



CONSELHO FEDERAL DE FARMÁCIA

SHIS - Setor de Habitações Individuais Sul, Lote L, s/n QI 15 - Bairro Lago Sul - CEP 71635-615 - Brasília - DF - www.cff.org.br

## TERMO DE REFERÊNCIA

PROCESSO ADMINISTRATIVO Nº 25.0.000002785-8

### ANEXO I

#### TERMO DE REFERÊNCIA - ATUALIZADO

#### 1. DO OBJETO

1.1. Fornecimento de solução integrada de serviços gerenciados de segurança (Managed Security Services - MSS) que deverão englobar provimento de equipamentos (hardware), software, serviços de segurança gerenciada em regime 24X7, monitoramento, gestão de vulnerabilidades, resposta a incidentes de segurança, migração dos serviços de maneira transparente (sem interrupções) e transferência de conhecimento para a equipe técnica do Conselho Federal de Farmácia - CFF, de acordo com as especificações constantes no item 3 (Especificações Técnicas) do Termo de Referência.

1.2. A solução integrada de segurança – MSS, deverá operar de forma integrada, ou seja, os equipamentos, softwares fornecidos e configurações aplicadas pela contratada deverão operar como um conjunto plenamente ajustado, de forma a garantir desempenho, disponibilidade e funcionalidades adequados aos requisitos do Conselho Federal de Farmácia - CFF.

1.3. A licitação será realizada em único item.

1.4. O critério de julgamento adotado será o menor preço do item, observadas as exigências contidas neste Edital e seus Anexos quanto às especificações do objeto.

#### 2. ESCOPO DA SOLUÇÃO

A Solução Integrada de Serviços Gerenciados de Segurança – MSS, é composta por itens de serviços contínuos em tecnologia da informação e deverá englobar alocação de equipamentos, produtos, peças, softwares e treinamento necessários à perfeita consecução das atividades e atendimento às especificações técnicas durante o prazo de vigência, incluindo manutenção e atualização dos produtos e softwares utilizados e monitoramento de segurança em regime 24x7 (vinte e quatro horas por dia, sete dias por semana).

Também farão parte do escopo, atividades relacionadas à transferência de conhecimento segundo os requisitos mínimos elencados no item 3 (Especificações Técnicas).

O modelo de prestação de serviços conterà, ainda, processos de trabalho que especificam como os serviços serão prestados, incluindo atividades a serem demandadas pelo Conselho Federal de Farmácia - CFF, tais como abertura de chamados técnicos para resolução de problemas e de consulta a informações, e aquelas a serem desenvolvidas periodicamente pela contratada, tais como análise de vulnerabilidades de segurança e monitoração das ferramentas utilizadas nos serviços. Ademais, a prestação dos serviços englobará entregas que serão utilizadas, principalmente, para mensuração e verificação dos serviços realizados, tais como os relatórios de monitoramento e relatórios de resolução de problemas. Em suma, o serviço objeto da contratação é subdividido conforme a Tabela 1 abaixo:

Tabela 1 – Solução Integrada de Serviços Gerenciados de Segurança – MSS objeto da contratação:

Descrição	Quantidade	Meses ou Horas
Firewall - UTM (Unified Threat Management)	1	12m
Solução de Endpoint	180	12m
Gestão de Vulnerabilidades	1	12m

Centro de Operações de Segurança - SOC	1	12m
Suporte Técnico 24X7	1	12m
Migração dos Serviços	1	1m
Treinamento em programação segura	1	20h

### 3. ESPECIFICAÇÕES TÉCNICAS (mínimas obrigatórias)

São apresentadas, a seguir, especificações técnicas mínimas obrigatórias dos serviços a serem ofertados.

Todos os equipamentos, produtos, peças ou softwares necessários à prestação dos serviços deverão ser novos e de primeiro uso e não constar, no momento da apresentação da proposta, em listas de end-of-sale, end-of-support ou end-of-life do fabricante, ou seja, não poderão ter previsão de descontinuidade de fornecimento, suporte ou vida, devendo estar em linha de produção do fabricante. Da mesma maneira, todo o hardware a ser utilizado na prestação dos serviços deverá estar coberto por garantia do fabricante pelo período da contratação.

#### **Firewall de Rede - UTM (Unified Threat Management) - Especificações Técnicas Mínimas Obrigatórias:**

Os equipamentos, produtos, peças ou softwares necessários à prestação dos Serviços de Firewall deverão ser instalados no Data Center do Conselho Federal de Farmácia – CFF, em Brasília/DF, e deverão observar os seguintes requisitos mínimos.

**3.1** Fornecimento de 01 (um) UTM (Unified Threat Management);

**3.2** O equipamento deverá ser do tipo appliance com no máximo “1U” de altura. Os equipamentos deverão ser fornecidos com fonte de alimentação para as tensões de entrada 110/220 Volts AC;

**3.3** Deverão ser fornecidos todos os cabos, suportes, parafusos e porca gaiola para a instalação dos equipamentos em rack padrão EIA 310-D 19 polegadas;

**3.4** Os equipamentos deverão possuir no mínimo 6 (seis) interfaces de rede com capacidade para 1Gbps (um gigabit por segundo), suportar pelo menos 2 interfaces de 10Gb e Throughput de 14.5 GBit/s;

**3.5** O Software de Firewall UTM (*Unified Threat Management*) deverá ter capacidade mínima de integrar em uma única solução: Endpoint, filtro de pacotes com controle de estado, filtro de conteúdo WEB, VPN com autenticação usando MFA, IDS/IPS, balanceamento de carga, QoS, Link Aggregation, Firewall de aplicação WAF e gerenciamento (administração) de redes Wireless;

**3.6** Toda solução local proposta deverá ter sido desenvolvida por um único fabricante de modo que tanto o suporte da solução, quanto as funcionalidades sejam integradas e administradas através de console de gerenciamento unificada;

**3.7** Interface Web para administração:

**3.8** Toda a administração da solução deve ser centralizada por meio de interface WEB compatível com os principais navegadores de Internet do mercado. A interface deve ser acessível com o protocolo de segurança HTTPS, permitindo a utilização de certificado de segurança;

**3.9** A solução deve permitir através da interface de administração a configuração de quais redes e hosts poderão acessar a interface de administração. Se houver tentativas de acesso sem sucesso, a ferramenta deve bloquear o acesso do IP de origem. A quantidade de vezes de tentativas permitidas antes do bloqueio, além do tempo de bloqueio, devem ser configuráveis pela própria interface. Deve ser possível configurar os acessos a interface Web de administração para usar Multifator de Autenticação (MFA). Deverá ser possível ativar notificação por e-mail para o Administrador quando houver acesso ou tentativa de acesso na interface;

**3.10** Deverá ser possível a configuração de porta de acesso para utilização da interface de administração, assim como ser possível a definição de tempo para desconexão do usuário após período de inatividade na interface;

**3.11** A solução deve permitir através da interface de administração a criação de usuários locais para acessar a interface de administração; grupos de usuários e utilização de usuários remotos (Radius, Active Directory, LDAP, Tacacs+, etc.). Deverá ser possível a criação de perfis diferenciados de acesso, permitindo liberar níveis diferentes de acesso, incluindo um acesso apenas leitura para utilização em auditorias;

**3.12** Deve ser possível consultar na interface de administração o histórico de alterações realizadas por cada usuário na ferramenta. Todo acesso deve ser registrado em Logs;

**3.13** A interface de administração deve permitir a criação de, pelo menos, as seguintes “definições” ou “objetos”: Hosts (cadastrados por IP), Grupos de Hosts, Serviços (incluindo protocolo, porta ou faixa de portas de origem e porta ou faixa de portas de destino), Grupos de Serviços, Redes (incluindo endereço IP e máscara), Grupos de Redes, Domínios (a solução deverá, a partir do domínio cadastrado, resolver todos os IPs a ele relacionados) e Grupos de Domínios. Uma vez

cadastrados, estas “definições” ou “objetos” poderão ser utilizados nas configurações da solução e na criação de regras. Quando alterados, as modificações realizadas nestes objetos deverão valer também, imediatamente, para todas as regras ou demais configurações que os utilizem;

**3.14** A interface de administração deve permitir visualizar informações básicas do estado de cada um dos UTM's, incluindo, pelo menos, a utilização de CPU e memória, a conectividade com a Internet e com a interface central de gerenciamento, a taxa de transferência das placas de rede e a utilização dos discos;

**3.15** A interface de administração deve ser capaz de controlar e gerenciar todas as funcionalidades presentes nos *access points*;

**3.16** A interface de administração deve gerenciar no mínimo 50 (cinquenta) *access points* (APs);

**3.17** A interface de administração deve permitir a visualização gráfica dos *access points*, bem como do estado de funcionamento dos mesmos;

**3.18** A interface de administração deverá possibilitar a visualização de informações de usuários WiFi incluindo: endereço MAC, taxa de transmissão, SSID, canais utilizados e *access points* aos quais está associado;

**3.19** Característica do UTM (*Unified Threat Management*):

**3.20** Possuir sistema operacional customizado especificamente para funções de UTM. Não serão aceitos sistemas de *firewall* que sejam executados sobre sistemas operacional em versões ou configurações distribuídas comumente no mercado, como o *Novell NetWare*, *Microsoft Windows*, *Linux* ou *FreeBSD*;

**3.21** Possuir uma interface para configuração e gerenciamento através de interface de linha de comando CLI (*Command Line Interface*);

**3.22** Firewall com Alarmes:

**3.23** Deve ser possível definir em qual posição a regra ficará na ordem de execução e agrupá-las visualmente;

**3.24** Cada vez que um pacote for atendido pelas condições da regra, as informações deverão ser registradas em LOG. Este registro deve ser configurável, permitindo ao administrador definir quais regras devem gerar LOG. A solução deve permitir que a regra seja Habilitada ou Desabilitada a qualquer momento pelo administrador;

**3.25** Permitir ao administrador verificar todas as tentativas de acesso negadas ou permitidas pelo Firewall e criar “alarmes” específicos, que poderão ser registrados na console de gerenciamento e enviados por e-mail no momento em que houver tentativa de invasão;

**3.26** Permitir a criação de regras, com base em objetos novos ou já existentes, tendo como parâmetros configuráveis, pelo menos, os endereços de origem e destino e o serviço (protocolo, porta ou faixa de portas de origem e porta ou faixa de portas de destino). Com base nestes parâmetros, deve ser possível determinar o aceite ou bloqueio do pacote;

**3.27** Deve permitir análise de tráfego em tempo real;

**3.28** A solução deve permitir o armazenamento e o encaminhamento de logs a um SIEM (*Security Information and Event Management*), além de permitir a exportação destas logs para que sejam gravadas em mídias externas. Deverá ser possível especificar o período (intervalo de data) das logs a serem exportadas;

**3.29** Além dos logs e relatórios gerados, permitir saber quais ações são tomadas pelos usuários que tem acesso à console de administração dos Firewalls;

**3.30** Deverá permitir acesso aos dispositivos com perfil de auditoria, sem permissão de alteração de quaisquer configurações;

**3.31** Cada vez que um pacote for atendido pelas condições da regra, as informações devem ser registradas em LOG. Este registro deve ser configurável, permitindo ao administrador definir quais regras devem gerar LOG. A solução deve permitir que a regra seja habilitada ou desabilitada a qualquer momento pelo administrador;

**3.32** Ao criar uma regra de NAT, a solução deve oferecer a opção para que sejam criadas automaticamente as regras no filtro de pacotes;

**3.33** Permitir a criação de regras, com base em objetos novos ou já existentes, tendo como parâmetros configuráveis, pelo menos, endereços de origem e destino e serviço (protocolo, porta ou faixa de portas de origem e porta ou faixa de portas de destino). Com base nestes parâmetros, deve ser possível a utilização de SNAT (Alteração dos dados de origem do pacote), DNAT (Alteração dos dados de destino do pacote) e FullNat (Alteração dos dados de origem e destino do pacote);

**3.34** Permitir a criação de Masquerading das interfaces de redes, incluindo os possíveis IPs adicionais da placa;

**3.35** Rede:

**3.36** Efetuar controle de tráfego por estado no mínimo para os protocolos TCP, UDP e ICMP baseados nos endereços de origem, destino e porta;

**3.37** Suportar o *Internet Protocol* Versões 4 e 6 (IPv4 e IPv6);

**3.38** Suportar o protocolo 802.1q, para uso e segmentação da rede com VLANs;

**3.39** IPS (*Intrusion Prevention Systems*):

- 3.40** A solução deve permitir habilitar ou desabilitar o IPS e permitir a configuração de regras para bloqueio de pacotes ou apenas habilitar alertas. O IPS deve fornecer grupos de regras de proteção a ataques conhecidos a sistemas operacionais, servidores WEB, e-mail, Banco de Dados, etc;
- 3.41** A base de dados de ataques conhecidos deve ter assinatura e atualização automatizada, além de possuir identificação para mais de 8.000 ataques conhecidos;
- 3.42** A proteção IPS deve possibilitar, pelo menos, o bloqueio de ataques do tipo “Flooding”, “DoS” e “PortScan”;
- 3.43** Deverá ser possível a configuração de lista de exceções para o IPS, permitindo relacionar hosts e redes que não terão o tráfego verificado pelo IPS, e, portanto, não serão bloqueados;
- 3.44** A solução deve permitir a ativação de notificação via e-mail para o administrador quando houver ação do IPS;
- 3.45** O IPS deverá suportar pelo menos 1.3Gbps de análises de tráfego de rede sem degradar a performance da rede.
- 3.46** Proxy WEB:
- 3.47** Possibilitar a definição do número da porta na qual o serviço de proxy irá responder as solicitações, assim como quais redes e hosts têm permissão para se conectarem a esta porta;
- 3.48** Possibilitar Habilitar/Desabilitar a utilização de caching para o proxy, e esta habilitação deve ser individual para tráfego do tipo SSL e conteúdos que utilizem cookies;
- 3.49** Permitir a utilização de Parent Proxies;
- 3.50** Possibilitar o “Bypass” de scanning em conteúdos de streaming;
- 3.51** Log de todas as transações do Proxy, registrando, no mínimo, Usuário, IP utilizado pelo usuário, URL acessada, Tempo de duração da request (incluindo horários de início e de término da transação), tamanho do pacote transferido, categorização do site;
- 3.52** Logs de todos os acessos bloqueados;
- 3.53** Permitir selecionar quais portas serão distribuídas pelo proxy;
- 3.54** Permitir scan de tráfego HTTPS (SSL);
- 3.55** Modos de autenticação que devem ser disponíveis:
- 3.56** Autenticação Local: Restringir o acesso a usuários e grupos criados localmente na solução;
- 3.57** Active Directory Single Sign-On: Controlar o acesso a usuários e grupos de domínio Windows para gerenciar o acesso à WEB. O Single Sign-On deve utilizar as credenciais do usuário autenticado na estação de trabalho, sem a necessidade de instalação de software cliente nas estações de trabalho e nem de digitação de usuário/senha pelos usuários finais. Deverá ser possível trabalhar com ilimitados perfis de acesso (cada um com suas próprias regras de acesso a WEB), onde cada usuário do domínio terá seu perfil de acesso determinado de acordo com o grupo de usuários do Active Directory do qual é membro;
- 3.58** Autenticação por Ldap, também com a possibilidade de se trabalhar com diversos perfis de acesso;
- 3.59** Permitir operar em Transparent Mode;
- 3.60** Ocultar a utilização do proxy aos usuários que acessem a Internet;
- 3.61** Garantir que os usuários utilizem o proxy, mesmo sem configuração dos navegadores;
- 3.62** Deverá ser possível a ativação ou desativação desta funcionalidade por meio da interface de administração da solução;
- 3.63** Possibilitar a criação de regras para restrição de acesso por, pelo menos:
- 3.64** Categorias de sites (Exemplo: jogos, compras, esportes etc.). Essa base de dados deve conter mais de 30 milhões de sites agrupados em, pelo menos, 90 categorias. Essa base deve ter atualização automática (on-line);
- 3.65** Deverá ser possível criar uma nova categoria agrupando um conjunto de categorias já existentes;
- 3.66** Deverá ser permitido o cadastro manual de “skips” ou exceções através da console de administração. Por meio destas exceções, deverá ser possível o cadastramento de ilimitadas listas de domínios e IPs. Cada uma destas listas criadas deverá ter suas próprias regras de exceções permitindo, no mínimo, que as seguintes verificações ou ações sejam ativadas ou desativadas para os endereços incluídos na lista: verificação de autenticação do usuário (se está autenticado e se possui um perfil que permita o acesso ao determinado endereço), realização de cache (se o determinado website deve ser armazenado em cache), verificação de filtro de conteúdo e de URL, verificações específicas para HTTPS que possam ser oferecidas pela solução;
- 3.67** Permitir a criação de domínios ou palavras chaves permitidas ou proibidas na URL;
- 3.68** Permitir o bloqueio de acesso também por IP e Mime-Type;
- 3.69** Listas editáveis de sites permitidos e bloqueados, incluindo a utilização de palavras chaves para o bloqueio de URLs;
- 3.70** A solução deverá permitir regras de restrições diferenciadas entre grupos de usuários (locais, do domínio Windows ou LDAP). Deverá ser possível definir o horário em que a regra deve ser aplicada;
- 3.71** Permitir a criação de exceções de websites – tanto para bloqueio quanto para liberação – que seja válido para todos

os usuários, independentemente dos perfis definidos;

**3.72** Permitir a customização das mensagens de bloqueio e inserção de logotipo;

**3.73** Controle de Banda / QoS:

**3.74** Implantar controle de banda permitindo o fracionamento dos links de comunicação de modo que serviços essenciais sejam priorizados através de regras, onde seja possível definir o tamanho de banda para cada tipo de tráfego;□

**3.75** Reserva de Largura de Banda Dinâmica de Saída (Limite Mínimo e Máximo Garantido);

**3.76** Rede ou servidor de origem/destino, serviço/porta;

**3.77** Bits TOS (Tipo de Serviço) / DSCP (Ponto Diferenciado de Código de Serviço);

**3.78** Seletores de tráfego predefinidos para os aplicativos P2P;

**3.79** Adaptação dinâmica, largura de banda reservada às velocidades de ligação disponíveis por protocolo;

**3.80** Alta Disponibilidade / Cluster / Redundância / Balanceamento:

**3.81** A solução deve prover, pelo menos, as seguintes possibilidades de operação:

**3.82** Failover (Ativo-Passivo): quando um equipamento parar de responder, o outro deverá assumir automaticamente e imediatamente, sem nenhuma intervenção. Os equipamentos que estiverem operando em failover deverão estar sempre sincronizados entre si, sendo que as alterações de configurações aplicadas em um deles sempre deverão ser repassadas para o outro automaticamente, também sem nenhuma intervenção.

**3.83** VPN (Site-to-Site, Remote Access):

**3.84** Implantar servidor de VPN (Virtual Private Network ou Rede Privada Virtual) com gerenciamento das conexões em tempo real. Devem ser suportadas, pelo menos, as seguintes VPNs:

**3.85** Site-To-Site IPsec, podendo selecionar o método de autenticação entre Chaves Locais RSA e PSK;

**3.86** Site-To-Site SSL;

**3.87** Remote Access, implementando conexão VPN para acesso remoto com, pelo menos, as tecnologias SSL, PPTP, L2TP over IPsec, IPsec;

**3.88** A solução deve permitir o estabelecimento de conexão VPN a partir de estações com plataforma Microsoft Windows 10, ou superior, e plataforma UNIX/LINUX, com ou sem a necessidade de instalações de software cliente nestas estações para que a conexão funcione. Se for necessário software cliente, este deverá ser fornecido pela CONTRATADA, incluindo as licenças necessárias, para quantidade ilimitada de usuários;

**3.89** A solução deve permitir a criação de número ilimitado de usuários VPN. Deverá permitir a criação de usuários locais, exclusivos para a VPN (que não funcionem para utilização em quaisquer outros tipos de acessos), sem a necessidade de que sejam criados também no Active Directory ou em qualquer outro local fora da solução contratada;

**3.90** Caso não haja software cliente de VPN específico para dispositivos móveis, deverão ser indicados pela CONTRATADA aplicativos que desempenhem a funcionalidade de VPN para Tablets, celulares e demais dispositivos móveis, disponíveis no momento da contratação do serviço, de preferência gratuitos;

**3.91** Gerenciamento, Relatórios, Estatísticas e Gráficos:

**3.92** Por meio da interface de administração, permitir verificar em tempo real e exportar para outras extensões (PDF, no mínimo), ao menos, os seguintes itens:

**3.93** Relatório de acessos negados por usuário, grupo ou geral, com opção de se especificar um período (intervalo de data);

**3.94** Relatório dos sites mais acessados por usuário e/ou geral, com opção de se especificar o período (intervalo de data) e de se ordenar o resultado obtido por tráfego gerado em cada site e por tempo gasto em cada site;

**3.95** Relatório de todos os sites acessados por um determinado usuário ou grupo, com opção de se especificar um período (intervalo de data);

**3.96** Relatório de tentativa de entrada no Firewall, com opção de se especificar endereço para pesquisa;

**3.97** Relatório estatístico de tráfego, por usuário, grupo ou geral, com informações de tráfego total do período, tráfego total do período por protocolo, tráfego por serviço e protocolo com quantitativos e percentuais. Os relatórios deverão ter a opção de se especificar um período (intervalo de data);

**3.98** Relatório dos alarmes gerados pelo IPS, com opção de se especificar um período (intervalo de data);

**3.99** Relatórios e gráficos de utilização de cache;

**3.100** Relatórios e gráficos de detecção de aplicação de "P2P" e "IM" (Instant Messaging) na rede por usuário;

**3.101** Gráficos de tráfego por usuário e/ou geral com opção de se especificar o período (intervalo de data);

**3.102** Gráficos sumarizados com a opção de especificar o período;

**3.103** Gráfico estatístico de requisições no Firewall; TCPSyn-Flood;

**3.104** Permitir o monitoramento em tempo real da navegação dos usuários logados, visualizando os acessos de um usuário escolhido;

- 3.105** Permitir monitoramento em tempo real das atividades do Firewall, com informações de endereços de origem e destino, incluindo porta, protocolo e qual regra aceitou ou bloqueou a conexão;
- 3.106** Permitir a visualização de todos os usuários que estão autenticados, com a opção de desconectar o usuário;
- 3.107** Permitir monitoramento em tempo real de todas as conexões abertas por cada usuário, informando quanto cada sessão está consumindo do link de Internet;
- 3.108** Permitir verificar informações do sistema, tais como: tipo e velocidade do processador usado, quantidade de memória instalada, usada e livre, inclusive de swap em disco, informações de armazenamento (espaço em disco, usado e livre), informações de placas de rede (tráfego atual, pico máximo e mínimo de utilização de cada uma delas) e informações do kernel (versão, release, tipo e arquitetura);
- 3.109** Deve ser gerado log detalhado de cada conexão, indicando, no mínimo, origem, destino, horário de início e fim, protocolos, portas, URLs e tráfego gerado;
- 3.110** A solução deve possibilitar o envio de relatórios gerenciais diários, semanais e mensais por e-mail, cujos endereços devem ser catalogados na solução, por meio da interface Web para administração;
- 3.111** Permitir o controle de, no mínimo, 10 (dez) aplicativos P2P (Bittorrent, Edonkey, WinMX etc.) permitindo controlar em nível de ação (Bloquear ou apenas registrar o acesso) de cada aplicativo;
- 3.112** Deverá ser possível a configuração de listas de exceção de hosts/redes para estes filtros. Redes e hosts cadastrados nestas listas não deverão ser verificados e, portanto, não deverão sofrer bloqueios e nem registros de acessos nas aplicações controladas por este filtro;
- 3.113** Backup / Restore:
- 3.114** A solução deve possuir recurso de backup de todas as configurações. O backup deve ser enviado diariamente de forma automática por e-mail ou FTP para o administrador. Também deverá ser possível gerar arquivos de backup sob demanda, por meio da interface web de administração;
- 3.115** O restore deve ser possível de ser realizado pela interface WEB de administração;
- 3.116** Link Aggregation:
- 3.117** A solução deve oferecer opção de Link Aggregation para sumarizar interfaces de rede;
- 3.118** Redundância de Conexão:
- 3.119** A solução deve oferecer a funcionalidade para que seja possível a configuração de mais de um link de Internet para que, em caso de falha, o outro assuma automaticamente. Quando os dois estiverem on-line, deverá ser possível a criação de regras para priorização do link;
- 3.120** Access Point:
- 3.121** Deverá fornecer cobertura total e com qualidade no ambiente físico do Conselho Federal de Farmácia - CFF;
- 3.122** Deverá ser implantado o protocolo de autenticação Radius para acesso Wireless a rede corporativa;
- 3.123** Deverá ter filtros de acesso à rede baseados em endereços MAC;
- 3.124** Deverá fornecer acesso a internet para a rede wireless visitante através de HotSpot;
- 3.125** Deverá suportar otimizações no portal de acesso wireless (Hotspot) para atender as necessidades do Conselho Federal de Farmácia - CFF;
- 3.126** Deverá suportar acesso wireless a celulares, *tablets* e outros.
- 3.127** Firewall de aplicação – WAF:
- 3.128** Deverá suportar no mínimo 10 (dez) servidores com aproximadamente 5 (cinco) aplicações web cada, com acessos internos e externos ao Conselho Federal de Farmácia - CFF;
- 3.129** Deverá atuar diretamente na camada 7 (aplicação) do modelo OSI e ser capaz de interceptar todas as requisições do cliente e as respostas do servidor Web;
- 3.130** Deverá ser capaz de detectar e bloquear ataques em HTTP, HTTPS, SOAP, XML-RPC, Web Service, entre outros;
- 3.131** Possibilitar autenticação criptográfica mútua entre servidor e usuário;
- 3.132** Possuir robustez contra ataques por tentativa de senhas (força bruta);
- 3.133** Deverá suportar criptografia SSL;
- 3.134** Deverá interceptar dados de saída, como informações confidenciais e identificá-la ou bloqueá-los para proteção contra vazamento de dados;
- 3.135** A contratada deverá configurar o *firewall* de aplicação de forma a evitar técnicas de evasão utilizando os protocolos IP e TCP;
- 3.136** A contratada deverá configurar o *firewall* de aplicação de forma a trabalhar com inspeção bidirecional de ataques;
- 3.137** Excetuando-se os casos para os quais existam solicitações específicas do Conselho Federal de Farmácia - CFF, nenhum equipamento localizado na rede externa ou interna deverá conseguir ter acesso aos servidores *Web*. Este acesso sempre deverá ser feito através do Firewall de Aplicação para os protocolos HTTP e HTTPS;

- 3.138** Deverá adotar o conceito de “assinaturas de ataques” com intuito de detectar ataques específicos e o conceito de “anomalia de comportamento” com intuito de detectar ataques através de tráfego anormal;
- 3.139** Todos os ataques detectados deverão ser logados. Esses logs serão analisados pela equipe de especialistas em ataques Web da contratada, para que possa ser tomada a melhor medida de prevenção;
- 3.140** Deverá proteger o ambiente contra as vulnerabilidades listadas no OWASP TOP 10;
- 3.141** Deverá fornecer relatórios com o mínimo as seguintes informações: IP do atacante, site atacado, tipo de ataque, por períodos, horário do ataque, qual campo foi atacado, quantas vezes esse ataque foi realizado, URL de ataque, entre outros;
- 3.142** Deverá detectar as seguintes classes de ataques:
- 3.142.1** Violações do protocolo HTTP;
  - 3.142.2** SQL Injection;
  - 3.142.3** LDAP Injection;
  - 3.142.4** Cookie Tampering;
  - 3.142.5** Cross-Site Scripting (XSS);
  - 3.142.6** Buffer Overflow;
  - 3.142.7** OS Command Execution;
  - 3.142.8** Remote Code Inclusion;
  - 3.142.9** Server Side Includes (SSI) Injection;
  - 3.142.10** File disclosure;
  - 3.142.11** Information Leak;
  - 3.142.12** Scanners de vulnerabilidade Web e Crawlers;
  - 3.142.13** Worms e Web Shell Backdoors;
  - 3.142.14** Ausência de tratamento de erros do Webserver.

## **Endpoint**

- 3.143** O software de gerenciamento do UTM deverá ter capacidade para gerenciar a solução endpoint para todas suas funcionalidades.
- 3.144** Os clientes de endpoint devem prover segurança para servidores e estações de trabalho (antivírus, antispymware, IPS, *firewall*, prevenção de roubo de informação).
- 3.145** Os clientes de endpoint devem ter suporte total para os sistemas operacionais cliente baseados nas plataformas: Window, todas as versões em 32 bits e 64 bits.
- 3.146** Suporte total aos sistemas operacionais servidor baseados nas plataformas Windows Server, todas as versões em 32 bits e 64 bits.
- 3.147** Atualizações automáticas das listas de definições de vírus a partir de local predefinido da rede, ou de site da Internet.
- 3.148** Permitir atualização incremental das definições de vírus.
- 3.149** Frequência de atualização no mínimo diária e com possibilidade de agendamento.
- 3.150** Suporte ao uso de múltiplos repositórios para atualização do produto e vacinas.
- 3.151** Permitir conexão através de proxy para efetuar as atualizações.
- 3.152** Varredura em tempo real: de arquivos (gravação, renomeio e leitura), de processos em memória.
- 3.153** Detecção e remoção de programas maliciosos como spyware, *adware*, trojans, *dialers*, *rootkits*, etc.
- 3.154** Possibilidade de reparar o registro do sistema após eliminação dos programas maliciosos.
- 3.155** Monitoramento em tempo real, processos na memória, para a captura de vírus que são executados em memória sem a necessidade de escrever o arquivo.
- 3.156** Capacidade de finalizar processos perigosos que possam causar instabilidade ou risco ao sistema através de análise heurística.
- 3.157** Solução única para proteção contra malwares em geral, incluindo vírus, trojans, *adware*, *rootkits*, spywares, aplicações potencialmente indesejadas (PUAs), e buffer overflow.
- 3.158** Possibilidade de verificar o arquivo apenas posicionando o cursor sobre o mesmo (pré-execução).
- 3.159** Permitir bloqueio de portas.
- 3.160** Permitir criação de regras baseadas em processos de sistema.
- 3.161** Permitir o bloqueio de compartilhamentos da máquina em caso de epidemia.
- 3.162** Oferecer proteção avançada de sistemas contra ameaças tais como ataques remotos de injeção de SQL ou HTTP.
- 3.163** Possuir proteção contra vulnerabilidades desconhecidas, tais como estouro de *buffer* (*buffer overflow*) e ataques de dia zero (*zero-day attacks*).
- 3.164** Possibilitar varredura HTTP e HTTPs, detectando ameaças antes de sua escrita em HD.

- 3.165** Possibilidade de recuperar arquivos da quarentena.
- 3.166** Possuir algum método de desinstalação de antivírus atual sem reinício do servidor/estação.
- 3.167** Possuir instalação “silenciosa” através de *Policies* do *Active Directory*, *script* de *logon*, etc.
- 3.168** Permitir atualização automática do produto.
- 3.169** Visualização das características básicas de hardware diretamente na console de gerenciamento do usuário.
- 3.170** Suporte a instalação do servidor em todas as plataformas Windows Server, tanto em máquinas físicas quanto virtuais.
- 3.171** Suportar o gerenciamento de no mínimo 25.000 máquinas a partir de um único servidor.
- 3.172** Permitir o gerenciamento do servidor utilizando os protocolos TCP/IP.
- 3.173** Permitir o gerenciamento centralizado da instalação nos clientes a partir de um único servidor, com possibilidade de sincronização com o Active Directory.
- 3.174** Permitir a alteração das configurações dos antivírus nos clientes de maneira remota e através de regras aplicáveis a uma máquina, um grupo de máquinas, etc.
- 3.175** Permitir a atualização incremental e através do uso de políticas da lista de definições de vírus nos clientes a partir de um único ponto da rede.
- 3.176** Permitir a criação de tarefas de atualização, verificação de vírus e upgrades de produto em intervalos de tempo pré-determinados.
- 3.177** Permitir o armazenamento das informações coletadas nos clientes em um banco de dados SQL Server centralizado.
- 3.178** Permitir diferentes níveis de administração da console de gerenciamento utilizando usuários do domínio.
- 3.179** Forçar a configuração determinada no servidor para os clientes.
- 3.180** Caso o cliente altere a configuração da estação, a console deverá gerar um alerta em tempo real com possibilidade de envio de e-mail informando a atividade.
- 3.181** Exportação dos relatórios para os seguintes formatos: PDF, XML, HTML, CSV, XLS, DOC e RTF.
- 3.182** Possuir Dashboard que forneça visibilidade em tempo real de incidência de vírus, status de atualização das máquinas, bem como quaisquer avisos ou erros que possam ocorrer.
- 3.183** A solução devera possuir um Dashboard que contenha as seguintes informações:
- 3.183.1** Máquinas com a lista de definições de vírus desatualizada.
- 3.183.2** Qual a versão do software instalado em cada máquina.
- 3.183.3** Os vírus que foram detectados.
- 3.183.4** Última comunicação com a console.
- 3.183.5** Quantidade de IDEs (definições de vacinas).
- 3.183.6** Data o último scan completo.
- 3.183.7** Possuir a capacidade de geração de relatórios gráficos.
- 3.184** O controle de dispositivos deve ocorrer no mínimo para os seguintes dispositivos:
- 3.184.1** Drive de CD/DVD;
- 3.184.2** Disquete;
- 3.184.3** Dispositivos de armazenamento em massa (ex.: *pen drives*, *memory cards*, discos rígidos externos, etc.);
- 3.184.4** Dispositivos de certificação digital (Token e Smart Card);
- 3.184.5** Modem;
- 3.184.6** Wireless;
- 3.184.7** IRDA;
- 3.184.8** Bluetooth.
- 3.185** A solução deverá prover controle de dispositivos com no mínimo as seguintes características: Somente Leitura (Read only), Acesso Completo (Full Access) e Bloqueado (Blocked).
- 3.186** A solução deverá permitir que o administrador defina uma White-List de dispositivos permitidos como Somente Leitura ou Acesso Completo.
- 3.187** Solução de controle de aplicativos para estações e servidores deverá ter as seguintes características:
- 3.187.1** Verificação na execução;
- 3.187.2** Verificação de aplicações no scan agendado;
- 3.187.3** Definição de mensagens personalizadas para os usuários finais;
- 3.187.4** Possuir uma lista de mais de 50 categorias de aplicativos diferentes.
- 3.188** Solução de controle de vazamento de dados confidenciais, integrado no mesmo agente, deve ter as seguintes características:
- 3.188.1** Controle de arquivos pelo seu tipo (ex: .docx, .xlsx, .zip, etc);
- 3.188.2** Controle de arquivos pelo seu conteúdo, utilizando tipos de informações (ex. Número de cartão de crédito) e



combinação de palavras chaves;

**3.188.3** Controle de arquivos com os tipos acima para os destinos de dispositivos como DVD e Pendrive e para destinos de aplicativos como Clientes de Email, redes sociais e Internet Browser;

**3.188.4** Mensagens Personalizadas para os usuários finais.

**3.189** Solução de bloqueio de navegação em determinados sites, integrado ao mesmo agente, deve ter as seguintes características:

**3.189.1** Lista de categorias específicas conforme o contexto, atualizadas automaticamente pelo fabricante;

**3.189.2** Opção de adicionais sites em uma lista de liberação de sites que não devem ser bloqueados (white-list);

**3.189.3** Opção de adicionais sites em uma lista de bloqueio de sites que devem ser bloqueados (black-list).

**3.190** Solução de verificação de patches pendentes nas máquinas protegidas informando quais os patches que faltam e as ameaças atreladas.

**3.191** Informar o tipo de patch, conforme o nível de criticidade.

**3.192** Possuir um controle de modificação do cliente Endpoint e contra a remoção não autorizada pelo cliente, possuindo uma senha.

**3.193** Solução de proteção de dados para Notebook e estações de trabalho deve suportar no mínimo as seguintes plataformas: Windows XP, Vista, 7 e versões superiores.

**3.194** A solução deve permitir autenticação automática no Windows através de single-sign-on.

**3.195** Deve possuir mecanismos e ferramentas próprias de recuperação de disco com possibilidade de Boot através de CD ou pendrive.

**3.196** Instalação Remota através do AD por Script de login.

**3.197** Serviços de detecção e remoção de Ransomware.

### **Gestão de vulnerabilidades**

Os serviços de “Gestão de Vulnerabilidades” deverão ser capazes de detectar e avaliar vulnerabilidades encontradas nos sistemas e recursos de TI e na solução de segurança fornecida, especialmente quanto ao impacto no ambiente computacional e ao risco inerente à segurança das informações custodiadas por meio de análises periódicas de conformidade.

**3.198** Para efeito de comprovar a conformidade do ambiente implantado, a cada 90 (noventa) dias a Contratada deverá realizar varreduras nos roteadores e equipamentos, que compõem o sistema, identificando e relatando possíveis vulnerabilidades encontradas;

**3.199** Deverá verificar vulnerabilidades no ambiente para, no mínimo: detecção de hot fixes, service packs, registros, backdoors, trojans, malwares, peer to peer, portas de serviço habilitadas e antivírus;

**3.200** Deverá detectar vulnerabilidades em aplicações baseadas em WEB, bases de dados, aplicações comerciais, sistemas operacionais e dispositivos de rede;

**3.201** Deverá propor a aplicação de melhorias na topologia utilizada pelo Conselho Federal de Farmácia - CFF;

**3.202** Deverá sugerir melhorias de segurança de forma a minimizar a exploração de vulnerabilidades no ambiente de redes;

**3.203** Deverá disponibilizar relatórios analíticos contendo dados, informações, indicadores e métricas que permitam avaliar a exposição dos ativos da aos riscos identificados com, pelo menos, as seguintes informações: Descrição da vulnerabilidade, Plataforma (sistema operacional, servidor web, banco de dados, etc) e nível de risco;

**3.204** O relatório deverá indicar níveis de severidade para os problemas encontrados, de modo a priorizar as ações a serem desenvolvidas. Estes níveis deverão estar classificados em uma escala de Risco Alto, Meio e Baixo;

**3.205** Os relatórios produzidos deverão ser submetidos à apreciação do Conselho Federal de Farmácia - CFF, de modo que possa ser comprovada a conformidade do ambiente em produção e/ou aprovada a implementação de medidas identificadas como necessárias para correção de problemas apontados;

**3.206** Para cada uma das vulnerabilidades apontadas nos relatórios, a Contratada deverá descrever a falha encontrada, indicar a(s) possível(eis) solução(ões) e o(s) responsável(eis) pela sua implantação. No caso de ainda inexistir uma solução específica, a Contratada deverá indicar qual ação deverá ser tomada para que, de forma paliativa, o problema seja contornado até que esteja disponível uma solução definitiva (inclusive instruções para aplicação de correções em produtos de terceiros);

**3.207** A data e a hora para execução dos procedimentos de varredura serão acordadas com o Conselho Federal de Farmácia - CFF, devendo ser executados fora dos horários de uso intenso da rede, no caso das sondagens interferirem no funcionamento normal dos equipamentos/sistemas avaliados;

**3.208** O Conselho Federal de Farmácia - CFF e a Contratada deverão responsabilizar-se pela implementação e eficácia das soluções que lhes couber, conforme indicado nos relatórios;

**3.209** Caberá ao Conselho Federal de Farmácia - CFF decidir pela implementação, ou não, de qualquer sugestão apresentada nos relatórios, assumindo a responsabilidade por problemas, que porventura vierem a ser causados nos equipamentos e serviços da rede, em função de ter optado por não acatar determinada recomendação.

#### **Centro de Operações de Segurança - SOC:**

**3.210** O Centro de Operações de Segurança (Security Operation Center - SOC) da contratada será o responsável por monitorar, gerenciar e administrar remotamente equipamentos e softwares componentes da solução de segurança fornecida e realizar a resposta a incidentes de segurança na rede do Conselho Federal de Farmácia - CFF, 24 horas por dia e 7 dias por semana.

**3.211** A contratada deverá manter 1 (um) Centro de Operações de Segurança (Security Operation Center - SOC) fora das dependências do Conselho Federal de Farmácia – CFF, administrando os sistemas de detecção a partir de um console centralizado, monitorando de forma pró-ativa o tráfego “ENTRANTE” e “SAINTE” e as tentativas de intrusão, buscando e interrompendo ataques e atividades suspeitas em tempo real, 24 horas por dia os 7 dias da semana;

**3.212** O Centro de Operações de Segurança – SOC deverá monitorar o ambiente do Conselho Federal de Farmácia - CFF utilizando canais de dados WAN próprios e redundantes dedicado a este fim, conectando a “solução de segurança” ao Centro de Operações de Segurança – SOC (“Rede de Gerência” e “Rede de Monitoração”) da contratada com acesso restrito e por meio de conexão segura e criptografada;

**3.213** O Centro de Operações de Segurança – SOC deverá monitorar o perímetro do Conselho Federal de Farmácia - CFF utilizando para isso um SIEM (Security Information and Event Management) para identificar e responder a ameaças de segurança em tempo real 24 horas por dia, 7 dias na semana;

**3.214** Os profissionais localizados no Centro de Operações de Segurança – SOC deverão instalar sensores nos servidores Web do Conselho Federal de farmácia – CFF de forma a monitorar qualquer mudança realizada de forma maliciosa em arquivos e pastas, através de verificação de hash em tempo real;

**3.215** Os profissionais localizados no Centro de Operações de Segurança – SOC deverão realizar a manutenção da infraestrutura de segurança, atualizando patches, correções e versões ou releases mais recentes dos softwares;

**3.216** Os profissionais localizados no Centro de Operações de Segurança – SOC deverão realizar a manutenção periódica de configurações, regras e políticas do ambiente monitorado remotamente ou on-site;

**3.217** Os profissionais localizados no Centro de Operações de Segurança – SOC deverão executar procedimentos, resolver problemas e esclarecer dúvidas relacionadas com instalação, configuração, atualização, funcionamento e uso dos equipamentos necessários ao funcionamento da solução de segurança;

**3.218** Os profissionais localizados no Centro de Operações de Segurança – SOC deverão fazer o ajuste fino (tunning) e às customizações de configuração de toda a solução, adequando-a ao ambiente do Conselho Federal de Farmácia - CFF;

**3.219** Os profissionais localizados no Centro de Operações de Segurança – SOC deverão monitorar e resolver problemas de mau funcionamento, baixo desempenho ou de excessivo consumo de recursos dos equipamentos componentes da solução de segurança;

**3.220** Os profissionais localizados no Centro de Operações de Segurança – SOC deverão executar a gestão estratégica de cada equipamento ou software utilizado na solução de segurança, monitorando a utilização de CPU, memória e demais recursos monitoráveis, de forma a construir baseline com informações de, pelo menos, 3 (três) meses;

**3.221** Os profissionais localizados no Centro de Operações de Segurança – SOC deverão definir e implantar as rotinas de backup de todos os equipamentos componentes da solução de segurança. Nesse sentido, será responsabilidade da contratada o backup realizado pela própria;

**3.222** Os profissionais localizados no Centro de Operações de Segurança – SOC deverão monitorar o funcionamento da solução de segurança (servidores e processos de serviços) 24 horas por dia, 7 dias da semana. Em caso de paralisação de servidores ou serviços monitorados, a equipe de especialistas da contratada deverá entrar em contato imediato com os responsáveis técnicos do Conselho Federal de Farmácia - CFF informando o tipo de alerta e a solução dele;

**3.223** Ao detectar tentativas de ataques, a equipe de especialistas da contratada deverá adotar, de imediato, as medidas de combate ao ataque identificado. No caso dessas medidas implicarem em interrupções e/ou descaracterização dos serviços em uso, a empresa deverá entrar em contato com o Conselho Federal de Farmácia - CFF em no máximo, 15 (quinze) minutos, para expor o problema identificado, as possíveis ações a serem tomadas e as suas respectivas consequências e, eventualmente, obter a autorização para adotá-las;

**3.224** A contratada deverá envidar seus melhores esforços para que, quando fizer parte do escopo da modalidade de serviço contratado, quaisquer ataques, invasões ou incidentes sofridos pelo Conselho Federal de Farmácia - CFF em suas redes e/ou sistemas, sejam identificados, controlados, interrompidos ou cessados, em caráter provisório ou definitivo, mantendo o Conselho Federal de Farmácia - CFF sempre a par de tais ocorrências;

**3.225** Os profissionais localizados no Centro de Operações de Segurança – SOC deverão informar sobre incidentes ou resultado de monitoração nos ativos sob gestão exclusiva de terceiros ou do Conselho Federal de Farmácia - CFF;

**3.226** A contratada deverá realizar perícia forense quando ocorrem ataques a redes e/ou sistemas do Conselho Federal de Farmácia – CFF, identificando a vulnerabilidade explorada e o dano sofrido pelos sistemas. A contratada deverá propor soluções em caráter provisório ou definitivo indicando o responsável por ela.

#### **Suporte Técnico 24X7:**

**3.227** A contratada concederá ao Conselho Federal de Farmácia - CFF garantia integral durante todo o período do contrato, on-site com atendimento 24 horas por dia e 7 dias por semana e sem número limite de chamados, a contar da data de instalação, contra qualquer defeito de fabricação que os equipamentos da solução venham a apresentar, incluindo avarias no transporte até o local de entrega, mesmo ocorrida sua aceitação/aprovação.

**3.228** O serviço de suporte técnico deverá ser prestado 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, na sede do Conselho Federal de Farmácia - CFF, em Brasília – DF, on-site e sem número limite de chamados, através de telefone ou e-mail para toda a solução ofertada, por técnicos devidamente habilitados e certificado pelo fabricante dos equipamentos integrantes da solução, e sem qualquer ônus adicional;

**3.229** A contratada deverá garantir a atualização dos microcódigos, firmwares, drivers e *softwares* instalados, provendo o fornecimento e instalação de novas versões por necessidade de correção de problemas ou por implementação de novos releases durante a vigência do contrato;

**3.230** Durante a vigência do contrato, deve ser efetuada manutenção preventiva de acordo com as recomendações do fabricante e critérios prescritos pelo Conselho Federal de Farmácia - CFF, destinada a reduzir a probabilidade de falha ou a degradação do funcionamento da solução, compreendendo: ajustes às especificações do fabricante, manutenção do bom estado de conservação dos equipamentos, substituição de componentes que comprometam o bom funcionamento ou estejam com a vida útil reduzida, modificações necessárias com objetivo de atualização dos equipamentos, limpeza externa e interna, regulação, ajustagem, execução de rotinas de testes padronizados e verificação da existência de danos físicos no equipamento, entre outras ações que garantam a operacionalidade dos equipamentos, com fornecimento de peças, componentes e acessórios, sem apresentar qualquer ônus adicional para o Conselho Federal de Farmácia - CFF. A contratada deve fornecer, quando da assinatura do contrato, cronograma com previsão das manutenções preventivas;

**3.231** A manutenção corretiva será efetuada sempre que a solução apresente falhas que impeçam o seu funcionamento normal e/ou requeiram a intervenção de técnico especializado;

**3.232** As manutenções corretivas deverão ter a cobertura de todo e qualquer defeito apresentado, inclusive substituição de peças, partes, mídias, componentes de acessórios, dos equipamentos integrantes da solução objeto desta licitação, garantindo a confiabilidade do seu funcionamento durante todo o prazo do contrato sem apresentar qualquer ônus adicional para o Conselho Federal de Farmácia - CFF;

**3.233** Nos casos em que as manutenções necessitem de paradas de equipamento(s), o Conselho Federal de Farmácia - CFF deve ser notificado para providenciar a aprovação da manutenção, ou agendar nova data para execução das atividades;

**3.234** As ferramentas e equipamentos necessários à manutenção serão de responsabilidade da CONTRATADA;

**3.235** As manutenções preventivas e corretivas serão de responsabilidade da CONTRATADA, sem custos adicionais;

**3.236** Definição das manutenções solicitadas segundo a norma ABNT NBR 5462-1994 ou posterior: **MANUTENÇÃO PREVENTIVA**: efetuada em intervalos predeterminados ou de acordo com critérios prescritos. Destinada a reduzir a probabilidade de falha ou a degradação do funcionamento de um item; e **MANUTENÇÃO CORRETIVA**: efetuada após a ocorrência de uma pane. Destinada a recolocar um item em condições de executar uma função requerida;

**3.237** Durante o período de garantia, qualquer componente da solução que apresente defeito ou mau funcionamento, deve ser substituído em até 04 (quatro) horas. As novas unidades utilizadas na substituição de peças defeituosas devem ter garantia de forma a atender o prazo inicialmente contratado;

**3.238** O suporte técnico será acionado em caso de quaisquer indisponibilidades da solução contratada, devendo haver o atendimento, no prazo máximo de 4 (quatro) horas a partir da abertura do chamado para todos os componentes deste termo;

**3.239** Todos os defeitos identificados devem ser solucionados em, no máximo 24 (vinte e quatro) horas após a abertura do chamado, incluída nesse intervalo eventual solução de contorno;

**3.240** Caso haja necessidade de retirada de algum produto, para fins de reparo, a contratada deverá substituir por outro produto em até 04 (quatro) horas, com características iguais ou superiores, sendo a instalação, configuração de responsabilidade da Contratada. Esta substituição será em caráter definitivo se no prazo de 30 (trinta) dias a CONTRATADA não devolver o produto retirado em perfeitas condições de uso;

**3.241** A CONTRATADA deve emitir relatórios de todas as intervenções realizadas, preventivas e corretivas, programadas ou de emergência, ressaltando os fatos importantes e detalhando os pormenores das intervenções, de forma a manter registros completos das ocorrências e subsidiar as decisões da administração do Conselho Federal de Farmácia - CFF, caso requeiram;

**3.242** Durante o período de garantia, a contratada compromete-se a substituir, em até 15 (quinze) dias úteis, sem qualquer ônus para o Conselho Federal de Farmácia - CFF, os equipamentos que apresentarem, em um período de 60 (sessenta dias), duas ocorrências de defeitos por inoperância de produto ou 3 (três) ocorrências de deficiência operacional do produto. Neste caso, as novas unidades empregadas na substituição das defeituosas ou danificadas deverão ter prazo de garantia igual ou superior ao das substituídas;

**3.243** Sempre que necessário um suporte “*in loco*” no Conselho Federal de Farmácia - CFF, O PROPONENTE deverá manter seus funcionários devidamente identificados por crachá em lugar visível;

**3.244** Deve ser disponibilizado canal de atendimento e chamado técnico, disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana através de site na Internet e canal telefônico 0800 (0800 quando o atendimento estiver fora de Brasília), ou número de telefone em Brasília - DF;

**3.245** Os atendentes do Centro de Operações de Segurança - SOC da contratada deverão ter conhecimento da infraestrutura organizacional do Conselho Federal de Farmácia - CFF, devendo identificar os funcionários em conjunto com a contratante após a assinatura do contrato;

**3.246** As informações referentes aos chamados efetuados pelo Conselho Federal de Farmácia - CFF deverão, logo que registradas, estar disponíveis para consultas no Portal de Serviços disponibilizado pela empresa contratada, pelo período de 01 (um) ano, contado a partir da data de fechamento do chamado;

**3.247** As informações de chamados, recuperadas por intermédio do Portal de Serviços deverão abranger: "Número", "Data e Hora da Abertura", "Status" (aberto/fechado), "Responsável pela Abertura", "Técnico Encarregado do Atendimento", "Descrição do Problema", "Histórico" (data/hora e descrição), "Ocorrências" (data/hora e descrição) e deverão ser de uso único e exclusivo do Conselho Federal de Farmácia - CFF;

**3.248** O Portal de Serviços deverá permitir a realização de consultas e impressão de relatórios, individualizados ou cumulativos, por número do chamado, status, data/período de abertura, unidade responsável pela abertura, técnico encarregado do atendimento e chamados com falhas de atendimento;

**3.249** Ao receber uma solicitação de abertura de chamado, o atendente deverá registrar as informações relativas ao mesmo (responsável pela abertura, descrição do problema, etc) e fornecer o número que lhe foi atribuído;

**3.250** Ao receber uma ligação para um chamado já aberto, o atendente deverá solicitar o número que lhe foi atribuído por ocasião da abertura, registrar as novas informações passadas e transmiti-las ao técnico responsável pelo acompanhamento e resolução;

**3.251** Quando as informações e solicitações passadas exigirem uma nova interlocução com o Conselho Federal de Farmácia - CFF, de forma análoga aos procedimentos de abertura, o técnico responsável pelo acompanhamento e resolução do chamado deverá entrar em contato com o responsável pela abertura, em um prazo máximo de 01 (uma) hora.

**3.252** Quando solucionados, os chamados deverão ser fechados pelo responsável pelo atendimento, de comum acordo com o Conselho Federal de Farmácia - CFF, não sendo admitido, em nenhuma hipótese, o fechamento de chamados sem o consentimento do responsável pela abertura.

#### **Migração dos Serviços:**

**3.253** A migração dos serviços deverá ser realizada em no máximo 15 (quinze) dias corridos, e de maneira transparente para que não haja interrupções, em nenhum instante, de todos os serviços descritos neste documento, que já estão em uso pelo CFF e são essenciais para o funcionamento seguro de todo parque computacional. Visto que este serviço será realizado apenas uma vez, o seu pagamento também será único.

#### **Treinamento:**

**3.254** Trata dos treinamentos a serem prestados ao Conselho Federal de Farmácia - CFF com vistas à transferência de conhecimento, compreendendo as tecnologias envolvidas nos serviços contratados, assim como capacitação nos produtos e softwares utilizados para atender aos requisitos das especificações técnicas;

**3.255** A CONTRATADA deverá realizar treinamento destinado a preparar técnicos do Conselho Federal de Farmácia - CFF na instalação, configuração e utilização de funcionalidades básicas e avançadas da solução, assim como realizar atividades de suporte (*troubleshooting*) para todos os equipamentos da solução;

**3.256** A CONTRATADA deverá realizar treinamento em programação segura, destinado a preparar técnicos do Conselho Federal de Farmácia - CFF na parametrização de regex do firewall de aplicação – WAF;

**3.257** O treinamento será realizado em Brasília (DF), nas instalações do Conselho Federal de Farmácia - CFF ou em

instalações próprias da CONTRATADA, com duração mínima de 10 (dez) horas para a solução de segurança e de 10 (dez) horas para a solução de segurança de aplicação WAF, para 4 (quatro) pessoas;

**3.258** O treinamento deverá contemplar, no mínimo, 20 (vinte) horas de atividades práticas. Para a consecução da parte prática, poderão ser utilizados equipamentos similares aos ofertados, além dos softwares que fazem parte da solução, ou os próprios equipamentos fornecidos, desde que o treinamento não cause impacto nas operações do ambiente corporativo do Conselho Federal de Farmácia - CFF;

**3.259** O instrutor designado pela CONTRATADA deverá possuir conhecimento na solução implantada para configurar, operar e prestar suporte técnico aos produtos contratados, assim como ter participado das etapas de instalação e configuração dos equipamentos durante a execução do projeto de implantação da solução de segurança contratada pelo Conselho Federal de Farmácia - CFF;

**3.260** As datas e horários para realização dos treinamentos serão definidos pelo Conselho Federal de Farmácia - CFF, em momento posterior à implantação dos equipamentos nas instalações;

**3.261** Deverá ser fornecido certificado de participação individual;

**3.262** Todos os custos de material didático e instalações são de responsabilidade da contratada;

**3.263** O pagamento deste serviço será realizado apenas quando este for solicitado.

#### **4. CONDIÇÕES DE ENTREGA**

**4.1** Os equipamentos integrantes da solução devem ser entregues na sede do Conselho Federal de Farmácia – CFF em Brasília - DF, de segunda a sexta-feira, das 08h às 11h30 e das 14h às 17h30, exceto feriados;

**4.2** O prazo de entrega será de 30 (trinta) dias corridos, contados da assinatura do contrato;

**4.3** Caso a CONTRATADA se veja impossibilitada de cumprir o prazo estipulado para a entrega dos produtos, deverá apresentar, até a data de vencimento fixada no contrato, justificativas escritas e devidamente comprovadas, apoiando o pedido de prorrogação em um ou mais dos seguintes fatos:

**4.4** Ocorrência de fato superveniente, excepcional ou imprevisível, estranho à vontade das partes que altere fundamentalmente as condições do contrato;

**4.5** Impedimento decorrente de fato ou ato de terceiros, reconhecido pelo Conselho Federal de Farmácia - CFF em documento contemporâneo à sua ocorrência.

**4.6** O pedido de prorrogação, com indicação de novo prazo de entrega, quando for o caso, deverá manifestar-se formalmente à fiscalização do Conselho Federal de Farmácia - CFF, que poderá acolher ou não o requerimento da CONTRATADA;

**4.7** Vencido o prazo fixado neste instrumento ou o de uma eventual prorrogação sem que os produtos tenham sido entregues, o Conselho Federal de Farmácia - CFF oficiará a CONTRATADA acerca do transcurso da data limite, passando o inadimplemento, a partir daí, a ser considerado como recusa do cumprimento da obrigação pactuada e, por conseguinte, sujeitando a CONTRATADA às penalidades previstas;

**4.8** Os equipamentos integrantes das soluções deverão ser novos e de primeiro uso e deverão ser entregues em perfeito estado de funcionamento, sem marcas, amassados e arranhões e com os lacres do fabricante;

**4.9** Correrão por conta da CONTRATADA as despesas com o frete, transporte, seguro e demais custos advindos da entrega dos produtos.

**4.10** Todas as informações referem-se ao item 3 (Especificações técnicas).

#### **5. CONDIÇÕES DE INSTALAÇÃO, IMPLEMENTAÇÃO E/OU CUSTOMIZAÇÃO**

**5.1.** Os equipamentos integrantes da solução devem ser instalados no Data Center do Conselho Federal de Farmácia - CFF em Brasília, DF, em qualquer dia da semana, inclusive fora do horário comercial, ficando a critério do Conselho Federal de Farmácia - CFF essa definição;

**5.2.** Antes do início do projeto deverá ser convocada pela contratada uma reunião com a equipe da Tecnologia da Informação (TI) do Conselho Federal de Farmácia - CFF. Serão apresentados todos os aspectos de concepção do projeto, incluindo configurações e políticas. Deverá ser apresentado pela contratada o plano de execução dos serviços, detalhando responsáveis, prazos e fases, além de previsão de eventos e seus impactos na infraestrutura existente. Novas reuniões poderão ser convocadas por ambas as partes de modo a definir todos os pormenores da solução e eliminar pendências;

##### **São premissas de projeto:**

**5.3.** A instalação deverá ser efetuada de forma a não afetar o funcionamento dos sistemas, recursos ou equipamentos atualmente em operação e nem impedir ou interromper, por períodos prolongados, a rotina de trabalho dos funcionários do Conselho Federal de Farmácia - CFF. Para tanto, quando necessário, o serviço deverá ser executado fora do horário comercial (períodos noturnos e finais de semana), em horários previamente agendados;

**5.4.** No caso de interrupção de sistemas, recursos, equipamentos ou rotinas de trabalho de qualquer setor funcional em decorrência da instalação a ser efetuada, esta parada deverá ser devidamente planejada e acordada com antecedência junto ao Conselho Federal de Farmácia - CFF;

**5.5.** Todos os componentes de *hardware* e *software* requeridos para atender as funcionalidades exigidas neste edital e tornar a solução operante, mesmo que não tenham sido especificados e cotados na proposta apresentada, serão consideradas partes integrantes dos serviços de instalação e deverão ser fornecidos pela contratada.

**É responsabilidade da contratada:**

**5.6.** Desenvolver e apresentar planejamento da instalação, indicando as atividades que serão realizadas, incluindo: Diagrama de configuração com a especificação dos componentes; Definição/requisitos de redes LAN; Montagem e instalação física dos equipamentos da solução, instalação no *rack* (*firewalls*) e nos tetos dos andares (*access points*) de acordo com as recomendações do fabricante, conexões lógicas e elétricas (com implementação de padrão de identificação dos cabos) e testes de funcionamento, atualizações de *software*, *patches*, *drivers* e *firmwares* para suas versões mais recentes;

**5.7.** Customização e operacionalização de todos os equipamentos envolvidos;

**5.8.** Apresentar testes de funcionamento de redundância para todos os equipamentos;

**5.9.** Instalação de softwares de gerência, quando disponíveis e/ou solicitados, em estação de gerenciamento indicada pelo Conselho Federal de Farmácia - CFF;

**5.10.** Executar o processo de integração dos equipamentos com os atualmente em operação, fazendo a devida compatibilidade técnica-operacional, garantindo desta forma que o ambiente atual possa ser integrado plenamente ao novo. Qualquer problema ou incompatibilidade deverá ser resolvido pela contratada;

**5.11.** Correrá por conta exclusiva do proponente a responsabilidade pelo deslocamento do seu técnico até o local de instalação do equipamento.

**Projeto e Documentação:**

**5.12.** O projeto deve ter, no mínimo, fases de concepção, implementação e homologação;

**5.13.** O início de cada fase deve ser marcado por uma reunião, onde serão definidas e concebidas as atividades da fase seguinte. Depois de identificadas as atividades, será confeccionado documento a ser aprovado pelo Conselho Federal de Farmácia - CFF através de “de acordo” em ata, descrevendo todas as necessidades e requisitos para cada fase;

**5.14.** Todo o projeto deve ser documentado no formato “*as built*”, utilizando metodologia apropriada. Ao final da implantação, a contratada deverá entregar a documentação para o Conselho Federal de Farmácia - CFF no formato impresso e eletrônico;

**5.15.** Todas as informações deste item referem-se ao Item 3 (Especificações Técnicas).

**6. CONDIÇÕES DE ACEITE**

**6.1.** O aceite da solução será efetuado após um período de testes de até 15 (quinze) dias uteis pelo Conselho Federal de Farmácia - CFF, quando verificará se os serviços atendem completamente todos os requisitos e condições deste projeto básico. Este período de testes se iniciará a partir do “comunicado formal da conclusão do serviço de instalação e configuração” pela contratada;

**6.2.** Não será permitida a subcontratação (terceirização) da execução dos serviços;

**6.3.** Caso sejam identificadas quaisquer imperfeições, o Conselho Federal de Farmácia - CFF poderá rejeitar no todo ou em parte o(s) item(s) entregue(s);

**6.4.** O prazo de conclusão do serviço de instalação e configuração será de até 15 (quinze) dias corridos e contados a partir da assinatura do contrato, sendo de responsabilidade da contratada a emissão do “comunicado formal da conclusão do serviço de instalação e configuração”;

**6.5.** O Conselho Federal de Farmácia - CFF emitirá o “termo de aceite definitivo” em até 10 (dez) dias corridos após a conclusão do período de testes. O “termo de aceite definitivo” será assinado pelo gestor do contrato ou seu substituto, e está vinculado ao atendimento completo dos requisitos, condições e funcionamento correto da solução conforme item 3 (Especificações Técnicas);

**6.6.** Caso ocorram inconformidades nos equipamentos/serviços entregues, o prazo estipulado para emissão do “termo de aceite definitivo” recomeçará a contar a partir da entrega dos equipamentos/serviços devidamente regularizados;

**6.7.** A contratada deverá substituir o(s) equipamento(s) entregue(s) com defeito ou fora das especificações no prazo de até 5 (cinco) dias corridos a partir da manifestação do Conselho Federal de Farmácia - CFF;

**6.8.** Caso ocorram inconformidades nos serviços entregues, o prazo estipulado para emissão do “termo de aceite definitivo” recomeçará a contar a partir da entrega dos serviços devidamente regularizados;

**6.9.** A contratada deverá corrigir falhas e erros em serviços executados no prazo de até 5 (cinco) dias corridos a partir da

manifestação do Conselho Federal de Farmácia - CFF;

**6.10.** A simples emissão do "termo de aceite definitivo" pelos equipamentos entregues e serviços prestados não isenta a contratada de obrigações futuras;

**6.11.** Para a entrega da documentação final, o prazo será de 30 (trinta) dias corridos após concluir a entrega, instalação e configuração de toda a solução fornecida.

## **7. REQUISITOS DE HABILITAÇÃO**

**7.1** As empresas participantes do processo licitatório deverão, obrigatoriamente, apresentar os seguintes documentos:

**7.2** Atestado de capacidade técnica fornecido por pessoa jurídica de direito público ou privado, no qual comprove e demonstre que a licitante executou serviços de segurança de rede utilizando UTM e EndPoint, fazendo menção ao fabricante e modelo utilizado e que atendeu satisfatoriamente;

**7.3** Atestado de capacidade técnica fornecido por pessoa jurídica de direito público ou privado, no qual comprove e demonstre que a licitante executou serviços de segurança de aplicação utilizando Firewall de Aplicação WAF, fazendo menção ao fabricante e modelo utilizado e que atendeu satisfatoriamente;

**7.4** Atestado de capacidade técnica fornecido por pessoa jurídica de direito público ou privado, no qual comprove e demonstre que a licitante executou serviços de monitoramento de arquivo de aplicação Web, através de verificação de Hash, fazendo menção ao fabricante e modelo utilizado e que atendeu satisfatoriamente;

**7.5** Atestado de capacidade técnica fornecido por pessoa jurídica de direito público ou privado, no qual comprove e demonstre que a licitante executou serviços de testes de intrusão (pentest) e atendeu satisfatoriamente;

**7.6** Atestado de capacidade técnica fornecido por pessoa jurídica de direito público ou privado, no qual comprove e demonstre que a licitante executou serviços de análises de vulnerabilidades e atendeu satisfatoriamente;

**7.7** Atestado de capacidade técnica fornecido por pessoa jurídica de direito público ou privado, no qual comprove e demonstre que a licitante executou serviços de SOC - Security Operation Center, com atendimento 24x7 e atendeu satisfatoriamente;

**7.8** Atestado de capacidade técnica fornecido por pessoa jurídica de direito público ou privado, no qual comprove e demonstre que a licitante executou serviços de SIEM SECURITY - Security Information and Event Management em SOC (Security Operation Center), fazendo menção ao fabricante e modelo utilizado e que atendeu satisfatoriamente;

**7.9** Atestado de capacidade técnica fornecido por pessoa jurídica de direito público ou privado, no qual comprove e demonstre que a licitante executou serviços de treinamento em programação segura e atendeu satisfatoriamente;

**7.10** A licitante deve apresentar declaração fazendo constar que concorda e atende integralmente os termos deste edital e seus anexos, sem restrições de qualquer ordem;

**7.11** A licitante deve apresentar declaração fazendo constar que concorda e atende integralmente a exigência de suporte técnico ON-SITE nas dependências do Conselho Federal de Farmácia - CFF, 24X7 sem limite de chamados técnicos, sem restrições de qualquer ordem;

**7.12** A licitante deve apresentar declaração fazendo constar que nos preços cotados já estão incluídas todas e quaisquer despesas necessárias para a perfeita execução do objeto desta licitação;

**7.13** A licitante deve apresentar declaração informando Fabricante, Modelo, versão de softwares e link (URL) da solução ofertada para o UTM e o EndPoint que deverão trabalhar em conjunto;

**7.14** Qualquer solicitação de esclarecimentos deverá ser efetuada ao pregoeiro via e-mail: [licitacao@cff.org.br](mailto:licitacao@cff.org.br).

## **8 JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO**

**8.1** A Justificativa e objetivo da contratação encontram-se pormenorizados em Tópico específico dos Estudos Preliminares, apêndice desse Termo de Referência.

## **9 DA CLASSIFICAÇÃO DOS SERVIÇOS E FORMA DE SELEÇÃO DO FORNECEDOR**

**9.1** Trata-se de serviço comum de caráter continuado sem fornecimento de mão de obra em regime de dedicação exclusiva, a ser contratado mediante licitação, na modalidade pregão, em sua forma eletrônica.

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

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

## **10 DAS OBRIGAÇÕES DA CONTRATANTE**

- 10.1** Exigir o cumprimento de todas as obrigações assumidas pela Contratada, de acordo com as cláusulas contratuais e os termos de sua proposta;
- 10.2** Exercer o acompanhamento e a fiscalização dos serviços, por servidor especialmente designado, anotando em registro próprio as falhas detectadas, indicando dia, mês e ano, bem como o nome dos empregados eventualmente envolvidos, e encaminhando os apontamentos à autoridade competente para as providências cabíveis;
- 10.3** Notificar a Contratada por escrito da ocorrência de eventuais imperfeições, falhas ou irregularidades constatadas no curso da execução dos serviços, fixando prazo para a sua correção, certificando-se que as soluções por ela propostas sejam as mais adequadas;
- 10.4** Pagar à Contratada o valor resultante da prestação do serviço, no prazo e condições estabelecidas neste Termo de Referência;
- 10.5** Efetuar as retenções tributárias devidas sobre o valor da Nota Fiscal/Fatura da contratada, no que couber, em conformidade com o item 6 do Anexo XI da IN SEGES/MP n. 5/2017.
- 10.6** Não praticar atos de ingerência na administração da Contratada, tais como:
- 10.6.1** exercer o poder de mando sobre os empregados da Contratada, devendo reportar-se somente aos prepostos ou responsáveis por ela indicados, exceto quando o objeto da contratação previr o atendimento direto, tais como nos serviços de recepção e apoio ao usuário;
- 10.6.2** direcionar a contratação de pessoas para trabalhar nas empresas Contratadas;
- 10.6.3** considerar os trabalhadores da Contratada como colaboradores eventuais do próprio órgão ou entidade responsável pela contratação, especialmente para efeito de concessão de diárias e passagens.
- 10.7** Fornecer por escrito as informações necessárias para o desenvolvimento dos serviços objeto do contrato;
- 10.8** Realizar avaliações periódicas da qualidade dos serviços, após seu recebimento;
- 10.9** Fiscalizar o cumprimento dos requisitos legais, conforme definido na Lei 14.133/2021.

## **11 DAS OBRIGAÇÕES DA CONTRATADA**

- 11.1** Executar os serviços em observância às obrigações constantes deste Termo de Referência, aos encargos e responsabilidade, com início para execução dos trabalhos em até 30 (trinta) dias após a data de assinatura do contrato.
- 11.2** Assegurar a excelência na qualidade da prestação de serviços.
- 11.3** Cumprir os prazos fixados neste Termo de Referência, visando assegurar a pontualidade na prestação de serviços.
- 11.4** Atender às observações e reclamações da fiscalização do CFF, concernentes à execução dos serviços, adotando as providências requeridas nos prazos determinados pela Contratante ou em data acertada entre as partes.
- 11.5** Apresentar o(s) documento(s) exigido(s) (Nota Fiscal, Relatórios e Certidões de Regularidade Fiscal e Social) pelo CFF para o pagamento das faturas emitidas.
- 11.6** Arcar com as despesas decorrentes de infração/multas, taxas, emolumentos, impostos e outras advindas da prestação de serviços.
- 11.7** Executar os serviços de acordo com as especificações constantes neste termo de referência e cumprir todas as orientações do CFF para o fiel desempenho das atividades específicas.
- 11.8** Aceitar, nas mesmas condições pactuadas, os acréscimos ou supressões que se fizerem necessárias, até 25% (vinte e cinco por cento) do valor inicial contratado.
- 11.9** Comunicar ao gestor do contrato qualquer anormalidade constatada e prestar os esclarecimentos solicitados.
- 11.10** Manter, durante o período de vigência do contrato, o atendimento das condições de habilitação exigidas no edital de licitação.
- 11.11** Assumir todos os encargos previdenciários e obrigações sociais previstos na legislação social e trabalhista em vigor, obrigando-se a saldá-los na época própria, vez que os seus funcionários não manterão nenhum vínculo empregatício com o CFF.
- 11.12** Assumir todos os encargos de possível demanda trabalhista, civil ou penal, relacionada à execução do contrato.
- 11.13** A inadimplência da Contratada, com referência aos encargos sociais, comerciais e fiscais não transfere a responsabilidade por seu pagamento ao CFF, nem poderá onerar o objeto desta contratação, razão pela qual a Contratada renuncia expressamente a qualquer vínculo de solidariedade, ativa ou passiva, com o CFF.
- 11.14** Sujeitar-se a ampla e irrestrita fiscalização por parte do CFF para acompanhamento da execução do contrato, prestando todos os esclarecimentos que lhes forem solicitados e acatar as recomendações efetuadas pelo gestor do contrato.



**11.15** A existência da fiscalização por parte do CFF de nenhum modo diminui ou altera a responsabilidade da Contratada na prestação do seu serviço.

**11.16** É vedada ao licitante vencedor a contratação de funcionário pertencente ao quadro de pessoal do CFF para execução do contrato decorrente desta licitação.

**11.17** É vedada a veiculação de publicidade acerca do contrato, salvo se houver prévia autorização expressa e por escrito do CFF.

**11.18** É vedada a subcontratação de outra empresa para a execução do objeto deste Termo de Referência.

**11.19** Não será admitida a transferência de qualquer responsabilidade da Contratada para outras entidades, sejam fabricantes, técnicos, subempreiteiros, dentre outros.

**11.20** Respeitar os critérios de sigilo aplicáveis à realização do serviço objeto deste termo de referência, preservando todas as informações, resultados, relatórios e quaisquer outros documentos obtidos, não podendo a Contratada utilizá-los para qualquer fim, ou divulgá-los, reproduzi-los ou veiculá-los, a não ser que prévia e expressamente autorizado pelo CFF.

**11.21** Orientar seus funcionários a manter sigilo sobre fatos, dados ou documentos de que tomem conhecimento e que tenham relação ou pertinência com a Contratante, durante e após a prestação dos serviços, sujeitando-se à aplicação das sanções civis e penais pelo descumprimento.

**11.22** Prestar os serviços com diligência e perfeição, cumprindo rigorosamente as normas pertinentes e o estabelecido no edital de licitação, no termo de referência e seus anexos.

## **12 CONTROLE E FISCALIZAÇÃO DA EXECUÇÃO**

**12.1** O acompanhamento e a fiscalização da execução do contrato consistem na verificação da conformidade da prestação dos serviços, dos materiais, técnicas e equipamentos empregados, de forma a assegurar o perfeito cumprimento do ajuste, que serão exercidos por um ou mais representantes da Contratante, especialmente designados, na forma da Lei 14.133/2021.

**12.2** O representante da Contratante deverá ter a qualificação necessária para o acompanhamento e controle da execução dos serviços e do contrato.

**12.3** A verificação da adequação da prestação do serviço deverá ser realizada com base nos critérios previstos neste Termo de Referência.

**12.4** A fiscalização do contrato, ao verificar que houve subdimensionamento da produtividade pactuada, sem perda da qualidade na execução do serviço, deverá comunicar à autoridade responsável para que esta promova a adequação contratual à produtividade efetivamente realizada, respeitando-se os limites de alteração dos valores contratuais previstos na Lei 14.133/2021.

**12.5** A conformidade do material/técnica/equipamento a ser utilizado na execução dos serviços deverá ser verificada juntamente com o documento da Contratada que contenha a relação detalhada dos mesmos, de acordo com o estabelecido neste Termo de Referência, informando as respectivas quantidades e especificações técnicas, tais como: marca, qualidade e forma de uso.

**12.6** O representante da Contratante deverá promover o registro das ocorrências verificadas, adotando as providências necessárias ao fiel cumprimento das cláusulas contratuais, conforme o disposto na Lei 14.133/2021.

**12.7** O descumprimento total ou parcial das obrigações e responsabilidades assumidas pela Contratada, sobretudo quanto às obrigações e encargos sociais e trabalhistas, ensejará a aplicação de sanções administrativas, previstas neste Termo de Referência e na legislação vigente, podendo culminar em rescisão contratual, conforme disposto na Lei 14.133/2021.

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

**12.9** Durante a execução do objeto, o fiscal técnico deverá monitorar constantemente o nível de qualidade dos serviços para evitar a sua degeneração, devendo intervir para requerer à CONTRATADA a correção das faltas, falhas e irregularidades constatadas.

**12.10** A CONTRATADA poderá apresentar justificativa para a prestação do serviço com menor nível de conformidade, que poderá ser aceita pelo fiscal técnico, desde que comprovada a excepcionalidade da ocorrência, resultante exclusivamente de fatores imprevisíveis e alheios ao controle do prestador.

**12.11** O Gestor do contrato poderá exigir, uma vez comprovada a necessidade, o imediato afastamento de qualquer funcionário ou preposto da Contratada que, por justas razões, vier a desmerecer a confiança, embarace a fiscalização ou ainda que venha a se conduzir de modo inconveniente ou incompatível com o exercício das funções que lhe foram delegadas.

**12.12** A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas, vícios redibitórios, ou emprego de material inadequado ou de qualidade inferior e, na ocorrência desta, não implica corresponsabilidade da CONTRATANTE ou de seus agentes, gestores e fiscais, de conformidade com a Lei 14.133/2021.

### **13 DO REAJUSTE**

**13.1** Os preços são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas.

**13.2** Decorridos 12 (doze) meses da data da assinatura do contrato, o valor da taxa de administração poderá ser reajustado, alcançando a data da formulação da proposta, aplicando-se o índice IPCA acumulado no período ou outro índice oficial que vir a substituí-lo.

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

### **14 DO PAGAMENTO**

**14.1** O pagamento será mensal e efetuado pela Contratante no prazo de 15 (quinze) dias, contados do recebimento da Nota Fiscal/Fatura.

**14.2** A emissão da Nota Fiscal/Fatura será precedida do recebimento definitivo do serviço, conforme este Termo de Referência

**14.3** A Nota Fiscal ou Fatura deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada na Lei 14.133/2021.

**14.3.1** Constatando-se, junto ao SICAF, a situação de irregularidade do fornecedor contratado, deverão ser tomadas as providências previstas no do art. 31 da Instrução Normativa nº 3, de 26 de abril de 2018.

**14.4** O setor competente para proceder o pagamento deve verificar se a Nota Fiscal ou Fatura apresentada expressa os elementos necessários e essenciais do documento, tais como:

**14.4.1** o prazo de validade;

**14.4.2** a data da emissão;

**14.4.3** os dados do contrato e do órgão contratante;

**14.4.4** o período de prestação dos serviços;

**14.4.5** o valor a pagar; e

**14.4.6** eventual destaque do valor de retenções tributárias cabíveis.

**14.5** Havendo erro na apresentação da Nota Fiscal/Fatura, ou circunstância que impeça a liquidação da despesa, o pagamento ficará sobrestado até que a Contratada providencie as medidas saneadoras. Nesta hipótese, o prazo para pagamento iniciar-se-á após a comprovação da regularização da situação, não acarretando qualquer ônus para a Contratante;

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

**14.7** Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

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

**14.9** Previamente à emissão de nota de empenho e a cada pagamento, a Administração deverá realizar consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018.

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

**14.11** Persistindo a irregularidade, a contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à contratada a ampla defesa.

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

**14.12.1** Será rescindido o contrato em execução com a contratada inadimplente no SICAF, salvo por motivo de economicidade, segurança nacional ou outro de interesse público de alta relevância, devidamente justificado, em qualquer

caso, pela máxima autoridade da contratante.

**14.13** Quando do pagamento, será efetuada a retenção tributária prevista na Instrução Normativa 1.234/2012, da Receita Federal, quando couber.

**14.14** É vedado o pagamento, a qualquer título, por serviços prestados, à empresa privada que tenha em seu quadro societário servidor público da ativa do órgão contratante.

**14.15** Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido, de alguma forma, para tanto, fica convencionado que a taxa de compensação financeira devida pela Contratante, entre a data do vencimento e o efetivo adimplemento da parcela é calculada mediante a aplicação da seguinte fórmula:

$EM = I \times N \times VP$ , sendo:

EM = Encargos moratórios;

N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

I = (TX)	I =	( 6 / 100 ) 365	I = 0,00016438 TX = Percentual da taxa anual = 6%
----------	-----	--------------------	--

## 15 DOS RECURSOS ORÇAMENTÁRIOS.

**15.1** O valor estimado anual para a contratação é de R\$ 238.600,00 (Duzentos e trinta e oito mil e seiscentos reais)

### 15.1.1 Tabela de Valores estimados

ITEM	DESCRIÇÃO	QUANT. ESTIMADA MENSAL	PERÍODO	VALOR TOTAL MENSAL	VALOR TOTAL ANUAL
1	Firewall - UTM (Unified Threat Management)	1	MENSAL	2.900,00	34.800,00
2	Solução de Endpoint	180	MENSAL	3.500,00	42.000,00
3	Gestão de Vulnerabilidades	1	MENSAL	5.500,00	66.000,00
4	Centro de Operações de Segurança - SOC	1	MENSAL	4.400,00	52.800,00
5	Suporte Técnico 24X7	1	MENSAL	2.500,00	30.000,00
	<b>VALOR TOTAL MENSAL</b>			<b>18.800,00</b>	<b>225.600,00</b>
6	Migração dos Serviços	1	ÚNICO	3.000,00	3.000,00
7	Treinamento em programação segura	20	ÚNICO	10.000,00	10.000,00
	<b>VALOR TOTAL ANUAL</b>				<b>238.600,00</b>

**15.2** As despesas para atender a esta licitação estão programadas em dotação orçamentária própria, Conta de Despesa nº 6.2.2.1.1.01.04.04.005.030.011 - Outros Serviços de Tecnologia da Informação.

## APÊNDICE II

**MODELO DE PROPOSTA DE PREÇOS**  
**CONSELHO FEDERAL DE FARMÁCIA**  
(Processo Administrativo n.º 25.0.000002785-8)

Razão Social da Preponente:		
Endereço (completo):		
CNPJ/MF nº:	Insc. Estadual nº:	Insc. Municipal nº:
Telefone:	http:	E-mail:
Dados do Responsável Legal que assinará o Contrato		
Nome:	RG:	CPF:
Cargo/Função:		
Dados Bancários da Preponente		
BANCO (NOME E Nº):	AGÊNCIA (NOME E Nº):	CONTA CORRENTE Nº:

Prezado(a),

1. Apresentamos, em uma via, nossa proposta para o Fornecimento de solução integrada de serviços gerenciados de segurança (Managed Security Services - MSS) que deverão englobar provimento de equipamentos (hardware), software, serviços de segurança gerenciada em regime 24X7, monitoramento, gestão de vulnerabilidades, resposta a incidentes de segurança, migração dos serviços de maneira transparente (sem interrupções) e transferência de conhecimento para a equipe técnica do Conselho Federal de Farmácia - CFF, conforme condições estabelecidas no Termo de Referência.

2. O preço global para prestação dos serviços, está discriminado no quadro a seguir:

ITEM	DESCRIÇÃO	QUANT. ESTIMADA MENSAL	PERÍODO	VALOR TOTAL MENSAL (R\$)	DESCONTO OBTIDO	VALOR MENSAL COM DESCONTO (R\$)	VALOR TOTAL (R\$)
1	Firewall - UTM (Unified Threat Management)	1	MENSAL	2.900,00	.....%		
2	Solução de Endpoint	180	MENSAL	3.500,00			
3	Gestão de Vulnerabilidades	1	MENSAL	5.500,00			
4	Centro de Operações de Segurança - SOC	1	MENSAL	4.400,00			
5	Suporte Técnico 24X7	1	MENSAL	2.500,00			
<b>VALOR TOTAL MENSAL ESTIMADO</b>				<b>R\$18.800,00</b>		R\$ xx,xx	R\$ xx,xx

6	Migração dos Serviços	1	ÚNICO	3.000,00			
7	Treinamento em programação segura	20	ÚNICO	10.000,00			
VALOR TOTAL ANUAL							R\$ xx,xx

**Obs.:** A proposta de preço não poderá ser inferior a 60 (sessenta) dias e declaração expressa de que, no preço proposto, estejam incluídos todos os custos, diretos e indiretos, impostos, taxas e outras despesas eventuais, para perfeita execução do objeto licitado e o atendimento de todas as fases de execução.

O valor total para prestação dos serviços descritos é de R\$......(.....).

· Pela presente, declaramos inteira submissão aos preceitos legais em vigor, especialmente da Lei 14.133/2021, com as alterações posteriores e as cláusulas e condições constantes deste Edital e seus anexos.

· Propomos ao Conselho Federal de Farmácia, prestar o serviço objeto desta licitação obedecendo às estipulações constantes no correspondente Pregão e asseverando que observaremos, integralmente, as normas existentes e aplicáveis quanto ao fornecimento do objeto desta licitação.

· O prazo de validade desta proposta é de 60 (sessenta) dias

Local e data.

(Nome e assinatura do representante legal)



Documento assinado eletronicamente por **Esteban Ariel Iraola, Programador**, em 30/04/2026, às 14:42, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Glauber Santos Ribeiro, Analista de Sistemas**, em 30/04/2026, às 14:43, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Luiz Carlos Viglongo Correa, Coordenador Executivo**, em 30/04/2026, às 17:38, conforme horário oficial de Brasília, com fundamento no art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade do documento pode ser conferida clicando [aqui](#) informando o código verificador **1139115** e o código CRC **B712491C**.