TERMO DE REFERÊNCIA

Processo nº 0060407931.000069/2023-12

Fazem parte deste Termo de Referência os seguinte anexos assinados por referência:

- ANEXO I - MATRIZ DE RISCO
- ANEXO II - MODELO DA PROPOSTA
- ANEXO III - TERMO DE COMPROMISSO

1. OBJETO

1.1. Contratação de **Solução Integrada de Proteção** de Rede com características de Next Generation Firewall (NGFW), com licenciamentos de software, atualizações de assinaturas de ameaças, garantia, bem como instalação, migração, operação assistida, treinamento, assistência e suporte técnico, para atender as necessidades de segurança e controle da rede corporativa de computadores da sede do LAFEPE, conforme especificações contidas neste Termo de Referência;

2. DESCRIÇÃO DO OBJETO

2.1. Descrição:

ITEM	DESCRIÇÃO	QUANTIDADE
01	Solução integrada de Proteção de Rede NGFW (Firewall)	01
02	Implantação e treinamento aos operadores da solução	01
03	Garantia/Suporte Técnico 60 meses	01

3. ESPECIFICAÇÕES DO OBJETO

3.1. Características Gerais

3.1.1. Deverão ser fornecidos para composição da solução, 02 (dois) equipamentos idênticos e dedicados (appliance fisicos) à função de Next Generation Firewall e SD-WAN, com suporte a VPN IPSEC e VPN SSL, não sendo permitido appliances virtuais ou solução open source (produto montado);

3.1.2. Os equipamentos deverão ser novos, sem utilização anterior e estar em linha de fabricação, sem previsão de descontinuidade;

3.1.3. Os equipamentos deverão possuir quantidade de memória e

processamento suficientes para atender a todas as funcionalidades e desempenho solicitados neste termo de referência;

3.1.4. Os softwares e firmwares dos equipamentos deverão ser fornecidos em sua versão mais atualizada;

3.1.5. Os equipamentos deverão ser configurados para prover alta disponibilidade em modo ativo/passivo;

3.1.6. Os equipamentos deverão ser fornecidos com as licenças de software e atualização de assinaturas para todas as funcionalidades de UTM/NGFW como: Filtro de Conteúdo, Filtro WEB, Controle de Aplicação, Antimalware/Antivírus, IPS, solicitadas neste termo de referência pelo período de 60 (sessenta) meses;

3.1.7. O fabricante deve ter figurado como líder no Quadrante Mágico do Gartner, na categoria de Network Firewalls, ao menos em 01 das suas 02 publicações mais recentes.

3.2. Características Técnicas da Solução

3.2.1. Firewall *Next Generation Firewall* (NGFW)

3.2.1.1. Permitir a criação de regras de firewall de forma a liberar ou bloquear acessos operando no formato stateful firewall;

3.2.1.2. Permitir vínculo das regras de firewall com objetos (zonas, endereços, portas, protocolos, aplicações, usuário e grupos de usuários), de forma individual e agrupada, para origem e destino do fluxo, de acordo com a granularidade que atenda às necessidades do LAFEPE;

3.2.1.3. Permitir vínculo das regras de firewall com país de origem e país de destino das conexões;

3.2.1.4. Permitir a criação de regras de firewall com período de validade de forma programada (data e horário iniciais e finais);

3.2.1.5. Permitir a tradução de endereços, de forma estática e dinâmica, por meio de NAT (Network Address Translation) nos formatos um-para-um e muitos-para-um, inclusive NAT64, NAT46 e NAT66;

3.2.1.6. Permitir a tradução de portas PAT (Port Address Translation) nos formatos um-para-um e muitos-para-um;

3.2.1.7. Permitir a configuração de DHCP Server e DHCP Relay para cada uma das zonas de firewall, nos protocolos IPv4 e IPv6, com características próprias em cada zona de firewall;

3.2.1.8. Permitir a configuração de roteamento estático e dinâmico utilizando RIP, BGP e OSPF para os protocolos IPv4 e IPv6;

3.2.1.9. Permitir OSPF graceful restart;

3.2.1.10. Permitir Policy Based Routing ou Policy Based Forwarding;

3.2.1.11. Permitir roteamento multicast no protocolo PIM Sparse Mode;

3.2.2. Filtro Web e Controle de Aplicações

3.2.2.1. Permitir a criação de regras de filtro web e controle de aplicações de forma a liberar, bloquear ou limitar acessos;

3.2.2.2. Permitir vínculo das regras de filtro web e controle de aplicações em

qualquer das regras de firewall previamente cadastradas, com a granularidade que atenda às necessidades do LAFEPE;

3.2.2.3. Permitir vínculo das regras de filtro web com categorias de sites, dispostas em uma base de dados catalogada e mantida pelo fabricante da solução, distribuídas por conteúdo do site em categorias distintas;

3.2.2.4. As categorias de sites devem possuir, no mínimo, agrupamentos baseadas nas seguintes características: Conexão Remota, Compartilhamento de Conteúdo, Mensagens Instantâneas, Multimídia (áudio, vídeo, streaming), Comunicação (telefonia, videochamadas), *Proxy, Phishing, Spam, Hacking, Websites* Maliciosos, Redes Sociais, Entretenimento, *Games*/Jogos, Pornografia/Pedofilia, Violência, Drogas, Sites Ilegais, Comércio Eletrônico, Finanças, Governo, Organizações Sociais, Propaganda;

3.2.2.5. Permitir a criação de categorias de sites específicas conforme necessidades do LAFEPE;

3.2.2.6. Permitir a criação de exceções para sites específicos conforme necessidades do LAFEPE;

3.2.2.7. Permitir a criação de regras de filtro web através de filtros específicos nos dados do conteúdo acessado por meio de busca textual;

3.2.2.8. Permitir a filtragem completa de todo o conteúdo de URLs conhecidas e consideradas como fonte de material impróprio, bem como de códigos maliciosos *(cookies, scripts,* binários, *applets, javascripts, activeX* e outros) através de base de dados catalogada e mantida pelo fabricante da solução;

3.2.2.9. Permitir vincular aplicações ou categorias de aplicações às regras de firewall, dispostas em uma base de dados catalogada e mantida pelo fabricante da solução, distribuídas por conteúdo de aplicação em categorias distintas;

3.2.2.10. As categorias de aplicações devem possuir, no mínimo, agrupamentos baseados nas seguintes características: Conexão Remota, *Peer-to-Peer, Proxy,* Compartilhamento (armazenamento/*backup*), Colaboração, Multimídia (áudio, vídeo, *streaming*), Comunicação (telefonia, videochamadas), Redes Sociais e *Games*/Jogos.

3.2.2.11. As categorias de aplicações devem identificar, no mínimo, as aplicações: *TeamViewer, LogMeIn, GoToMeeting, Citrix, Webex, Microsoft Remote Desktop, VNC, SSH, OpenVPN, Telnet, Http-Proxy, Http-Tunnel, Gnutella, BitTorrent, Emule, Onedrive, 4Shared, Dropbox, Google Drive, Google Docs, Evernote, GMail, Office 365, iTunes, Youtube, SIP, WhatsApp, Skype, Facebook, Twitter, LinkedIn, Google+, Hangouts, Facebook Chat, AIM, HTTP, HTTPS, DNS, DHCP, WINS, NTP, FTP, RADIUS, Kerberos, Microsoft RPC, XML.RCP, RCP over HTTP, Microsoft Active Directory, LDAP, PostgreSQL, MySQL, Microsoft SQL Server, Oracle, DB2, SNMP, Whois, SMTP, POP3, IMAP e Rsync*, bem como suas funcionalidades e recursos internos específicos;

3.2.2.12. Permitir a liberação e bloqueio de aplicações sem a necessidade de liberação adicional de portas e protocolos, efetuando apenas a liberação ou bloqueio da aplicação desejada na respectiva regra de controle de aplicações;

3.2.2.13. Permitir a criação de regras baseado nas características, comportamento e funcionalidades das aplicações, de forma que seja possível permitir e bloquear funcionalidades específicas de uma aplicação. Exemplo: Permitir acesso ao Facebook, porém impedir acesso ao recurso Like ou Permitir acesso ao Google Hangout via chat, porém impedir videochamadas;

3.2.2.14. Permitir a criação de exceções para aplicações específicas nas categorias de aplicações conforme necessidades do LAFEPE. Exemplo: Bloquear a categoria de aplicações Redes Sociais mais criar uma exceção liberando o Instagram

que é uma aplicação pertencente à categoria Redes Sociais;

3.2.2.15. Permitir a criação de inspeções personalizadas capazes de reconhecer aplicações proprietárias sem necessidade de ação do fabricante, utilizando como critério expressões regulares, sessões e *payload* de pacotes TCP e UDP;

3.2.2.16. Permitir controle, inspeção e descriptografia de pacotes de conexões TLS/SSL estabelecidas, para fluxos de entrada e saída, efetuando o controle individual e isolado dos certificados (adição, remoção e utilização) em cada ambiente de firewall virtual, independente da aplicação;

3.2.2.17. Permitir o monitoramento do tráfego web e de aplicações em tempo real, podendo filtrar a utilização por objetos (zonas, endereços, portas, protocolos, aplicações, usuários e grupos de usuários), de forma individual e agrupada, para origem e destino do fluxo, sem bloquear o acesso dos usuários ao conteúdo acessado;

3.2.2.18. Permitir a customização da página de bloqueio de forma a informar ao usuário que o acesso não foi autorizado, bem como o motivo pelo qual o bloqueio ocorreu.

3.2.3. **QOS**

3.2.3.1. Permitir a configuração da utilização de banda através da criação de classes, para download e upload, baseado em objetos (zonas, endereços, portas, protocolos, aplicações, usuários e grupos de usuários), de forma individual e agrupada, para origem e destino do fluxo;

3.2.3.2. Permitir a definição da banda máxima, banda garantida e fila de prioridade, sendo que a priorização do tráfego deve ocorrer em tempo real;

3.2.3.3. Permitir a priorização do tráfego baseado em ToS (Type of Services);

3.2.3.4. Permitir sFlow ou NetFlow;

3.2.3.5. Permitir o monitoramento da utilização de banda em tempo real podendo filtrar a utilização por objetos (zonas, endereços, portas, protocolos, aplicações, usuários e grupos de usuários), de forma individual e agrupada, para origem e destino do fluxo, sem bloquear o acesso dos usuários ao conteúdo acessado, de forma a identificar a utilização excessiva de banda;

3.2.4. **Controle de Ameaças;**

3.2.4.1. Permitir a criação de regras de detecção e controle de ameaças capazes de realizar inspeção, detecção, proteção e bloqueio a ataques através dos recursos de IPS integrados internamente à solução fornecida;

3.2.4.2. Permitir vínculo das regras de controle de ameaças em qualquer das regras de firewall previamente cadastradas, com a granularidade que atenda às necessidades do LAFEPE;

3.2.4.3. Permitir a criação de regras por objetos (zonas, endereços, portas, protocolos, aplicações, usuários e grupos de usuários), de forma individual e agrupada, incluindo regras de exceção conforme necessidades do LAFEPE;

3.2.4.4. Permitir proteção e bloqueio para requisições de resolução de nomes para domínios maliciosos de botnets conhecidas;

3.2.4.5. Permitir proteção e bloqueio para conexões com servidores e redes considerados botnets, C&C ou ataque a partir da execução de malwares;

3.2.4.6. Permitir proteção e bloqueio para download e upload de conteúdos considerados maliciosos (*adwares, spywares, worms, hijackers, keyloggers,* etc), inclusive injetados em *HTML e javascript*, bem como bloqueio de download de arquivos por nome, extensão e tipo (independente da extensão do arquivo);

3.2.4.7. Permitir proteção e bloqueio para ataques do tipo *portscan, buffer overflow, syn flood, ICMP flood, UDP flood*, bem como outras formas de exploração conhecidas e consideradas críticas;

3.2.4.8. Permitir a detecção e bloqueio de aplicações que se utilizem de mecanismos de conexão evasivos, criptografados ou através de túneis, com o objetivo de burlar os métodos de bloqueio e proteção;

3.2.4.9. Permitir proteção e bloqueio para ataques de negação de serviços;

3.2.4.10. Permitir a construção de novos padrões de ataque para proteção e bloqueio;

3.2.4.11. Permitir a definição de ações distintas para os casos de ataque detectados: Permitir, Bloquear, Resetar conexão.

3.2.4.12. Permitir detecção de ameaças baseada em assinaturas atualizáveis automaticamente;

3.2.4.13. Permitir a ativação e desativação de assinaturas específicas;

3.2.4.14. Permitir o agrupamento de assinaturas conforme o tipo de protocolo e serviço a ser inspecionado;

3.2.4.15. Permitir o registro por meio de logs de todas as ameaças e ataques identificados, independente da ação definida, armazenando endereços e portas de origem e destino da conexão, horário, usuário (se existir), aplicação e identificação do ataque, bem como os pacotes necessários para utilização em investigação forense e identificação de falsos positivos. Deve ser possível identificar o momento exato em que se refere o registro, utilizando horário GMT ou o fuso horário da configuração do equipamento;

3.2.4.16. Permitir o cadastro de endereços de e-mail para recebimento de notificações das ameaças e ataques identificados, bem como parametrização do nível mínimo para envio dos alertas;

3.2.4.17. Possuir antivírus de gateway que opere de forma integrada à solução fornecida capaz de realizar inspeção, detecção, proteção e bloqueio ao conteúdo trafegado. Suportar operação, no mínimo, nos protocolos *HTTP, FTP, SMTP, IMAP e POP3;*

3.2.4.18. Permitir configuração de proteção *anti-spoofing*;

3.2.4.19. Permitir a criação de usuários e grupos de usuários no próprio *firewall* com os mesmos recursos e funcionalidades de usuários autenticados nos serviços de diretório do LAFEPE (*LDAP, Microsoft Active Directory e RADIUS*);

3.2.4.20. Permitir *single-sign-on* para usuários autenticados através de *Microsoft Active Directory*, independente da quantidade de usuários, sem necessidade de licenciamentos adicionais ou restrições de utilização, para todos os ambientes virtuais de firewall;

3.2.4.21. Permitir autenticação de usuários que estejam utilizando redes IPv4 e IPv6.

3.2.5. **Administração**

3.2.5.1. Possuir interface de administração no próprio equipamento;

3.2.5.2. Não deve ser necessária a instalação de qualquer software no dispositivo cliente para realizar o acesso ou a administração dos recursos do equipamento, bem como adição e utilização de servidores e/ou *appliances*;

3.2.5.3. Permitir acesso a todos os módulos do equipamento de forma integrada, através da mesma interface de administração, sem exigir a instalação de *plugins*, emuladores ou *runtimes* para sua utilização;

3.2.5.4. Permitir a utilização de todas as suas funcionalidades pela interface web, através do protocolo HTTPS, em qualquer um dos navegadores atuais, sempre nas versões mais recentes e suportando, no mínimo, *Microsoft Edge, Mozilla Firefox e Google Chrome* e outros que venham a ocupar posição relevante nos *rankings* globais dos navegadores mais utilizados;

3.2.5.5. Permitir acesso à interface de administração por interface *CLI* através do protocolo *SSH*;

3.2.5.6. Permitir a exportação do backup das configurações do equipamento fornecido em arquivo no formato textual de forma que seja possível sua edição manual por qualquer pessoa com conhecimento da estrutura e novamente importado no equipamento ou outro equipamento similar, independente da interface de administração;

3.2.5.7. Permitir cópia do backup gerado para recurso externo à solução por meio de *FTP, TFTP, SFTP* ou *SCP*;

3.2.5.8. Permitir a configuração de ambientes virtuais na mesma solução fornecida (*firewalls* virtuais), de forma que cada ambiente administre domínios de *firewall* de forma independente, não impondo restrições e limitações quanto à utilização de recursos e funcionalidades nos ambientes virtuais em relação ao ambiente físico;

3.2.5.9. Permitir a criação de administradores com possibilidade de autenticação local na própria solução fornecida ou autenticação em serviços de diretório do LAFEPE (*LDAP, Microsoft Active Directory e RADIUS*), possibilitando, inclusive, utilizar vários serviços de diretório distintos para cada ambiente virtual, inclusive com níveis de permissões distintos para cada administrador, com a granularidade que atenda às necessidades do LAFEPE, para todos os módulos e componentes, para cada ambiente virtual de firewall.

3.2.6. **ZTNA (ZERO TRUST NETWORK ACCESS)**

3.2.6.1. A solução deverá permitir a implementação futura de ZTNA através do licenciamento dos Endpoints, permitindo a ativação das seguintes funcionalidades:

a) Deverá permitir ao administrador a solicitação enforcement de identificação do usuário no login, de modo que o usuário necessite realizar uma confirmação de identidade através de no mínimo:

- Informação pessoal do sistema operacional;
- LinkedIn;
- Google;
- SalesForce;

b) Deverá permitir aplicar perfis de segurança baseado em status de serviços do endpoint, permitindo que seja atribuído um perfil de acesso para os endpoints baseado em no mínimo:

- DHCP Server: Atribui um perfil de segurança se o endpoint estiver conectado a

um servidor DCHP específico;
- DNS Server: Atribui um perfil de segurança se o endpoint estiver conectado a um servidor DNS específico;
- Conexão ao Servidor: Atribui um perfil de segurança se o endpoint estiver online e com sua versão atualizada de acordo com o servidor de gerenciamento.
- Local IP/Subnet: Atribui um perfil de segurança se o endpoint estiver em um range de IPs específico
- Default Gateway: Atribui um perfil de segurança se o endpoint estiver enviando informações para um gateway de internet específico, permitindo também a configuração de endereço MAC do Gateway;
- Ping Server: Atribui um perfil de segurança se o endpoint conseguir enviar um ping para um servidor específico de rede;
- VPN Tunel: Atribui um perfil de segurança se o endpoint estiver acessando a rede através de um Túnel de VPN, deve ser permitida a escolha de túnel de VPN para cada perfil.

c) Deve permitir a atribuição de usuários ou grupos de usuários a políticas de acesso

3.2.7. **VPN**

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

3.2.7.2. Suportar IPSec VPN;

3.2.7.3. Suportar SSL VPN;

3.2.7.4. A VPN IPSec deve suportar Autenticação MD5 e SHA-1;

3.2.7.5. A VPN IPsec deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14.

3.2.7.6. A VPN IPSEc deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

3.2.7.7. A VPN IPSEc deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

3.2.7.8. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

3.2.7.9. Suportar VPN em IPv4 e IPv6, assim como tráfego IPv4 dentro de túneis IPSec IPv6;

3.2.7.10. Deve permitir habilitar e desabilitar túneis de VPN IPSEC a partir da interface gráfica da solução, facilitando o processo de throubleshooting;

3.2.7.11. 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;

3.2.7.12. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

3.2.7.13. Suportar autenticação via AD/LDAP, Secure id, certificado e base de usuários local;

3.2.7.14. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

3.2.7.15. Deverá manter uma conexão segura com o portal durante a sessão;

3.2.7.16. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows 7 (32 e 64 bits), Windows 8 (32 e 64 bits), Windows 10 (32 e 64 bits) e Mac OS X (v10.10 ou superior);

3.2.7.17. Deve suportar Auto Discovery Virtual Private Network (ADVPN);

3.2.7.18. Deve suportar agregação de túneis IPSec;

3.2.7.19. Deve suportar algoritmo de balanceamento do tipo WRR (Weighted Round Robin) em agregação de túneis IPSec;

3.2.7.20. A VPN IPSec deve suportar Forward Error Correction (FEC);

3.2.7.21. Deve suportar TLS 1.3 em VPN SSL.

3.2.8. **SD-WAN**

3.2.8.1. Entende-se como tecnologia SD-WAN (Software-Defined WAN) a rede de área ampla definida por software que centraliza a gerência da rede WAN em uma console única, eliminando a necessidade de intervenções manuais em roteadores em localidades remotas, proporcionando visibilidade do tráfego, seleção de caminho dinâmico baseado em políticas de QoS, aplicação ou performance e utilização de túneis VPN para comunicação entre os sites remotos;

3.2.8.2. Por funcionalidades de SD-WAN entende-se: roteamento inteligente, uso do melhor link por aplicação, abstração do tráfego em relação aos circuitos físicos e controle do tráfego por aplicação;

3.2.8.3. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;

3.2.8.4. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping ou http;

3.2.8.5. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;

3.2.8.6. A solução deve permitir a definição do roteamento para cada aplicação;

3.2.8.7. Deve permitir balanceamento de pacotes de uma mesma sessão;

3.2.8.8. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e todos os links abaixo do threshold definido (estatísticas dos links);

3.2.8.9. Deve possibilitar a definição do link de saída para uma aplicação específica;

3.2.8.10. Deve implementar balanceamento de link por hash do IP de origem;

3.2.8.11. Deve implementar balanceamento de link por hash do IP de origem e destino;

3.2.8.12. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, quatro links;

3.2.8.13. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;

3.2.8.14. A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;

3.2.8.15. Para IPv4, deve suportar roteamento estático e dinâmico (BGP);

3.2.8.16. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, 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 shaping. Dentre as tratativas possíveis, a solução deve contemplar:

3.2.8.17. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;

3.2.8.18. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;

3.2.8.19. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;

3.2.8.20. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações;

3.2.8.21. Suportar a criação de políticas de QoS e Traffic Shaping por porta;

3.2.8.22. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

3.2.8.23. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc;

3.2.8.24. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;

3.2.8.25. O QoS deve possibilitar a definição de fila de prioridade;

3.2.8.26. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;

3.2.8.27. A capacidade de agendar intervalos de tempo onde as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;

3.2.8.28. Uma vez que o tráfego é identificado, as políticas de shaping/QoS podem ser compartilhadas a todos os acessos que fizerem match na regra ou por IP. Ex: 10 Mbps de banda garantida por IP ou para todos os IPs que fizerem match na regra;

3.2.8.29. Deve possibilitar a definição de bandas distintas para download e upload;

3.2.8.30. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);

3.2.8.31. A solução de SD-WAN deve suportar IPv6;

3.2.8.32. Deve suportar o recurso de duplicação de pacotes, para mitigar cenários onde todos os links apresentam perda moderada;

3.2.8.33. Deve suportar recurso que permite correções de erro na transmissão;

3.2.8.34. As funcionalidades de SD-WAN podem ser fornecidas no NGFW ofertado ou em uma solução à parte, na mesma quantidade de equipamentos definida para os firewalls;

3.2.8.35. Em caso de composição de solução, a solução de SD-WAN deverá suportar tráfego compatível com a capacidade do equipamento de firewall.

3.2.9. **Logs**

3.2.9.1. Permitir a gravação de logs de todos os módulos existentes no equipamento de forma que seja possível identificar objetos (zonas, endereços, portas, protocolos, aplicações, usuários e grupos de usuários), para origem e destino da conexão, incluindo o timestamp (momento que ocorreu a identificação) e a ação tomada;

3.2.9.2. Permitir a gravação de logs de auditoria de configurações realizadas e alteradas, informando o *timestamp* (momento que ocorreu a identificação) e o administrador que realizou a operação;

3.2.9.3. Permitir o envio de logs para a console de relatórios que compõe a solução;

3.2.9.4. Permitir o envio de logs de forma simultânea para sistemas de monitoramento externos através de *syslog* ou *rsyslog;*

3.2.9.5. Permitir a customização de todas as configurações de logs de forma específica para cada ambiente virtual habilitado no equipamento.

3.2.10. **Hardware, Licenciamento e Capacidades**

3.2.10.1. O equipamento deve ser baseado no formato de *appliance* físico, composta por hardware, software e sistema operacional do mesmo fabricante;

3.2.10.2. Permitir a operação dos equipamentos como uma instância única, com cluster configurado no formato ativo-ativo, com alta disponibilidade entre ambos, incluindo todas as configurações, administradores, permissões, regras, políticas,catálogos, objetos de rede, sessões, tabelas, associações de segurança de VPNs, ambientes virtuais e outras informações necessárias para que, em caso de falha em quaisquer dos equipamentos configurados, o outro equipamento assuma o completo funcionamento e a continuidade da solução sem perdas de configurações já aplicadas no ambiente;

3.2.10.3. Permitir que a administração possa ser realizada em qualquer dos equipamentos componentes do cluster, de forma que quaisquer alterações e configurações efetuadas sejam replicadas ao outro equipamento;

3.2.10.4. Permitir a sincronização de dados no cluster por meio de agregação de links, configuração de interfaces redundantes ou através de interfaces dedicadas para essa funcionalidade;

3.2.10.5. Possuir fontes de alimentação redundantes, internas ao equipamento, com tensão de entrada automática entre 100-240V AC e frequência de 60Hz. Em caso de falha de qualquer das fontes ou falta de alimentação elétrica em qualquer dos circuitos de alimentação, todo o equipamento e seus respectivos módulos devem permanecer em funcionamento;

3.2.10.6. Possuir características para montagem e instalação em rack no CPD do LAFEPE, devendo ser acompanhado de trilhos, suportes, parafusos, conectores e demais acessórios necessários a sua correta afixação;

3.2.10.7. Não será aceita a instalação de equipamentos sobre bandeja;

3.2.10.8. Todos os módulos e fontes devem ser internos ao chassi do equipamento;

3.2.10.9. Possuir indicação frontal, por meio de display LCD ou LEDs, do status operacional do equipamento: desligado, energizado, ligado, falha em dispositivo e

configuração do *cluster*;

3.2.10.10. Permitir monitoramento remoto através de SNMPv3 de forma a identificar falhas de hardware e utilização dos recursos (processador, memória, conexões, utilização das interfaces);

3.2.10.11. Permitir agregação de links conforme padrão IEEE 802.3ad e LACP, inclusive quando o equipamento estiver operando no modo cluster;

3.2.10.12. Permitir a configuração de várias agregações de links em cada equipamento, habilitando ou não tais agregações para cada ambiente virtual criado, conforme as necessidades do LAFEPE;

3.2.10.13. Permitir a criação de VLANs no padrão IEEE 802.1q, podendo vincular várias VLANs a uma porta física ou agregação de link no equipamento;

3.2.10.14. Permitir a utilização de *Jumbo Frames;*

3.2.10.15. Permitir operação, através das interfaces físicas de rede, de forma simultânea nas camadas 2 e 3 do modelo OSI, bem como no modo *sniffer* (espelhamento do tráfego das portas de rede);

3.2.10.16. Cada equipamento fornecido deve atender individualmente às seguintes capacidades:

- Possuir 4 portas 10GbE no padrão SFP+.
- Acompanhar 4 módulos de rede 10GbE no padrão Duplex LC, para fibra multimodo para 300m, no modelo IEEE 802.3ae do mesmo fabricante da solução de segurança.
- Possuir 8 portas 1GbE no padrão SFP.
- Possuir 16 portas 1GbE no padrão UTP (conexão RJ45).
- Possuir 2 portas 1GbE no padrão UTP (conexão RJ45), para gerenciamento e configuração da alta disponibilidade entre os equipamentos.
- Possuir porta de console para acesso aos recursos de administração com todos os adaptadores necessários para sua utilização no LAFEPE.

3.2.11. Permitir taxa de transferência de 3 Gbps estando habilitadas, de forma concomitante, as funcionalidades de firewall, controle de aplicação e controle de ameaças, conforme especificações dos itens 3.2.1, 3.2.2, 3.2.4 e 3.2.5 (Firewall, Filtro Web e Controle de Aplicações, Controle de Ameaças e Logs) deste Termo, considerando os logs de eventos habilitados em todo o tráfego do equipamento;

3.2.12. A métrica utilizada para medição da taxa de transferência deve considerar ambiente empresarial de produção. Caso o fabricante divulgue múltiplos números de desempenho para as funcionalidades, serão considerados os valores aferidos em situações do mundo real e, na ausência destes, será considerado o menor valor, pois será o limitante para o uso de múltiplas funções da solução;

3.2.13. Permitir 3.000.000 de sessões simultâneas;

3.2.14. Permitir 270.000 novas sessões por segundo;

3.2.15. Permitir criação de 10.000 políticas de segurança, incluindo regras de firewall, controle de aplicação e controle de ameaças;

3.2.16. Possuir base de dados catalogada mínima de 4.000 aplicações web;

3.2.17. Possuir base de dados catalogada mínima de 8.000.000 assinaturas de ameaças conhecidas;

3.2.18. Permitir 500 clientes de VPN SSL simultâneos;

3.2.19. Permitir 15.000 clientes de VPN IPsec simultâneos;

3.2.20. Permitir a criação de 10 ambientes virtuais de firewall;

3.2.21. Permitir a identificação de 10 servidores LDAP e Microsoft Active Directory distintos;

3.2.22. Permitir a identificação de 4 servidores RADIUS distintos;

3.2.23. Não deve haver limitação na quantidade de usuários e grupos identificados nos serviços de diretório do LAFEPE (LDAP, Microsoft Active Directory e RADIUS). Caso haja limitação o equipamento deve ser entregue licenciado para a quantidade máxima;

3.2.24. Não deve haver limitação na quantidade de usuários ou dispositivos cliente que estiverem utilizando a solução concomitantemente. Caso haja limitação o equipamento deve ser entregue licenciado para a quantidade máxima;

3.2.25. Permitir a criação de usuários com autenticação local no equipamento;

3.2.26. Permitir a criação de perfis de gerenciamento distintos;

3.2.27. Permitir a criação de usuários de gerenciamento distintos.

3.2.28. Caso o equipamento seja composto de módulos de expansão de portas, todos os módulos devem ser idênticos;

3.2.29. As quantidades de portas requisitadas devem estar totalmente disponíveis, não sendo aceito sobreposição de portas (by pass);

3.2.30. O licenciamento do equipamento não deve estar atrelado a configurações de rede do equipamento, como endereço IP, domínio ou interface de rede;

3.2.31. Todas as portas e módulos de rede fornecidos com o equipamento devem estar licenciados para utilização de forma completa;

3.2.32. Todas as funcionalidades e recursos do equipamento devem estar licenciadas para operação nas quantidades solicitadas para cada funcionalidade enquanto estiver vigente o direito de atualizações do sistema operacional, software e firmware, exceto as funcionalidades e recursos atendidas pelos tópicos 3.1.1, 3.2.1, 3.2.3, 3.2.4.21 e 3.2.5 (VPN, Firewall, QOS, Autenticação, Administração) deste TERMO, que devem estar licenciadas para operação de forma perpétua.

3.3. **Console de Relatórios**

3.3.1. **Logs**

3.3.1.1. Os logs dos equipamentos que compõem a solução devem ser armazenados de forma consolidada e centralizada em uma console única, possibilitando que consultas na base de dados retornem registros de qualquer dos dispositivos componentes da solução, específicos para cada ambiente virtual;

3.3.1.2. Devem ser do mesmo fornecedor das soluções ofertadas, suportando nativamente todos os recursos listados;

3.3.1.3. Deve considerar o volume de equipamentos ofertados, considerando todo o licenciamento necessário para a correta gestão dos elementos de rede;

3.3.1.4. Pode ser ofertado em VM, desde que compatível com Hyper-V 2019 ou superior, caso ofertado dessa forma, deve ser fornecido servidor com as seguintes características:

- Servidor até 2U;
- baias de discos 2,5” ou 3,5” hot-swap;

- Fontes redundantes hot-swap, 110/220VAC, 50/60Hz;
- Processador Intel Xeon Silver 4314;
- 64GB RAM DDR4;
- 2 (duas) interfaces Ethernet 10/100/1000Base-T;
- 2 (duas) interfaces Ethernet SFP+ 10GBase-X acompanhando 4 (quatro) transceivers 10GBase-SR;
- Controladora RAID em hardware com cache e suporte a RAID0/1/5;
- 2 (duas) unidades SSD SATA mixed-use com 960GB de capacidade cada;
- Volumetria necessária para a guarda dos LOGs requeridos para dados quentes e frios utilizando unidades NL-SAS;
- Licença perpetua Windows Server 2019 Standard ou superior;
- 5 anos de garantia e suporte on-site com troca de peças na modalidade 8x5xNBD, prestado diretamente pelo Fabricante ou pela Contratada.

3.3.1.5. Pode ser ofertado em hardware, desde que em appliance do próprio fabricante, possuindo fontes redundantes e operação do armazenamento em RAID via hardware

3.3.1.6. Possuir recurso que permita identificar a quantidade de registros de logs armazenados, o equipamento que efetuou o registro, o espaço utilizado em disco e o espaço restante de armazenamento;

3.3.1.7. Possuir mecanismo que remova automaticamente os logs armazenados conforme regras definidas pelo administrador, para cada ambiente virtual: quantidade de tempo e quantidade de espaço ocupado;

3.3.1.8. Possuir recurso de exportação de logs, em formato textual, por período inicial e final, específico para cada ambiente virtual;

3.3.1.9. Permitir armazenamento diário mínimo de 10 GB de logs para funcionalidades de todos os módulos da solução.

3.3.1.10. Possuir capacidade de armazenamento para dados quentes de relatoria de pelo menos 6 (seis) meses utilizando a premissa 10GB de logs por dia;

3.3.1.11. Adicionalmente, possuir capacidade de armazenamento para dados frios de relatoria de pelo menos 60 (sessenta) meses utilizando a premissa 10GB de logs por dia;

3.3.1.12. Deverá ser apresentado cálculo do fabricante utilizando sua calculadora oficial ou através de cálculo baseado em suas boas práticas documentada de forma oficial;

3.3.1.13. Permitir armazenamento dos logs de todos os dispositivos da solução, de forma irrestrita e perpétua, pelo período mínimo de 5 (cinco) anos, dentro dos parâmetros mencionados acima.

3.3.2. **Relatórios**

3.3.2.1. Permitir a geração de relatórios sob os logs armazenados, individualizados para cada ambiente virtual.

3.3.2.2. Permitir a definição de filtros para cada um dos campos dos relatórios, podendo informar intervalos inicial e final para os parâmetros além de expressões do tipo caractere que possam abranger mais de um valor por parâmetro. Deve ser capaz de criar consultas SQL ou semelhante para uso nos gráficos e tabelas de relatórios.

3.3.2.3. Permitir a customização dos dados exibidos pelos relatórios,

selecionando os campos a serem exibidos na listagem, configurando o layout (página, cabeçalho, rodapé, alinhamento dos dados, fontes, cores, quebras de página, totalizadores e operadores de agregação), bem como, aplicando opções de filtro por meio de expressões regulares ou utilizando recursos de linguagem de consulta de dados similar à linguagem SQL.

3.3.2.4. Permitir a geração de relatórios nos formatos planilha eletrônica (CSV, ODS, XLS ou XLSX) e PDF, possibilitando visualização de forma tabular ou gráfica,conforme o contexto dos dados que compõem o relatório.

3.3.2.5. Permitir a identificação dos países de origem e destino nos logs de acesso e relatórios gerados.

3.3.2.6. Permitir a geração de relatórios de logs em tempo real e através de agendamentos, conforme definições do administrador.

3.3.2.7. Permitir a monitoração de incidentes e posterior automação de ações relacionadas a fluxos de trabalho, gerenciamento e escalonamento.

3.3.2.8. Possuir atualização de assinaturas diretamente com o fabricante para análise e detecção de ameaças contidas nos padrões de LOGs recebidos e geração de relatórios relacionados a esses surtos

3.3.2.9. Permitir o envio automático de cópia dos relatórios gerados para caixa de correio eletrônico, a ser configurada em cada relatório da solução, para cada ambiente virtual.

3.3.2.10. Permitir a customização de relatórios da ferramenta, de acordo com as necessidades do LAFEPE, de forma que as customizações geradas possam sem salvas para novas execuções dentro da ferramenta.

3.3.2.11. Permitir a criação de telas de monitoramento (dashboards) para análise e visibilidade do tráfego, customizados de acordo com as necessidades e particularidades do LAFEPE, podendo analisar, de formas
independentes, firewall, filtro web, aplicações e ameaças.

3.3.2.12. A gravação, exportação, exclusão ou a geração de relatórios, independente do período considerado ou do volume de dados envolvidos, não deve onerar ou causar gargalos na operação das demais funcionalidades ou capacidades da console de relatórios.

3.3.3. **Administração**

3.3.3.1. Permitir acesso à console de relatórios por interface web através do protocolo HTTPS.

3.3.3.2. Permitir a utilização de todas as suas funcionalidades em qualquer um dos navegadores atuais sempre nas suas versões mais recentes suportando, no mínimo, Microsoft Edge, Mozilla Firefox e Google Chrome e outros que venham a ocupar posição relevante nos rankings globais dos navegadores mais utilizados.

3.3.3.3. Permitir acesso a todos os recursos da console de forma integrada, através da mesma interface, sem exigir a instalação de plugins, emuladores ou runtimes para sua utilização.

3.3.3.4. Permitir a exportação do backup das configurações da console de relatórios.

3.3.3.5. Permitir a criação de administradores com possibilidade de autenticação local na própria solução fornecida ou autenticação em serviços de diretório do LAFEPE (LDAP, Microsoft Active Directory e RADIUS), possibilitando, inclusive, utilizar

serviços de diretório distintos para cada ambiente virtual do firewall, inclusive com níveis de permissões distintos para cada administrador, com a granularidade que atenda às necessidades do LAFEPE, para todos os módulos e componentes.

3.3.3.6. Permitir a criação de perfis de gerenciamento distintos.

3.3.3.7. Permitir a criação de usuários de administração distintos.

3.3.3.8. Permitir operação nos protocolos IPv4 e IPv6.

3.3.3.9. Permitir monitoramento remoto através de SNMPv3 de forma a identificar falhas de hardware e utilização dos recursos (processador, memória, conexões, utilização das interfaces).

3.3.3.10. Todas as funcionalidades e recursos do equipamento devem estar licenciados para operação enquanto estiver vigente os licenciamentos, exceto as funcionalidades e recursos atendidos pelos tópicos 3.3.1, 3.3.2 e 3.3.3 (Logs, Relatórios e Administração) deste TERMO que devem estar licenciados para operação de forma perpétua.

3.3.3.11. Permitir a identificação de hosts infectados nas diversas redes através de mecanismo de inspeção de logs, que avalie padrões apoiado em indicadores sólidos e base de conhecimento da solução, ampla e constantemente atualizada.

3.4. **Detalhes Gerais da Solução**

3.4.0.1. Os objetos especificados nos itens 3.2 e 3.3 (Firewall NGFW e Console de Relatórios) deste TERMO devem atender às seguintes regras:

3.4.0.2. Os objetos classificados como zonas devem suportar o vínculo de todas as zonas de segurança do ambiente de configuração;

3.4.0.3. Os objetos classificados como endereços devem suportar o vínculo de IP específico, intervalo de endereços IP, blocos de endereços IP (endereço e máscara), nos protocolos IPv4 e IPv6, além de endereços no formato FQDN (Full Qualified Domain Name);

3.4.0.4. Os objetos classificados como portas devem suportar o vínculo de portas e intervalo de portas;

3.4.0.5. Os objetos classificados como protocolos devem suportar o vínculo de protocolos, independente da porta de comunicação utilizada;

3.4.0.6. Os objetos classificados como usuários devem suportar o vínculo de usuários e grupos de usuários do serviço de diretório do LAFEPE (LDAP, Microsoft Active Directory e RADIUS) ou usuários locais criados na solução;

3.4.0.7. Os equipamentos fornecidos para compor a solução devem ser todos do mesmo fabricante, exceto quando fornecido Console de Relatórios em modo virtualizado (VM).

3.4.0.8. Os equipamentos, inclusive suas peças e componentes, devem ser novos, de primeiro uso, fazer parte do catálogo de equipamentos comercializados pelo fabricante e estar em linha de produção e comercialização na data de entrega, não sendo aceitos equipamentos que constem como end-of-sale, end-of-support,end-of-engineering-support ou end-of-life;

3.4.0.9. Todos os equipamentos fornecidos para compor a solução devem ser idênticos, conforme as características e especificações de cada modelo.

3.4.0.10. O fabricante da Solução (Firewall NGFW e Console de Relatórios) deve ter figurado como líder no Quadrante Mágico do Gartner, na categoria de Network Firewalls, em sua publicação mais recente.

3.5. **Treinamento**

3.5.1. Deve ser fornecido treinamento que ofereça os conhecimentos necessários e suficientes para a instalação, administração, configuração, otimização, resolução de problemas e utilização da solução, com carga horária mínima de 30 horas, para a equipe de até 10 pessoas responsáveis pela operação da solução.

3.5.2. O treinamento deverá contemplar, no mínimo, os seguintes tópicos:

3.5.2.1. 1. Funcionalidades básicas do equipamento: senha de administração, hora e data, schedules etc.;

3.5.2.2. 2. Procedimento de registro e ativação de licenças;

3.5.2.3. 3. Procedimento de atualização de software;

3.5.2.4. 4. Procedimento de HA;

3.5.2.5. 5. Zonas de segurança e objetos;

3.5.2.6. 6. Interfaces físicas, interfaces virtuais (VLANs) e roteamento interno;

3.5.2.7. 7. NAT;

3.5.2.8. 8. Serviços de segurança como IPS e Anti-Malware;

3.5.2.9. 9. Regras de firewall;

3.5.2.10. 10. VPN IPSEC e SSL;

3.5.2.11. 11. Regras de aplicação, incluindo visibilidade das mesmas;

3.5.2.12. 12. Operação da solução de relatoria;

3.5.2.13. 13. Geração de relatórios diversos da plataforma;

3.5.2.14. 14. Operações de resolução de problemas na solução;

3.5.2.15. 15. Monitoramento da plataforma.

3.5.3. O Treinamento poderá ser realizado através de ferramentas de videoconferência ou presencialmente. Para melhor didática, a empresa fornecedora deverá disponibilizar um ambiente (laboratório) para simular o uso dos equipamentos de firewall.

3.5.4. O ambiente tecnológico a ser utilizado durante a capacitação fica sob responsabilidade da contratada, podendo o LAFEPE auxiliar no que for possível.

3.5.5. Os materiais didáticos (apostila, slides, livros etc.), sejam eles impressos ou digitais, deverão ser providos pela empresa fornecedora e disponibilizados para consulta posterior.

3.5.6. A contratada deverá emitir certificado ao final da capacitação indicando a carga horária, nome do participante, tópicos abordados no curso, bem como outras informações apropriadas.

3.6. **Implantação da Solução**

3.6.1. A instalação dos equipamentos deverá ser feita por profissionais devidamente qualificados contemplando os itens abaixo:

3.6.1.1. Análise da topologia e arquitetura da rede da contratante, considerando os roteadores e *switches* de *backbone* instalados, acesso à Internet, sites remotos, serviços de rede oferecidos aos funcionários da contratante, serviços externos, regras de firewall existentes, bem como qualquer outro equipamento ou sistema

relevante na segurança do perímetro, sendo então feitas as configurações gerais do sistema de firewall de acordo com a configuração atual.

3.6.1.2. Deverão ser migradas e otimizadas as políticas de segurança e acesso existentes na solução em operação (Sonicwall), para a nova solução e configuradas as integrações entre a nova solução de segurança e o ambiente *Microsoft Active Directory* existente para controle e rastreabilidade dos acessos através dos usuários do LAFEPE.

3.6.1.3. Deverão ser migradas as configurações de VPN existentes na solução em operação, para a nova solução sendo elas IPSEC VPN ou SSL VPN ou outras.

3.6.1.4. Para as regras específicas de usuários e aplicações deverá ser repassado o modo de criação do modelo destas regras, ficando a cargo deste órgão o desenvolvimento conforme suas políticas.

3.6.1.5. Deverá ser implantada e ativada a solução de logs e relatoria, para recepção dos logs e geração de relatórios de segurança e operação da solução.

3.6.1.6. Todo o processo de instalação e configuração do sistema deverá ser documentado pela contratada sob a forma de relatório ou roteiro, de forma que os técnicos da contratante possam reproduzir a instalação do firewall quando necessário consultando a documentação.

3.6.1.7. A contratada terá o prazo de 30 (trinta) dias a partir da entrega física dos equipamentos para finalização da instalação, implantação, configuração e ativação de toda a solução.

3.6.1.8. A contratada deverá disponibilizar profissional devidamente qualificado para operação assistida pelo prazo de 2 (duas) semanas após finalização da ativação da solução para execução de eventuais ajustes ou correções na solução ativada.

4. DA GARANTIA E SUPORTE TÉCNICO

4.1. Devem ser fornecidos serviços de garantia e manutenção técnica para a solução, a ser prestado pelo Fabricante da solução ou por empresa credenciada oficialmente por este, de forma remota e presencial, pelo período de 60 meses, a contar da data de entrega dos produtos.

4.2. Deve ser fornecido por todo o período de garantia, serviço de suporte e garantia oficial do Fabricante ou a CONTRATADA credenciada pelo mesmo, para todos os elementos do subsistema pelo período de 60 meses, incluindo:

I - a) suporte técnico 24x7 direto pelo fabricante através de 0800 do fabricante,

II - b) suporte técnico *ON-SITE* 8x5 direto pelo fabricante ou CONTRATADA com acionamento através de 0800 ou telefone local DDD 081.

III - c) reposição pelo fabricante de componentes defeituosos no modelo 8x5xNBD (8 horas por dia, 5 dias na semana, em até o próximo dia útil da confirmação do defeito),

IV - d) atualização de firmware, softwares e atualizações de assinaturas de ameaças.

4.3. A Contratada/Fabricante deverá disponibilizar especialista com conhecimento técnico e com expertise nas configurações dos equipamentos disponibilizados a prestar os serviços de Suporte Operacional e configurações,

atender a todas as normais técnicas e boas práticas de segurança e garantindo o funcionamento e Manutenção Preventiva e Corretiva, com fornecimento de peça e serviço, pelo período de 60 (sessenta) meses;

4.4. Os serviços de assistência técnica deverão ser prestados diretamente pelo fabricante e/ou através de sua rede de assistência técnica autorizada, podendo ser a CONTRATADA, desde que devidamente comprovado por declaração e/ou cópia do contrato, localizada no Estado de Pernambuco. Caso o fabricante não disponha de Assistência Técnica no Estado de Pernambuco, será aceita a declaração de que este se compromete a implantar ou credenciar uma Assistência Técnica até a assinatura do contrato;

4.5. Caso os serviços de assistência técnica sejam prestados pela CONTRATADA, ela deverá possuir, pelo menos um profissional técnico, detentor de certificação de nível associate válido do fabricante ofertado. A comprovação deverá ser feita, através, da apresentação da certificação válida em nome do funcionário e CTPS ou contrato de trabalho firmado com a empresa, até a assinatura do contrato.

5. DA JUSTIFICATIVA DA CONTRATAÇÃO E DO QUANTITATIVO ESTIMADO

5.1. DA CONTRATAÇÃO

5.1.1. A abertura de procedimento licitatório para o **FORNECIMENTO DE SOLUÇÃO INTEGRADA DE PROTEÇÃO DE REDE (FIREWALL)**, objetiva atender as necessidades do **LAFEPE** de utilização de linhas de defesa e aplicação camadas de segurança e proteção nos acessos via internet contra ameaças cibernéticas, tais como: tentativas de ataque e invasão, malware avançado, espionagem cibernética, negação de serviço (DDOS), ataques a dispositivos IoT, aplicações nocivas à rede, aos sistemas e arquivos eletrônicos da instituição - entre outras ameaças relativas a ambientes em rede - além do monitoramento de tráfego e controle de conteúdo, permitindo apenas acesso autorizado definido em regras.

5.1.2. Manter uma solução de Firewall disponível e atualizada é item indispensável às necessidades de segurança da informação e de acessos, evitando ou minimizando as ameaças cibernéticas listadas no item 5.1.1, e não dar atenção a este item de segurança poderá causar prejuízos inestimáveis aos dados e acessos da organização, disponíveis através sua rede corporativa, bem como nos acessos externos, via *WEB*.

5.2. DO QUANTITATIVO ESTIMADO

5.2.1. O quantitativo solicitado na presente contratação, prevê uma solução completa, com equipamento principal e de contingência com as mesmas capacidades, bem como as licenças e dispositivos necessários à utilização de todas as funcionalidades presentes neste Termo de Referência.

5.3. DA VIGÊNCIA

5.3.1. O prazo de 60 meses visa prover segurança e estabilidade do serviço de controle de acessos e ameaças à rede corporativa e seus dispositivos, com uma contingência efetiva, para fazer face aos constantes aprimoramentos e surgimentos de novas ameaças cibernéticas, assim como frequentes tentativas de sequestro e roubo de informações confidenciais, principalmente às instituições públicas como é caso do LAFEPE.

6. CUSTO ESTIMADO DA CONTRATAÇÃO

6.1. O preço **máximo admitido** para o objeto do presente processo licitatório é **sigiloso**, nos termos do art. 34 da Lei 13.303/2016.

7. DA MODALIDADE DE LICITAÇÃO E CRITÉRIOS DE JULGAMENTO

7.1. A modalidade de licitação é o **PREGÃO ELETRÔNICO**;

7.2. Critério de Julgamento: **MENOR PREÇO;**

8. DOS RECURSOS ORÇAMENTÁRIOS

8.1. Os recursos destinados para a presente contratação serão todos provenientes de receita própria do **LAFEPE**.

9. DO REGIME DE EXECUÇÃO

9.1. Regime de execução indireta: empreitada por preço GLOBAL.

10. DA VISTORIA

10.1. É facultado ao licitante realizar uma Vistoria Técnica onde serão executados os serviços, a fim de conhecer as instalações pertinentes e o grau de dificuldade existentes, mediante prévio agendamento, no horário das 9h às 16h, por meio do telefone (81) 3183-1185, na Coordenadoria de Informática - COINF, ou através do email: diinf@lafepe.pe.gov.br.

10.2. Tendo em vista a faculdade de realização da vistoria, as empresas não poderão alegar o desconhecimento das condições e grau de dificuldade existentes como justificativa para se eximirem das obrigações assumidas ou em favor de eventuais pretensões de acréscimos de preços, em decorrência da execução do objeto deste instrumento.

10.3. O prazo para a realização da Vistoria Técnica terá início no primeiro dia útil após a publicação do Edital e encerrar-se-á no dia útil anterior à abertura da sessão pública.

11. DA PROPOSTA

11.1. O prazo de validade da proposta será de 90 (noventa) dias, contados da data da sua apresentação;

11.2. Deverão estar incluídos no preço total ofertado, todos os custos, materiais, tributos, mão de obra, encargos sociais e trabalhistas, que incidam na entrega do serviço pela contratada, conforme detalhamento da proposta **ANEXO II** do termo de referência;

11.3. DA DESCLASSIFICAÇÃO

11.3.1. Serão desclassificadas as propostas que apresentarem o objeto fora das especificações técnicas estabelecidas neste TR ou fora do prazo estabelecido.

12. DA GARANTIA

12.1. No prazo de até 10 (dez) dias, contados da data da assinatura do contrato, deverá ser comprovada a prestação de garantia no percentual de 4% (quatro por cento) do valor total do contrato, conforme **Artigo 71 da Lei Federal n° 13.303/2016**.

12.2. A critério do contratado, a garantia poderá ser prestada nas seguintes modalidades:

a) Caução em dinheiro ou títulos da dívida pública;

b) Seguro-garantia; ou

c) Fiança bancária.

12.3. Não será aceita a prestação de garantia que não cubra todos os riscos ou prejuízos eventualmente decorrentes da execução do contrato, tais como a responsabilidade por multas e obrigações trabalhistas, previdenciárias ou sociais.

12.4. A garantia deve estar em vigor durante toda a execução do contrato.

12.5. Em caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser readequada ou renovada nas mesmas condições.

12.6. Se o valor da garantia for utilizado, total ou parcialmente, pela Contratante, para compensação de prejuízo causado no decorrer da execução contratual por conduta da Contratada, esta deverá proceder à respectiva reposição no prazo de 5 (cinco) dias úteis, contados da data em que tiver sido notificada.

12.7. Após a execução do contrato, constatado o regular cumprimento de todas as obrigações a cargo da Contratada, a garantia por ela prestada será liberada ou restituída e, quando em dinheiro, atualizada monetariamente, deduzidos eventuais valores devidos à Contratante."

13. PRAZO, LOCAL E DEMAIS CONDIÇÕES DE PRESTAÇÃO DO OBJETO

13.1. O fornecimento dos itens físicos do objeto (Hardware) se dará de forma **INTEGRAL** *em até 60 (sessenta) dias corridos, contados da emissão da Ordem de Fornecimento,* na Divisão de Almoxarifado (DIALM), situada no Largo de Dois Irmãos, 1.117 – Recife / PE, em compartimento de carga fechada, com frete CIF da origem até o destino, de segunda à sexta-feira, das 08h00min às 16h00min horas, de acordo com a necessidade do LAFEPE, obedecendo ao prazo contratual e às especificações descritas neste Termo de Referência; O Telefone para eventual agendamento da entrega será: (81) 3183- 1173.

13.2. O recebimento dar-se-á em duas etapas:

a) provisoriamente , para efeito de posterior verificação da conformidade do material com a especificação;
b) definitivamente, após a verificação da qualidade e quantidade do material e consequente aceitação.

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

13.4. Nos casos dos materiais serem entregues em desconformidade com as condições, especificações e legislação respectiva, a Contratada será notificada para realizar as correções e entregar novamente o objeto licitado em até 15 (quinze) dias

úteis, às suas expensas, renovando-se, dessa forma, o prazo para nova análise da Contratante.

13.5. Caso haja algum feriado local ou nacional, o fornecedor deverá realizar a entrega no primeiro dia útil subsequente.

13.6. A implantação e configuração integral dos equipamentos, softwares e licenças deverá ser concluída em no máximo 30 dias após o recebimento dos equipamentos.

13.7. A contratada deverá disponibilizar profissional devidamente qualificado para operação assistida pelo prazo de 2 (duas) semanas após finalização da ativação da solução para execução de eventuais ajustes ou correções na solução ativada.

13.8. Finalizado o prazo de operação assistida, deverá ser iniciado o período de treinamento aos responsáveis pela operação da solução, conforme delineado no item 3.5 deste Termo.

14. DO PRAZO DE VIGÊNCIA E ASSINATURA DO CONTRATO

14.1. O prazo de vigência do Contrato decorrente da licitação será de 60 (sessenta) meses contados da data de sua assinatura, seguindo exposto no art. 71, da Lei 13.303/2016.

14.2. O licitante terá o prazo de 05 (cinco) dias para assinatura do contrato, contados a partir da convocação pelo CONTRATANTE.

15. DOS CRITÉRIOS DE ACEITAÇÃO DO OBJETO

15.1. Em conformidade com o art. 175, inciso I, do Regulamento Interno de Licitações, Contratos e Convênios do LAFEPE, o recebimento dar-se-á em duas etapas:

15.1.1. PROVISORIAMENTE – – pelo responsável na fiscalização, mediante visto no relatório dos serviços realizados, e posterior atesto na Nota fiscal;

15.1.2. DEFINITIVAMENTE – pelo gestor do contrato, mediante conferência dos serviços, quantitativos e valores contratados, com o atesto final da nota Fiscal.

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

16. DAS OBRIGAÇÕES DO CONTRATANTE

16.1. **O CONTRATANTE obriga-se a:**

16.1.1. Aprovar os serviços prestados, desde que atendidas às especificações acordadas no Termo de Referência e respectivos anexos;

16.1.2. Rejeitar, no todo ou em parte, os serviços em desacordo com a ordem de fornecimento;

16.1.3. Solicitar que seja providenciada a correção dos serviços prestados, quando estiver fora das especificações estabelecidas neste termo de referência;

16.1.4. Disponibilizar todas as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA com relação ao objeto desta licitação;

16.1.5. Efetuar o pagamento à CONTRATADA no prazo estipulado neste Termo de Referência;

16.1.6. Proporcionar todas as facilidades necessárias ao bom cumprimento do contrato;

16.1.7. Fiscalizar, como lhe prover e no seu exclusivo interesse, o exato cumprimento das cláusulas e condições contratadas, registrando as deficiências porventura existentes, devendo comunicá-las, por escrito, à CONTRATADA para correção das irregularidades apontadas;

16.1.8. Acompanhar a prestação do serviço conforme agendamento;

16.1.9. Conferir ao final dos serviços a fatura de acordo com o que foi realizado e ainda, os documentos enviados.

17. DAS OBRIGAÇÕES DA CONTRATADA

17.1. **A CONTRATADA obriga-se a:**

17.1.1. Atender com presteza a solicitação do Gestor/Fiscal do Contrato;

17.1.2. Prestar o serviço em estrita conformidade com as especificações e condições exigidas, devendo estar já inclusos nos valores propostos todos os custos do produto, impostos, taxas, fretes e demais encargos pertinentes à formação do preço;

17.1.3. Responder por quaisquer danos pessoais e/ou ao patrimônio, causados diretamente ou indiretamente ao CONTRATANTE, ou a terceiros, decorrentes de sua culpa ou dolo, dos materiais fornecidos, não excluindo ou reduzindo sua responsabilidade, mesmo que não haja a fiscalização ou o acompanhamento por este Órgão;

17.1.4. Emitir fatura mensal, conforme serviço prestado e os documentos necessários para a exatidão da prestação do fornecimento;

17.1.5. A Contratada se obriga a corrigir, substituir componentes ou restabelecer o serviço prestado, conforme o Item 4.1 deste Termo de Referência, que esteja em desconformidade com o solicitado ou que se apresente de qualidade inferior;

17.1.6. A contratada fica obrigada a manter durante a execução do contrato todas as condições de habilitação e qualificação exigidas para participação na licitação;

17.1.7. É de responsabilidade da empresa, todo e qualquer serviço de instalação e contratação de acessos físicos através de subcontratadas, devendo ser comunicado previamente ao CONTRATANTE, não cabendo o repasse das responsabilidades da CONTRATADA.

17.1.8. É de responsabilidade total da empresa quaisquer problemas gerados nos serviços TCP/IP, pela instalação eventual de protocolos de comunicação diferentes dos utilizados na conectividade
IP atual, uma vez constatados que tais problemas não tenham origem na rede local, após uma avaliação conjunta com os técnicos do CONTRATANTE e da CONTRATADA.

18. GESTÃO/FISCALIZAÇÃO DO CONTRATO

18.1. A gestão do contrato será exercida pelo Coordenador de Informática - COINF.

18.2. O acompanhamento e a fiscalização do objeto do contrato serão exercidos por meio de um servidor indicado pela Coordenadoria de Informática - COINF, designado como fiscal do contrato, ao qual competirá acompanhar, fiscalizar,

conferir e avaliar a execução, bem como dirimir e desembaraçar quaisquer dúvidas e pendências que surgirem, determinando o que for necessário à regularização das faltas, falhas, problemas ou defeitos observados, dando ciência de tudo à Contratada, conforme determina o art. 40 inciso VII da Lei nº 13.303/2016 e suas alterações.

18.3. O Contratante ao constatar qualquer irregularidade no fornecimento de bens por parte da Contratada, expedirá notificação, para que a mesma, regularize a situação, sob pena de, não o fazendo, ser aplicada a multa pertinente.

19. DAS SANÇÕES

19.1. Além do que dispõe no Edital a **CONTRATADA**, em caso de inadimplemento de suas obrigações, garantido o contraditório e a ampla defesa anteriormente a sua aplicação definitiva, ficará sujeita às sanções previstas no Capítulo X da RILC e a Seção III da Lei 13.303/2016.

20. DO PRAZO E DA FORMA DE PAGAMENTO

20.1. O pagamento será efetuado em moeda brasileira (Real) através de depósito bancário, em conta corrente da empresa Contratada, mediante atesto da nota fiscal/fatura, em conformidade com Capítulo II, seção I da lei 13.303/2016.

20.2. O LAFEPE efetuará a CONTRATADA o pagamento do objeto deste Termo de Referência pelo valor global, dividido nas seguintes condições:

a) 1ª parcela - 30 dias após a entrega física dos equipamentos no LAFEPE - correspondente ao item 01 da descrição do objeto;

b) 2ª parcela - 30 dias após conclusão dos serviços de implantação e treinamento aos responsáveis pela operação - correspondente ao item 02 da descrição do objeto;

c) 60 parcelas em valores iguais e consecutivos, referentes à Garantia/Suporte Técnico por 60 meses, correspondentes ao item 03 da descrição do objeto, com 1º pagamento 30 dias após entrega do item b acima.

20.3. Deverão estar inclusos nos preços apresentados todos os gastos do frete, inclusive quaisquer tributos, sejam eles sociais, trabalhistas, previdenciários, fiscais, comerciais ou de qualquer outra natureza resultantes da execução do contrato;

20.4. O contratante reserva-se o direito de suspender o pagamento se o(s) produto(s) for(em) entregue(s) em desacordo com as condições e especificações constantes neste Termo de Referência, Edital e seus respectivos anexos;

20.5. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido de alguma forma para tanto, o valor devido deverá ser acrescido de encargos moratórios proporcionais aos
dias de atraso, apurados desde a data limite prevista para o pagamento até a data do efetivo pagamento, com base na variação do Índice de Preços ao Consumidor Ampliado – IPCA, do IBGE, aplicando-se a seguinte fórmula:

EM = I x N x VP

EM = Encargos Moratórios a serem acrescidos ao valor originariamente devido

N = Número de dias entre a data limite prevista para o pagamento e a data do efetivo pagamento
VP = Valor da Parcela em atraso
I = Índice de atualização financeira, assim apurado:
I = (TX/100)/365)
TX = Percentual do IPCA anual

21. DA HABILITAÇÃO JURÍDICA

21.1. A documentação a regularidade Jurídica será a que está prevista no Edital Padrão do **LAFEPE** para prestação de serviços comuns.

22. REGULARIDADE FISCAL

22.1. Os documentos para **HABILITAÇÃO TRABALHISTA e FISCAL** devem seguir a que está prevista no Edital Padrão do **LAFEPE** para prestação de serviços comuns.

23. DA QUALIFICAÇÃO TÉCNICA

23.1. A empresa arrematante que não for fabricante dos produtos ofertados deverá comprovar, que é revendedora autorizada a comercializar os bens e que está apta a prestar os serviços de garantia exigidos, mediante declaração emitida pela empresa fabricante dos produtos, ou outros documentos capazes de comprovar as condições exigidas;

23.2. Comprovação de aptidão para desempenho de atividade pertinente e compatível em características, quantidades e prazos com o objeto da licitação, por meio de atestado de capacidade técnica fornecido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) o bom desempenho da empresa (qualidade, suporte e cumprimento de prazo) com seus clientes, o(s) qual(is) deverá(ão) especificar a(s) quantidade(s) fornecida(s), contabilizando no mínimo 50% (cinquenta por cento) do objeto deste Termo de Referência.

23.3. Para fins de comprovação das características e quantidades a que se refere este subitem, o atestado deverá comprovar a realização de fornecimento (nas modalidades como serviço ou revenda) e a instalação/configuração de 1 (um) par de firewalls NGFW em cluster ativo-ativo ou ativo-passivo **ou** 1 (um) firewall NGFW operando de forma standalone;

23.4. Para fins de comprovação das características e quantidades a que se refere este subitem, o atestado deverá comprovar a realização de execução de assistência técnica em modalidade on-site por um período mínimo de 12 meses em solução de firewall NGFW;

23.5. É proibida a apresentação de atestados de capacidade técnica emitidos em nome de empresa coligada ou pertencente ao mesmo grupo econômico da licitante.

23.6. Comprovar através de documentação do Fabricante, que é um canal autorizado e capacitado para o fornecimento dos produtos e prestação do suporte aos sistemas envolvidos.

24. DA HABILITAÇÃO ECONÔMICA E FINANCEIRA

24.1. Certidão Negativa de Falência ou Recuperação Judicial, ou Liquidação

Judicial, ou de Execução Patrimonial, conforme o caso, emitida pelo Cartório distribuidor da sede do licitante, ou de seu domicilio, dentro do prazo de validade previsto na própria certidão, ou, na omissão, expedida a menos de 180 (cento e oitenta) dias, contados da data de apresentação dos documentos de Habilitação e da Proposta Comercial, caso no documento não conste o prazo de validade.

24.2. Certidão Negativa de Falência, Recuperação Judicial ou Extrajudicial referente aos processos distribuídos pelo PJE (**Processos Judiciais Eletrônicos**) da sede da pessoa jurídica;

24.3. A certidão descrita no subitem 24.2. somente é exigível quando a Certidão Negativa de Falência ou Recuperação Judicial, ou Liquidação Judicial, ou de Execução Patrimonial Falência, Recuperação Judicial ou Extrajudicial do Estado da sede da licitante contiver a ressalva expressa de que não abrange os processos judiciais eletrônicos..

24.4. Balanço patrimonial e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, comprovando índices de liquidez geral (LG), liquidez corrente (LC), e solvência geral (SG) igual ou superior a 1 (um), vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrado há mais de 3 (três) meses da data de apresentação da proposta;

24.4.1. No caso de empresa constituída no exercício social vigente, admite-se a apresentação de balanço patrimonial e demonstrações contábeis referentes ao período de existência da sociedade;

24.4.2. É admissível o balanço intermediário, se decorrer de lei ou contrato/estatuto social.

24.5. As empresas, que apresentarem resultado inferior ou igual a 1(um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), deverão comprovar patrimônio líquido de 10% (dez por cento) do valor total estimado da contratação pertinente.

24.6. O balanço patrimonial e as demonstrações contábeis deverão estar assinadas por Contador ou por outro profissional equivalente, devidamente registrado no Conselho Regional de Contabilidade.

24.7. O Balanço Patrimonial também poderá ser disponibilizado via Escrituração Contábil Digital – ECD, desde que comprovada a transmissão desta à Receita Federal do Brasil, por meio da apresentação do Termo de Autenticação (recibo gerado pelo Sistema Público de Escrituração Digital - SPED).

24.8. Será aceita também a apresentação de balanços e demais demonstrações contábeis intermediárias, referentes ao exercício em curso, na forma da lei, devidamente assinados pelo representante legal e pelo Contador responsável, e registrados em Junta Comercial.

25. DO REAJUSTE

25.1. O preço somente será reajustados após decorrido 12 (doze) meses da data fixada para apresentação da proposta, utilizando-se para tanto o Índice de Preços ao Consumidor Amplo - IPCA.

25.2. Deve ser verificado previamente pelo fiscal do contrato a permanência da vantajosidade pela constatação dos valores atualizados do mercado, não sendo necessária a solicitação pela contratada;

25.3. Havendo interesse da parte CONTRATANTE em prorrogar o contrato, a empresa CONTRATADA deverá pleitear o reajuste dos preços até a data anterior a efetivação da prorrogação contratual, sob pena de, não fazendo dentro do prazo, ocorrer sua preclusão.

25.4. Reajustes apenas se aplicarão aos pagamentos referentes às parcelas restantes designadas à garantia e suporte técnico da solução.

26. DO CONSÓRCIO

26.1. Será vedada a participação de empresas em consórcio e que sejam controladoras, coligadas ou subsidiárias entre si para o caso concreto, por ser o que melhor atende o interesse público, prestigiando os princípios da competitividade, economicidade e moralidade. A reunião de empresas em consórcio que, individualmente, poderiam prestar os serviços, reduziria o número de licitantes participantes e poderia, eventualmente, proporcionar a formação de conluios/cartéis para manipular os preços nas licitações. Assim, no presente caso, a vedação de participação de consórcios visa afastar possível restrição à competição e proporcionar a obtenção de proposta mais vantajosa.

27. DA SUBCONTRATAÇÃO

27.1. É expressamente vedada a subcontratação total do objeto deste contrato, sob pena de rescisão contratual, sem prejuízo da aplicação de penalidade prevista na minuta do contrato.

28. DA PROPRIEDADE, SIGILO E RESTRIÇÕES

28.1. Entre as medidas de segurança a serem tomadas no tocante à execução contratual, ao sigilo de todas as informações e à segurança dos documentos que compõem este instrumento, deve a CONTRATADA seguir as seguintes recomendações:

28.1.1. Identificar qualquer equipamento da empresa que venha a ser instalado nas dependências do CONTRATANTE, utilizando placas de controle patrimonial, selos de segurança, etc;

28.1.2. Manter sigilo absoluto sobre informações, dados e documentos integrantes dos serviços a serem executados, inclusive com a assinatura, pelo representante legal da CONTRATADA, do Termo de Compromisso (modelo conforme Anexo III);

28.1.3. Não permitir que dados ou informações do CONTRATANTE aos quais tenha acesso a CONTRATADA e/ou seus colaboradores sejam retirados das dependências do CONTRATANTE, não importando o veículo em que estes se encontrem, notadamente discos rígidos, discos óticos, pentes de memórias, documentos, mensagens eletrônicas e outros meios;

28.1.4. Observar, rigorosamente, todas as normas e procedimentos de segurança implementados no ambiente de Tecnologia da Informação do CONTRATANTE.

29. DAS DISPOSIÇÕES FINAIS

29.1. Os casos omissos neste Instrumento serão resolvidos pela Lei nº 13.303/2016 e subsidiariamente, pelas demais leis vigentes que tratem sobre o

assunto;

29.2. Fica eleito o Foro da Comarca de Recife/PE, com exclusão de qualquer outro, por mais privilegiado que possa ser, como o competente para dirimir quaisquer questões oriundas do presente instrumento.

De acordo.

À autoridade superior para consideração.

Em, data da assinatura digital

_____

Simone Carla Alves Pereira

COINF – COORDENADORIA DE INFORMÁTICA

Coordenadora de Informática

Matrícula nº 3409

Aprovo o Termo de Referência, pelos seus próprios fundamentos e pela necessidade do serviço.

_____

Kelby de Menezes Lafayette

SUADM – SUPERINTENDÊNCIA ADMNISTRATIVA

Matrícula nº 3440

ANEXO I - MATRIZ DE RISCO

CATEGORIA DO RISCO	DESCRIÇÃO	CONSEQUÊNCIA	ALOCAÇÃO DO RISCO
RISCO ATINENTE AO TEMPO DA EXECUÇÃO	Atraso no fornecimento do objeto contratual por culpa do Contratado.	Paralisação temporária das atividades	Contratado
	Fatores retardadores ou impeditivos do fornecimento do contrato próprios do risco ordinário da atividade empresarial ou da execução.	Paralisação temporária das atividades.	Contratado
	Fatos retardadores ou impeditivos do fornecimento do contrato que não estejam na sua álea ordinária, tais como fatos do príncipe.	Paralisação temporária das atividades.	Contratante
RISCO DA ATIVIDADE EMPRESARIAL	Alteração de enquadramento tributário, em razão do resultado ou de mudança da atividade empresarial, bem como por erro do Contratado na avaliação da hipótese de incidência tributária	Aumento ou diminuição do lucro do Contratado	Contratado
	Variação da taxa de câmbio	Aumento ou diminuição do custo do produto e/ou do serviço.	Contratado
	Elevação dos custos operacionais para o desenvolvimento da atividade empresarial em geral e para a fornecimento do objeto em particular, tais como aumento de preço de insumos, prestadores de serviço e mão de obra devidamente comprovados	Aumento do custo do produto e/ou do serviço.	Contratado
RISCO TRABALHISTA E PREVIDENCIÁRIO	Responsabilização do LAFEPE por verbas trabalhistas e previdenciárias dos profissionais do Contratado alocados na fornecimento do objeto contratual	Geração de Custos trabalhistas e/ou previdenciário para o LAFEPE, além de eventuais honorários advocatícios, multas e verbas sucumbenciais	Contratado
RISCO TRIBUTÁRIO E FISCAL (NÃO TRIBUTÁRIO)	Responsabilização do LAFEPE por recolhimento indevido em valor menor ou maior que o necessário, ou ainda de ausência de recolhimento, quando devido, sem que haja culpa do LAFEPE	Débito ou crédito tributário ou fiscal (não tributário)	Contratado

ANEXO II - MODELO DE PROPOSTA (PAPEL TIMBRADO DA EMPRESA)

Recife, xx de 2024.

Ao Laboratório Farmacêutico do Estado de Pernambuco Governador Miguel Arraes S.A. – LAFEPE Largo de Dois Irmãos, 1117 – Dois Irmãos - Recife/PE
Processo de Licitação nº xxxxxxxx - Pregão Eletrônico nº xxxxxxxx

Prezado Senhor(a),
A (nome completo da empresa, CNPJ, número de telefone, endereço eletrônico, endereço comercial), apresenta a sua proposta para o serviço de XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX**,** conforme detalhamento contido no TERMO DE REFERÊNCIA.

1 -PREÇOS:

Item	Descrição	CÓD.	UND.	QUANTIDADE	PREÇO UNIT
1	Solução integrada de Proteção de Rede NGFW (Firewall)		UN	01	XX
2	Implantação e treinamento aos operadores da solução		UN	01	XX
3	Garantia/Suporte Técnico 60 meses		UN	01	XX
PREÇO GLOBAL					

PREÇO GLOBAL POR EXTENSO: xxxxxxxxxxxxxxxxxxxxxxxxxxxx

2. VALIDADE DA PROPOSTA

A presente proposta é válida por 90 (noventa) dias.

3 - DECLARAÇÕES

Declaro que em nossos preços estão incluídas todas as despesas diretas e indiretas, **tais como**: mão de obra, seguros, embalagens, cargas, descargas, tributos (impostos, taxas, emolumentos e contribuições fiscais) que sejam devidos, em decorrência direta ou indireta do contrato a ser celebrado entre as partes, ou de sua execução e serão de inteira responsabilidade da contratada.

Nome Legível e Assinatura

(Física ou eletrônica, do representante legal da empresa)

ANEXO III – TERMO DE COMPROMISSO

O LABORATÓRIO FARMACÊUTICO DO ESTADO DE PERNAMBUCO GOVERNADOR MIGUEL ARRAES - LAFEPE - sediado no Largo de Dois Irmãos, 1117, Dois Irmãos, CEP 52171-010, Recife-PE, CNPJ nº 10.877.926/0001-13, doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em <ENDEREÇO>, CNPJ n.° <CNPJ>, doravante denominada CONTRATADA;

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

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

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

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

Cláusula Primeira – DO OBJETO
Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõe o Decreto 4.553 de 27/12/2002 - Salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES
Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:
Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.
Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômico, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.
Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgação possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Contrato Principal: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS
Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada. O TERMO informação abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de idéias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

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

Parágrafo Segundo – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

Parágrafo Terceiro – As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:
I – Sejam comprovadamente de domínio público no momento da revelação;
II – Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;
III – Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES
As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO.
Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos

comprobatórios.

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

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

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

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

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:
I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;
II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;
III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

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

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

Cláusula Sexta – DAS PENALIDADES
A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 87 da Lei nº. 8.666/93.

Cláusula Sétima – DISPOSIÇÕES GERAIS
Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

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

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

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:
I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;
II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.
III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;
IV – Todas as condições, TERMOs e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;
V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;
VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;
VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo a CONTRATO PRINCIPAL;
VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações Sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava – DO FORO

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

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

_____, _____ de _____ de 20____

De Acordo

CONTRATANTE CONTRATADA

_____ _____

<Nome> <Nome>

<Matrícula> <Qualificação>

Documento assinado eletronicamente por **Simone Carla Alves Pereira**, em 19/08/2024, às 17:00, conforme horário oficial de Recife, com fundamento no art. 10º, do Decreto nº 45.157, de 23 de outubro de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.pe.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **54487959** e o código CRC **733237FC**.

Referência: Processo nº 0060407931.000069/2023-12 SEI nº 54487959