

1.7.3.1.2. Servidores de LDAP, RADIUS, SAML.

1.7.3.1.3. Captura de autenticação via protocolos (Kerberos, NTLM, Captive Portal).

1.7.4. **Qualidade de serviço (QoS):** deve ser possível priorizar tráfego, com controle de banda (Traffic Shapping), baseado em critérios como:

1.7.4.1. Por IP/sub-rede.

1.7.4.2. Porta/protocolo.

- 1.7.4.3. Por aplicação.
- 1.7.4.4. Por usuário.
- 1.7.4.5. Por DSCP/ToS

1.8. Performance e capacidade do hardware

1.8.1. **Descrição:** a solução deve ser composta por um par de equipamentos físicos (*appliances*) idênticos, configurados para operar em Alta Disponibilidade (HA), garantindo a redundância e a continuidade dos serviços de segurança sem interrupção. Os requisitos de performance mínimos listados abaixo devem ser medidos e comprovados com múltiplas funcionalidades de segurança habilitadas simultaneamente (modo NGFW), incluindo, no mínimo, IDS/IPS, Prevenção Avançada de Ameaças, Filtro de URL, Filtro de DNS e inspeção de tráfego criptografado (SSL/TLS). Os *appliances* deverão vir acompanhados de todos os conectores, cabeamento e peças de fixação no Rack, necessários à sua instalação e funcionamento, conforme as especificações neste documento.

1.8.2. Requisitos de Throughput (Vazão) Mínima

- 1.8.2.1. Throughput de Prevenção de Ameaças (NGFW/*Threat Protection*): 2.5 Gbps.
- 1.8.2.2. Throughput de VPN: 3 Gbps.
- 1.8.2.3. Throughput de IPS: 4 Gbps.

1.8.3. Requisitos de Conexão e Sessão

- 1.8.3.1. Máximo de Sessões Concorrentes: 900 mil sessões.
- 1.8.3.2. Novas Sessões por Segundo: 90 mil sessões por segundo.
- 1.8.3.3. Usuários VPN: 1000 usuários (licenças devem ser incluídas).

1.8.4. Requisitos de Hardware e Interfaces

- 1.8.4.1. Formato: *appliance* físico montável em rack.
- 1.8.4.2. Fontes de Alimentação: fontes de alimentação duplas (redundantes).
- 1.8.4.3. Armazenamento: deve possuir armazenamento interno (SSD) para logs, relatórios e quarentena de ameaças, com capacidade de, no mínimo, 120 GB.
- 1.8.4.4. Interfaces de Rede: deve possuir uma combinação de portas incluindo no mínimo: 4 portas 10G SFP+ (com *transceivers* padrão multimodo), 2 portas 1G SFP (com *transceivers* padrão multimodo) e 8 portas 1G RJ45 (incluindo gestão/HA), ou, alternativamente: 4 portas 10G SFP+ (com *transceivers* padrão multimodo) e 12 portas 1G RJ45 (incluindo gestão/HA). Todas as portas deverão ter conector do tipo LC (*Lucent Connector*).

1.8.5. Alta disponibilidade

- 1.8.5.1. Modo de Operação: a solução deve suportar configuração em Alta Disponibilidade (HA) no modo Ativo/Passivo.
- 1.8.5.2. *Failover Stateful*: deve garantir a sincronização de sessões, de forma que as conexões ativas não sejam interrompidas durante um evento de *failover*.
- 1.8.5.3. Tempo de *Failover*: o tempo de ativação para o equipamento secundário deve ser de menos de um segundo.
- 1.8.5.4. Interfaces HA Dedicadas: deve possuir, ou permitir a configuração de portas dedicadas para a sincronização de HA (*heartbeat* e dados de sessão).
- 1.8.5.5. Monitoramento de Links e Caminhos: deve ser capaz de monitorar o estado de interfaces físicas (*link monitoring*) e caminhos de rede (*path monitoring*) para acionar o *failover* proativamente.

1.8.6. Arquitetura resiliente

- 1.8.6.1. A arquitetura do *appliance* deve garantir a separação funcional entre o Plano de Controle (responsável pela gerência do equipamento) e o Plano de Dados (responsável pelo processamento de tráfego).

1.8.6.2. A interface de gerenciamento (CLI e GUI) deve permanecer acessível e responsiva para um administrador mesmo quando o Plano de Dados estiver sob ataque de Negação de Serviço (DDoS) ou em condição de alta utilização.

ITEM 2 - Serviço de Suporte Técnico e Manutenção 24/7, para o item 1, por 5 anos

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

2.1. **Descrição:** suporte para 2 equipamentos de firewall em HA, com acesso direto ao fabricante para assistência e cobertura de incidentes críticos.

2.2. Deve ser feito um plano de implantação para toda a solução contratada.

2.3. A CONTRATADA é responsável por realizar a instalação e configuração inicial, que incluirá as seguintes etapas:

2.3.1. Plano de implantação.

2.3.2. Sessões práticas de ambientação de 16 horas, para familiarizar a equipe da CONTRATANTE a respeito das atividades básicas de administração da ferramenta e o plano de implantação. **Essa atividade é distinta do treinamento formal que deverá ser conduzido após a implantação.**

2.3.3. Instalação física no datacenter da CONTRATANTE, com a conectorização completa dos equipamentos.

2.3.4. Configuração de alta disponibilidade (HA), *failover* e redundância.

2.3.5. Migração de políticas e configurações.

2.3.6. Configuração básica de rede (IP, *gateways*, VLANs).

2.3.7. Configuração de zonas de segurança, interfaces e roteamento.

2.3.8. Definição de políticas de acesso, regras de firewall e NAT.

2.3.9. Implementação de VPN.

2.3.10. Configuração de logs, alertas e monitoramento.

2.3.11. Integração com sistemas de repositório de logs, SIEM, e sistemas de auditoria.

2.3.12. Implementação de políticas de priorização de tráfego.

2.3.13. Limites de banda para aplicações críticas e não críticas.

2.3.14. Testes de conectividade, regras e filtros.

2.3.15. Verificação de redundância e failover.

2.3.16. Relatório detalhado de todas as configurações e procedimentos realizados.

2.3.17. Diagrama de rede atualizado.

2.3.18. Realização de backup das configurações realizadas.

2.3.19. O documento de *as-built* da solução implantada.

2.4. Migração completa de todas as políticas, regras, em funcionamento dos equipamentos Palo Alto modelo PA-3220 em uso na Codevasf. Incluindo planejamento desta atividade que deverá englobar levantamento prévio de informações, de forma a deixar a nova solução completamente funcional, e cobertura dos serviços em uso, devendo observar rotas, zonas, redes e sub-redes, certificados de segurança, de forma deixar a nova solução operacional.

2.5. Serviços de atualização

2.5.1. **Patches e hotfixes:** inclusão de atualizações de firmware e correções emergenciais de vulnerabilidades.

2.5.2. **Release management:** planejamento e consulta para atualizações de software para melhorias contínuas de desempenho.

2.6. **Melhores Práticas:** o serviço de suporte técnico deve após instalação, realizar a adoção de melhores práticas e *health check* do ambiente com participação do fabricante da solução. Estas práticas envolverão integrante da Codevasf, integrante do CONTRATADO, e, **engenheiro(s) do fabricante para revisar, recomendar e aplicar melhorias nas políticas e regras de proteção no firewall** em todas as funcionalidades e *features* habilitadas. Ao término o engenheiro do fabricante, responsável na condução do trabalho, deve entregar documentação das políticas existentes. A periodicidade de revisão de aplicação das melhores práticas deverá, ser realizada regularmente no ambiente da CONTRATADA, em intervalos de tempos não superior a 6 (seis) meses.

2.7. **Alertas Críticos e Violação de Defesa:** o serviço de suporte técnico deve permitir o atendimento com participação de engenheiro(s) do fabricante em caso de atividade(s) de ataque(s) que cause instabilidade ou impacto no ambiente da CONTRATANTE, ou de violação de mecanismos de defesa. A critério da CONTRATANTE poderá ser solicitado relatório com detalhes da ocorrência, que deverão ser elaborados em até 24 (vinte e quatro) horas.

2.8. **Assistência Técnica em Garantia:** o serviço de assistência técnica em garantia deve cobrir todos os procedimentos técnicos destinados ao reparo de falhas nos equipamentos ou sistemas, assegurando o restabelecimento de seu estado normal de operação. Inclui substituição de peças, ajustes e reparos técnicos em conformidade com as especificações dos manuais e normas do fabricante, sem custos adicionais para o CONTRATANTE.

2.9. **Manutenção Preventiva e Corretiva:** os serviços de suporte técnico incluirão manutenção preventiva para evitar falhas, bem como manutenção corretiva para resolver problemas existentes. Abrange esclarecimento de dúvidas e reparo de questões relacionadas ao desempenho e funcionamento da solução contratada.

2.10. **Elaboração de Relatórios e Diagnósticos:** a CONTRATADA deverá fornecer relatórios técnicos detalhados, diagnósticos e estudos sobre o ambiente de operação da solução, permitindo ao CONTRATANTE uma visão precisa sobre o estado atual e eventuais necessidades de aprimoramento.

2.11. **Transferência de Conhecimento:** a CONTRATADA se compromete a compartilhar conhecimento técnico com a equipe do CONTRATANTE, detalhando problemas vivenciados e as soluções aplicadas, conforme acordado entre as partes.

2.12. **Instalação, Atualização e Configuração:** o suporte técnico incluirá a instalação, atualização e configuração de novas versões dos produtos, sempre que o fabricante liberar atualizações tecnológicas. Isso garantirá que a solução esteja atualizada com as melhorias e correções mais recentes.

2.13. **Suporte para Instalação e Configuração:** o suporte técnico deverá fornecer atendimento para esclarecer dúvidas relacionadas à instalação, configuração e uso do software, além de suporte para corrigir problemas como falhas, erros, defeitos ou vícios no funcionamento da solução. Também incluirá suporte para problemas na instalação ou configuração de softwares básicos e de infraestrutura de TIC (ex.: sistemas operacionais, servidores de banco de dados e servidores de aplicação) necessários para o pleno funcionamento da solução.

2.14. **Atualização de Versões e Patches:** o serviço de suporte técnico deverá incluir a atualização de versões do software aplicativo, com incorporação de correções de erros, melhorias implementadas e funcionalidades adicionais. O serviço deverá cobrir:

2.14.1. Fornecimento de novas versões e releases durante o período de vigência da garantia.

2.14.2. Disponibilização de manuais e documentos técnicos em formato digital para cada atualização, bem como notas informativas sobre as funcionalidades adicionadas.

2.14.3. Comunicação imediata ao CONTRATANTE sobre a disponibilização de patches de correção, detalhando os defeitos que serão corrigidos e a forma de obtenção do patch. Essa comunicação deverá

ocorrer no prazo máximo de 30 (trinta) dias após o lançamento da atualização ou solução de correção. Para patches de alta criticidade, o prazo será de 48 horas.

2.15. Implantação de Novas Versões e Patches: a CONTRATADA será responsável pela implementação de novas versões, releases, e pela aplicação de patches de correção e pacotes de serviço (*service packs*) para os produtos fornecidos como parte da solução. A implantação deverá ser agendada com os responsáveis pela solução no CONTRATANTE, de acordo com o nível de severidade do chamado técnico.

2.16. Assistência para Reinstalação de Ferramentas: a CONTRATADA auxiliará o CONTRATANTE na reinstalação das ferramentas, se necessário, durante o período de garantia da solução.

2.16.1. Canais de Suporte Técnico: a CONTRATADA deverá disponibilizar múltiplos canais de acesso ao suporte técnico, incluindo: Portal Web, E-mail, Central 0800 e/ou telefone fixo.

2.17. Atendimento Ininterrupto: o atendimento deverá estar disponível 24 horas por dia, 7 dias por semana, durante os 365 dias do ano, com atendimento em língua portuguesa.

ITEM 3 - Treinamento de no mínimo 40h para até 6 pessoas para o item 1

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

3.1. Tipo e Objetivo do Treinamento

3.1.1. O treinamento deverá ser de capacitação técnica, diretamente alinhado com as práticas recomendadas pelo fabricante da solução de *firewall* adquirida.

3.1.2. O curso abordará todos os aspectos fundamentais da solução, incluindo instalação, configuração, administração, monitoramento, e suporte técnico, capacitando a equipe para gerenciar a solução de *firewall* de forma eficaz.

3.2. Formato e Local de Treinamento

3.2.1. O treinamento será realizado online, em uma plataforma de fácil acesso, com recursos que permitam tanto o aprendizado teórico quanto prático.

3.2.2. A CONTRATADA deverá prover um ambiente virtual que contemple demonstrações ao vivo, sessões interativas e atividades práticas.

3.3. Carga Horária e Horário

3.3.1. O treinamento deverá ter uma carga horária mínima de 40 (quarenta) horas, não se incluem nessas 40 horas as 16 horas das sessões de ambientação descritas no **ITEM 2**.

3.3.2. Será realizado em dias úteis, conforme a conveniência da CONTRATANTE (matutino ou vespertino).

3.3.3. A data e o horário serão acordados entre a CONTRATADA e a CONTRATANTE para maior flexibilidade e adequação à disponibilidade dos participantes.

3.4. Turma e Participantes

3.4.1. A turma deverá ser composta por participantes indicados pela CONTRATANTE, que terão acesso completo aos conteúdos e atividades práticas.

3.5. Pré-requisitos e Condições de Realização

3.5.1. O treinamento deverá ocorrer após a conclusão da implementação da solução, permitindo que a equipe já esteja familiarizada com o ambiente.

3.5.2. O conteúdo programático do curso deverá ser aprovado previamente pela CONTRATANTE, e qualquer alteração deverá ser acordada entre as partes.

3.5.3. O curso deve abranger todas as funcionalidades nativas da solução, bem como recursos customizáveis, garantindo um domínio completo das funcionalidades do *firewall*.

3.6. Instrutor Certificado: o treinamento deverá ser ministrado por um instrutor certificado pelo fabricante da solução de *firewall*, com comprovação de qualificação técnica.

3.6.1. A CONTRATADA deverá apresentar o documento de certificação do instrutor em até 5 (cinco) dias antes do início do treinamento, em formato original ou cópia autenticada.

3.7. Certificação e Capacitação Final dos Participantes: ao final do curso, cada participante deverá receber um certificado, contendo a carga horária, o conteúdo programático e demais informações pertinentes.

3.7.1. Concluído o treinamento, os participantes deverão estar aptos a realizar as seguintes atividades com autonomia:

- 3.7.1.1. Instalação, configuração e atualização da solução.
- 3.7.1.2. Administração e suporte técnico.
- 3.7.1.3. Monitoramento e ajustes de desempenho.
- 3.7.1.4. Criar, gerenciar e otimizar regras de firewall.
- 3.7.1.5. Diagnóstico de problemas.
- 3.7.1.6. Ferramentas de *troubleshooting* e análise de tráfego.
- 3.7.1.7. Auditoria de eventos.
- 3.7.1.8. QoS e gerenciamento de tráfego.
- 3.7.1.9. Controle de banda (*traffic shaping*).
- 3.7.1.10. Geração de relatórios.
- 3.7.1.11. Inspeção de tráfego.
- 3.7.1.12. Configuração de VPN.
- 3.7.1.13. Execução de backups e restauração, entre outras atividades essenciais para a gestão da solução de firewall na Codevasf.