EMATER-DF – Empresa de Assistência Técnica e Extensão Rural do Distrito Federal

TERMO DE REFERÊNCIA EMATER-DF	
Processo 072.000.131/2017	
NATUREZA DA DESPESA	**33.90.39 – Outros Serviços de Terceiros – Pessoa Jurídica**
	44.90.52 – Equipamentos e Material Permanente
	44.90.39 – Outros Serviços de Terceiros – Pessoa Jurídica

1. DO OBJETO:

1.1. Aquisição de equipamentos de FIREWALL para prover maior segurança ao ambiente de rede da Emater-DF.

2. DA JUSTIFICATIVA:

2.1. Atualmente, a EMATER-DF conta com link de internet exclusivo da SUTIC/SEPLAG, apesar de possuirmos um ambiente com certa proteção, devido à recursos de segurança lógica dos servidores e do AD *(active directory*), a GETIN considera a segurança e auditoria insuficiente. Além da segurança, o firewall vai permitir a utilização de mais de uma rede como redundância, ADSL e GDFNET ou GDFNET e Link Dedicado, com isso, a disponibilidade de internet e a possibilidade de implementação de tunelamento VPN resultará na melhoria dos serviços e segurança da informação.

3. DAS ESPECIFICAÇÕES MÍNIMAS DO OBJETO:

3.1 Requisitos técnicos relacionados à solução:

3.1.1 A solução deve consistir de appliance de proteção de rede com funcionalidades de Next Generation Firewall (NGFW), e console de gerência e monitoração;

3.1.2 Por funcionalidades de NGFW entende-se: reconhecimento e controle granular de aplicações web 2.0, prevenção de ameaças, identificação de usuários e controle granular de permissões;

3.1.3 Todas as funcionalidades descritas no item 3.1.2 devem funcionar em um único appliance sem a necessidade de composição de mais produtos;

3.1.4 Não serão aceitas soluções personalizadas, diferentes das oferecidas pelo fabricante para o mercado;

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

3.1.6 O software deverá ser fornecido em sua versão mais atualizada do fabricante;

3.1.7 O sistema operacional da solução deverá ser customizado pelo próprio fabricante do firewall para garantir segurança e melhor performance ao firewall, permitindo o monitoramento de recursos no appliance;

3.1.8 Tanto os gateways de segurança como a gerência centralizada, deverão suportar monitoramento através do protocolo SNMP v1, v2 e v3;

3.1.9 Tanto os gateways de segurança como a gerência centralizada, deverão suportar a sincronização de horário através do protocolo NTP v1, v2, v3 e v4;

3.1.10 Os equipamentos a serem fornecidos devem ser próprios para montagem em rack 19”, incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

3.2 Requisitos técnicos da política de Firewall

3.2.1 A solução de segurança deve usar Stateful Inspection com base na análise granular de comunicação e de estado do aplicativo para monitorar e controlar o fluxo de rede;

3.2.2 Deve suportar a definição de VLAN no firewall conforme padrão IEEE 802.1q e ser possível criar, no mínimo, 1024 (mil e vinte e quatro) subinterfaces lógicas associadas a VLANs e estabelecer regras de filtragem (Stateful Firewall) entre elas;

3.2.3 A comunicação entre a solução de gerencia e os appliances de segurança, deverá ser criptografada, sendo que a comunicação entre eles deve ser autenticada através de uma estrutura de certificado digital;

3.2.4 Deve ser possível suportar arquitetura de armazenamento de logs através de redundância, permitindo a configuração de equipamentos distintos;

3.2.5 A solução deve permitir que em caso de falha da comunicação entre o appliance de segurança e a solução de armazenamento de logs seja possível a retenção temporária local no appliance de segurança;

3.2.6 As regras deverão ser consistidas de objetos de rede baseadas no protocolo TCP/IP. Durante a criação da regra, tais objetos deverão ser associados automaticamente às suas interfaces de rede correspondentes, sem que haja necessidade de o administrador associar, na regra, qual é a interface de rede ou zona de segurança, de origem da conexão, nem a interface de rede de destino da conexão;

3.2.7 Deverá possibilitar a implementação de balanceamento de links em modos de ativo/ativo ou ativo/standby;

3.2.8 A funcionalidade de balanceamento de links deve suportar a implementação de monitoração de links Internets, através de teste de conectividade com endereços específicos e implementar alertas em caso de indisponibilidades;

3.2.9 Após uma queda da conexão primária, quando essa retornar deve ser possível configurar ações a serem executadas, suportando, no mínimo, alertas SNMP (trap SNMP), log e scripts customizados pelo usuário;

3.2.10 Deve autenticar sessões para qualquer protocolo ou aplicação baseada em TCP/UDP/ICMP;

3.2.11 A solução deve suportar os seguintes esquemas de autenticação nos módulos de Firewall e VPN: Tokens (como SecurID), TACACS, RADIUS e certificados digitais;

3.2.12 Deve oferecer as funcionalidades de backup/restore e deve permitir ao administrador agendar backups da configuração em determinado dia e hora;

3.2.13 Em caso de falhas nas rotas primárias deve desviar dinamicamente o tráfego para um link secundário (roteamento com base em prioridades);

3.2.14 Deve suportar VLAN Tags padrão 802.1q;

3.2.15 Deve implementar roteamento multicast;

3.2.16 Possuir funcionalidade de DHCP Relay e DHCP Server;

3.2.17 Deve suportar os seguintes tipos de NAT:

3.2.17.1 Nat dinâmico (Many-to-1);

3.2.17.2 Nat dinâmico (Many-to-Many);

3.2.17.3 Nat estático (1-to-1);

3.2.17.4 NAT estático (Many-to-Many);

3.2.17.5 Nat estático bidirecional 1-to-1;

3.2.17.6 NAT de Origem;

3.2.17.7 NAT de Destino;

3.2.18 Prover mecanismo de proteção para ataques de falsificação de endereços (IP Spoofing) através da especificação da interface de rede pela qual uma comunicação deve se originar;

3.2.19 A solução deve suportar IPv6, assim como criação de regras simultânea de regras IPv4 e Ipv6;

3.2.20 Deve implementar roteamento estático IPv4 e IPV6;

3.2.21 Deve implementar roteamento dinâmico (RIP, BGP e OSPF) para IPv4;

3.2.22 Deve implementar roteamento dinâmico (OSPFv3) para IPv6;

3.2.23 Deve implementar roteamento por origem, por destino ou por serviço (PBR - Policy Based Routing);

3.2.24 Deve suportar no mínimo as seguintes funcionalidades em IPv6: Address auto configuration (DHCP), NAT64, Identificação de usuários a partir do LDAP/AD, Captive Portal, IPv6 over IPv4 IPSec, De-criptografia SSL, PBF (Policy Based Forwarding), QoS, DHCPv6 Relay, Ativo/Ativo, Ativo/Passivo, SNMP, NTP, SYSLOG, DNS e controle de aplicação;

3.2.25 Deve ter a capacidade de inspecionar e bloquear tráfego operando nos seguintes modos: camada 2 (l2) e camada 3 (l3);

3.2.26 Deve inspecionar e bloquear os dados em linha e controle do tráfego em nível de aplicações;

3.2.27 Deve inspecionar e bloquear os dados operando como default gateway das redes protegidas e controlar o tráfego em nível de aplicações;

3.2.28 Deve permitir a verificação de regras por intervalo de tempo e/ou período (data e horário de início e fim de validade);

3.2.29 Na ocorrência de falhas, as conexões existentes em um firewall deverão ser mantidas pelo(s) outro(s) sem perdas destas conexões, não acarretando interrupções no tráfego da rede e nem redução de desempenho da solução;

3.2.30 Na aplicação de regras as conexões existentes deverão ser mantidas sem perda das conexões ativas;

3.2.31 Promover a integração com diretórios LDAP (X.500) e Active Directory para a autenticação de usuários, de modo que o Firewall possa utilizar das informações armazenadas para realizar autenticações;

3.2.32 Para configuração e administração do Firewall deve possibilitar o acesso via CLI (SSH), console do fabricante e interface Web HTTPS;

3.2.33 A solução de Firewall, deve ser capaz de apresentar contagem/percentual de utilização de regra de acordo com a utilização;

3.2.34 Deve estar licenciado e habilitado para uso ilimitado de usuários e endereços de rede de acordo com as funcionalidades deste documento.

3.2.35 Não serão aceitas soluções nas quais as interfaces de origem e destino tenham que ser obrigatoriamente explicitadas na configuração das regras;

3.2.36 Toda alteração de políticas e definições na console de gerenciamento deverá ser registrada e passível de auditoria;

3.2.37 Deverá permitir a ativação/desativação de regras de forma programada conforme a data/hora;

3.2.38 Deverá suportar métodos de autenticação de usuário, cliente e sessão;

3.2.39 A solução deve suportar, no mínimo, 20.000 (vinte mil) entradas na tabela ARP;

3.2.40 A solução de Firewall deve suportar, no mínimo, 5.000 (cinco mil) regras;

3.2.41 Possibilitar o bloqueio da interface para alterações, evitando o conflito de configurações entre administradores quando tiver mais de um administrador executando alterações simultaneamente;

3.2.42 A solução deve suportar realizar upgrade via SCP ou https via interface WEB;

3.2.43 O appliance de segurança deve possuir 01 (um) slot modular, permitindo inclusão ou remoção de interfaces;

3.2.44 A Solução ofertada deverá possuir uma única interface para gerenciamento de regras para IPv4 e IPv6.

3.2.45 A solução deverá possuir aceleração de regras de firewall implementado através de software para aumentar a performance da análise das regras de firewall.

3.3 Requisitos técnicos de alta disponibilidade

3.3.1 Suporte a configuração de alta disponibilidade Ativo/StandBy e Ativo/Ativo:

3.3.1.1 Em modo Transparente:

3.3.1.2 Em Layer 2

3.3.1.3 Em Layer 3

3.3.2 O cluster deve sincronizar:

3.3.2.1 Todas as sessões;

3.3.2.2 Certificados de-criptografados;

3.3.2.3 Todas Associações de Segurança das VPNs;

3.3.2.4 Todas as assinaturas de Antivírus, Antispyware, Aplicações Web 2.0 e IPS;

3.3.2.5Todas as configurações;

3.3.3 O cluster deverá realizar monitoração de interfaces de rede e processos críticos, de forma a garantir que somente máquinas integras continuem no cluster;

3.3.4 Para melhor desempenho ou em caso de crescimento da rede, a solução deve suportar mais de dois membros no cluster de Firewall;

3.3.5 A solução deve suportar agregação de interfaces (link aggregation), suportando os protocolos 802.3ad e XOR para escolhas entre aumento de throughput e alta disponibilidade de interfaces;

3.4 Requisitos técnicos de VPN

3.4.1 A solução deve suportar CA Interna e CA Externa de terceiros;

3.4.2 Deve incluir a capacidade de confiar em CAs externas ilimitadas com a opção de verificar o certificado de cada gateway externo através de, no mínimo, DN e IP;

3.4.3 Solução deve suportar 3DES e AES-256 de criptografia para IKE Fase I e II IKEv2 plus "Suite-B-MCG-128" e "Suite-B-GCM-256" para a fase II;

3.4.4 Solução deve suportar pelo menos os seguintes grupos Diffie-Hellman: Grupo 1 (768 bits), Grupo 2 (1024 bits), Grupo 5 (1536 bits), Grupo 14 (2048 bits), Grupo 19 e Grupo 20;

3.4.5 Solução deve suportar a integridade dos dados com md5, sha1 SHA-256 ou sha1 SHA-192, SHA-384 e AES-XCBC;

3.4.6 Solução deve suportar a configuração VPN através de uma interface do tipo GUI (console do fabricante ou interface web);

3.4.7 A Solução deve suportar clientless VPNs SSL para acesso remoto;

3.4.8 A Solução deve suportar VPNs L2TP, incluindo suporte para iPhone, Windows Phone, Android com suporte a cliente L2TP;

3.4.9 Solução deve suportar VPNs baseadas em redes e VPNs através de rotas com suporte a protocolos de roteamento dinâmico;

3.4.10 Solução deve incluir a capacidade de estabelecer VPNs com gateways com IPs públicos dinâmicos;

3.4.11 Solução deve incluir compressão IP para cliente-to-site e VPN site-to-site;

3.4.12 Suportar IPSec VPN:

3.4.12.1 3DES, AES;

3.4.12.2 Autenticação MD5 e SHA-1;

3.4.12.3 Algoritmo Internet Key Exchange (IKE);

3.4.12.4 AES 128 ou 192, e 256 (Advanced Encryption Standard);

3.5 Requisitos técnicos de controle de aplicações web 2.0

3.5.1 A solução deverá contar com ferramentas de visibilidade e controle de aplicações WEB integrada no próprio appliance de segurança que permite a criação de políticas de liberação ou bloqueio baseando-se em aplicações WEB 2.0;

3.5.2 A solução deve ser capaz de identificar qualquer tipo de aplicação Web 2.0 em camada 7 (sete) independente de porta e protocolo;

3.5.3 Possuir reconhecimento de, no mínimo, 6.500 (seis mil e quinhentas) aplicações diferentes, incluindo categorização para tráfego relacionado a aplicações peer-to-peer, redes sociais, acesso remoto, atualização de software, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

3.5.4 Possuir controle de regras de aplicações, grupos de aplicações, categorias de aplicações, social widgets com controle granular para usuários ou grupos de usuários;

3.5.5 A fim de otimização de tempo operacional dos administradores, a solução deverá possuir pelo menos 150 (cento e cinquenta) categorias de aplicações WEB pré-definidas pelo fabricante;

3.5.6 Deve possibilitar a inspeção de tráfego HTTPS (Inbound/Outbund);

3.5.7 Deve possibilitar não apenas o bloqueio das aplicações, mas também de portas e protocolos. Deve ainda distinguir protocolos de aplicações, por exemplo o protocolo GRE não deve ser tratado como aplicação na política.

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

3.5.9 Deve inspecionar o payload de pacote de dados com o objetivo de detectar através de expressões regulares assinaturas de aplicações conhecidas pelo fabricante, independente de porta e protocolo. A checagem de assinaturas também deve

determinar se uma aplicação está utilizando a porta padrão ou não, incluindo, mas não limitado a: RDP na porta 80 ao invés de 3389;

3.5.10 Deve possibilitar a permissão ou bloqueio de aplicações por pelos seguintes critérios:

3.5.10.1 Aplicação da Web;

3.5.10.2 Categorias;

3.5.10.3 Nível de risco;

3.5.10.4 IP/Range de IP's/Redes;

3.5.10.5 Usuários do AD/LDAP;

3.5.10.6 Diferentes grupos de usuários;

3.5.10.7 Aplicações que sejam passiveis a técnicas de evasão por malwares e uso excessivo de banda como (ultrasurf, torrent, dropbox e file sharing);

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

3.5.12 Deve atualizar a base de assinaturas de aplicações automaticamente sem a necessidade de reboot nos gateways e gerencia;

3.5.13 Devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;

3.5.14 Deve suportar o controle de aplicações conhecidas e possibilitar a inclusão de aplicações desconhecidas. Sendo possível executar esta tarefa através da interface de gerência GUI ou WEB, ou, através de ticket direto com o fabricante;

3.5.15 Deve possibilitar a customização, por regra, da tela de interação com o usuário, permitindo: informar, questionar e limitar a banda de acesso;

3.5.16 Deve permitir diferentes "telas" de interação com o usuário para equipamentos móveis;

3.5.17 Deve possibilitar a diferenciação e controle de partes das aplicações, como por exemplo, bloquear o Gtalk chat e permitir o acesso ao Gmail;

3.5.18 Deve permitir o bloqueio total de aplicações Proxies (ex.: Ultrasurf, GPass, FreeGate, Hopster, Tor, HotSpot Shield, etc);

3.5.19 "Deve possibilitar a integração da solução com base do Active Directory, LDAP, RADIUS ou base local para criação de políticas. Possibilitando a criação de regras utilizando:

3.5.19.1 Usuários

3.5.19.2 Grupo de usuários;

3.5.19.3 Máquinas (estações de trabalho);

3.5.19.4 Endereço IP;

3.5.19.5 Endereço de Rede;

3.5.19.6 Combinação das opções acima.

3.5.20 A solução deve suportar a criação de, no mínimo, 500 (quinhentas) regras de controle de aplicações no mesmo dispositivo de segurança, permitindo o controle granular de qualquer tipo de acesso não permitido pelo órgão;

3.5.21 Possuir controle granular para quais funcionalidades de proteção, endereços IPs será executada a inspeção e de-criptografia de SSL tanto para tráfego de entrada (inbound), quanto para tráfego de saída (outbound). É obrigatório que seja possível desligar a inspeção para sites de bancos baseados em categorização automática executada pelo Fabricante;

3.5.22 A Solução deve possuir um mecanismo configurável de bypass onde o administrador consegue definir grupos específicos de usuários que estão autorizados a ignorar as regras de controle de aplicações para um período de tempo específico;

3.5.23 Deve permitir a verificação de regras por intervalo de tempo e/ou período (data e horário de início e fim de validade);

3.5.24 Deve possibilitar a customização por regra utilização as seguintes ações de controle:

3.5.24.1 Permitir;

3.5.24.2 Bloquear;

3.5.24.3 Monitorar;

3.5.24.4 Informar o usuário;

3.5.24.5 Interagir com o usuário para decisão da ação (permitir/bloquear) possibilitando que o usuário utilize uma justificativa para tal utilização, sendo que a justificativa poderá ser analisada posteriormente através do log;

3.5.25 A solução deverá garantir a performance indicada neste projeto caso sejam habilitadas as funcionalidades aqui descritas;

3.5.26 A solução de ser capaz de identificar qualquer tipo de aplicação Web em camada 7, independente de porta e protocolo;

3.5.27 O mecanismo de controle de aplicação web deve possuir contagem de utilização de regra;

3.6 Requisitos técnicos de controle de URL

3.6.1 Para prover maior visibilidade e controle dos acessos dos usuários do ambiente, deve ser incluído um módulo de filtro de URL integrado no firewall;

3.6.2 A solução deve ter um mecanismo configurável de by-pass, onde o administrador consegue definir grupos específicos de usuários que estão autorizados a ignorar as regras de filtragem de URL para um período de tempo específico;

3.6.3 A solução deve permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

3.6.4 A solução deve suportar a criação de políticas por usuários e/ou grupos de usuários cadastradas no Active Directory/LDAP, endereço IP, endereço de rede, e grupos de redes;

3.6.5 A solução deve fornecer um mecanismo para solicitação de categorização de URL caso esta não esteja categorizada ou categorizada incorretamente;

3.6.6 A solução de filtro de URL deverá ser totalmente integrada com a solução de controle de aplicações WEB 2.0 para melhor gerenciamento;

3.6.7 A solução deve suportar a criação de, no mínimo, 500 (quinhentas) regras de controle de URL no mesmo dispositivo de segurança, permitindo o controle granular de qualquer tipo de acesso não permitido pelo órgão;

3.6.8 Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

3.6.9 A solução deve possuir engine de bloqueio de conteúdo em sites de busca como (Google, Bing e Yahoo). Assim como o bloqueio de sites que estão em modo cache.

3.6.10 Deve possibilitar a customização por regra utilização as seguintes ações de controle:

3.6.10.1 Permitir;

3.6.10.2 Bloquear;

3.6.10.3 Monitorar;

3.6.10.4 Informar o usuário;

3.6.10.5 Interagir com o usuário para decisão da ação (permitir/bloquear) possibilitando que o usuário utilize uma justificativa para tal utilização, sendo que esta justificativa poderá ser analisada posteriormente através dos logs;

3.6.11 Deve possibilitar base de URLs local no Appliance, evitando delay de comunicação/validação da URLs;

3.6.12 Deverá possuir, no mínimo, 90 (noventa) categorias de URLs;

3.6.13 Deverá possibilitar a criação de categorias de URLs customizadas;

3.6.14 Deverá possibilitar a exclusão de URLs do bloqueio por categoria;

3.6.15 Deve possibilitar a customização de página de bloqueio de interação com usuário;

3.6.16 Os logs do produto devem incluir informações das atividades dos usuários.

3.7 Requisitos técnicos de identificação de usuários

3.7.1 Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações e/ou URL's através da integração com serviços de diretório, Active Directory, LDAP e Radius;

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

3.7.3 A identificação do usuário registrado no Microsoft Active Directory, deverá ocorrer sem qualquer tipo de agente instalado nos controladores de domínio e estações dos usuários;

3.7.4 Para usuários não registrados ou não reconhecidos no domínio, a solução deve ser capaz de fornecer uma autenticação baseada em navegador (Captive Portal), sem a necessidade de agente;

3.7.5 Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular;

3.7.6 A solução deverá ser capaz de identificar nome do usuário, login, maquina/computador registrados no Microsoft Active Directory;

3.7.7 Deve suportar autenticação para Smartphone e tablet's;

3.7.8 Deve suportar autenticação Kerberos transparente para single sign on;

3.7.9 A solução deverá compartilhar a identificação de usuários com outros gateways de segurança do mesmo fabricante;

3.7.10 Na integração com o AD, todos os controladores de domínio em operação na rede do cliente devem ser cadastrados de maneira simples e sem utilização de scritps de comando;

3.7.11 A solução de identificação de usuários deverá se integrar com as funcionalidades Firewall, controle de aplicação web 2.0, controle de URL, antivírus e DLP, sendo estas do mesmo fabricante;

3.7.12 Não serão aceitas soluções de identificação de usuários onde a configuração do Captive Portal exige a especificação de 01 (um) processador específico, pois tal configuração ocasionará perda de performance ou até mesmo indisponibilidade da autenticação devido a manipulação errada da rajada de usuários;

3.7.13 A solução deve suportar a opção de instalação de softwares agentes nos PCs/laptops para que os próprios PCs/laptops enviem suas credenciais de IP/nome de usuário do domínio/nome da máquina para o gateway diretamente, evitando consultas do gateway aos controladores de domínio.

3.8 Requisitos técnicos de prevenção de ameaças

3.8.1 O dispositivo de proteção deve possuir módulo de IPS integrado no próprio appliance de firewall sem a necessidade de uso de quaisquer interfaces externas, onde sua console de gerencia deverá residir na mesma console centralizada dos appliances de segurança;

3.8.2 A solução de IPS deve fazer a inspeção de toda sessão, independentemente do tamanho, sem degradar a performance do equipamento solicitado neste termo;

3.8.3 A solução de IPS deve fazer a inspeção de todo o trafego de forma bi-direcional, analisando qualquer tamanho de pacote sem degradar a performance do equipamento solicitada neste termo;

3.8.4 O mecanismo de inspeção deve receber e implementar em tempo real atualizações para os ataques emergentes sem a necessidade de reiniciar o appliance;

3.8.5 Em cada proteção de segurança, deve estar incluso informações como: código CVE, tipo de impacto na ferramenta, severidade, e tipo de ação que a mesma irá executar;

3.8.6 A solução deve fazer captura de pacotes para proteções específicas;

3.8.7 Deve incluir a habilidade de detectar e bloquear ataques conhecidos, protegendo pelo menos, os seguintes ataques conhecidos: SQL Injection, ICMP Denial of Service, Non Compliant SSL, IKE aggressive Exchange;

3.8.8 Deve ser capaz de bloquear tráfego SSH enviados em portas não permitidas, como por exemplo, 443.

3.8.9 A solução de IPS deve incluir um modo de solução de problemas, que define o uso de perfil de detectar, sem modificar as proteções individuais já criadas e customizadas;

3.8.10 A ferramenta de log deve possuir a capacidade onde em apenas um clique o administrador possa criar uma regra de exceção a partir do log visualizado na gerencia centralizada, sem precisar fazer qualquer tipo de query ou analise avançada;

3.8.11 A solução deve ser capaz de inspecionar tráfego HTTPS (inbound/outbound);

3.8.12 Proteger o ambiente contra ataques de negação de serviços – DoS;

3.8.13 Disponibilizar relatório gráfico do percentual de eventos por CVE (Common Vulnerabilities and Exposures);

3.8.14 Baseado nas melhores práticas se segurança e otimização de tempo operacional dos administradores, a solução de IPS integrada no appliance de segurança, deve possuir uma base de assinaturas de segurança não inferior a 5000 (cinco mil) assinaturas;

3.8.15 Na própria interface de gerencia, a solução de IPS deve possuir índices por período (hora, semana ou mês) onde aponta o nível de ação das assinaturas baseada pela sua severidade;

3.8.16 O gerenciamento centralizado via interface gráfica deve possibilitar a configuração de captura dos pacotes por regra individualmente visando otimizar a performance do equipamento;

3.8.17 Na própria interface de gerencia, a solução de IPS deverá apresentar sumario de todos os appliances que estão sendo gerenciados que possuem a solução de IPS ativa e qual o tipo de perfil assinalado de forma individual, bem como notificação se alguns dos appliances estão em alto consumo de processamento;

3.8.18 Para melhor administração da solução, a solução deve permitir incorporar de forma automática novas proteções de IPS através de sua severidade, nível de confiança da proteção e através do impacto da performance;

3.8.19 O modulo de IPS deve possuir assinaturas voltadas para ambientes de servidores de mail, Web e DNS, onde os mesmo poderão ser assinalados no momento da criação do objeto de rede na solução;

3.8.20 Deverá possibilitar a inclusão de novas assinaturas e customização no formato SNORT;

3.8.21 O mecanismo de inspeção deve receber e implementar em tempo real atualizações de novas assinaturas sem a necessidade de reiniciar o appliance;

3.8.22 Para cada proteção, ou para todas as proteções suportadas, deve incluir a opção de adicionar exceções baseado na fonte, destino, serviço ou qualquer combinação dos três;

3.8.23 A solução deve ser capaz de detectar e bloquear ataques nas camadas de rede e aplicação, protegendo pelo menos os seguintes serviços: Aplicações web, serviços de e-mail, DNS, FTP, serviços Windows (Microsoft Networking) e VoIP;

3.8.24 O administrador deve ser capaz de configurar quais comandos FTP são aceitos e quais são bloqueados a partir de comandos FTP pré-definidos;

3.8.25 A solução deve permitir que o administrador possa configurar quais métodos e comandos HTTP são permitidos e quais são bloqueados.

3.8.26 Deve incluir proteção contra vírus em conteúdo ActiveX e applets Java e worms;

3.8.27 A solução deve permitir a pré-configuração de, no mínimo, 15 perfis de proteção de IPS que podem ser utilizados a qualquer momento.

3.8.28 Deve incluir uma tela de visualização situacional a fim de monitorar graficamente a quantidade de alertas de diferentes severidades em diversas áreas de interesse do administrador e a evolução no tempo. As diferentes áreas de interesse devem ser definidas usando filtros customizáveis para selecionar alertas baseados em qualquer propriedade ou combinação de propriedades do mesmo, incluindo pelo menos: origem, destino, serviço, tipo e nome do alerta.

3.8.29 A solução deve permitir a configuração de inspeção do IPS baseado em políticas que utilizem o posicionamento geográfico de origens ou destinos e combinações entre os dois;

3.8.30 A solução que permite a configuração de políticas baseada em países, deve possuir, no mínimo, 200 (duzentos) países já cadastrados em sua base;

3.8.31 A solução deve possuir os seguintes esquemas de atualização de assinaturas:

3.8.31.1 Atualização instantânea, através de um click;

3.8.31.2 Atualização através de agendamento onde engloba horário, dias da semana ou dia do mês;

3.8.31.3 Atualização em mode offline, onde poder ser baixado na base do fabricante e posteriormente fazer o upload do arquivo na solução;

3.8.32 A solução deve suportar a atualização da base de assinaturas, e suportar se as novas assinaturas serão ativadas automaticamente ou não;

3.8.33 A solução de IPS deve ser capaz de criar um acompanhamento das assinaturas da base local onde o administrador pode assinalar as assinaturas para analise futura. Com isso é possível tomar decisões de criação de exceção, rastrear registros e mudar sua forma de atuação;

3.8.34 A solução deve suportar importar certificados de servidor para inspeções de tráfego HTTP de entrada. Depois de importar esses certificados, a solução deve permitir o uso desses certificados na configuração de regra de IPS para Inspeção HTTPS;

3.8.35 A solução deve possuir inspeção de trafego HTTPS sendo possível criar by-pass para determinados sites evitando qualquer tipo de quebra de sigilo de informações pessoais;

3.8.36 A engine de inspeção HTTPS da solução deve permitir a criação de diferentes regras onde será especificado origem, destino, tipo de serviço, ação e certificado que será utilizado por regra;

3.9 Requisitos técnicos de antimalware

3.9.1 Visando a proteção do ambiente contra malwares, devem ser incluídos módulos de antivírus e antibot integrados no próprio appliance de segurança;

3.9.2 A solução deve possuir nuvem de inteligência proprietária do fabricante, responsável por atualizar toda a base de assinaturas dos appliances;

3.9.3 Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

3.9.4 Implementar funcionalidade de detecção e bloqueio de callbacks (comunicação do malware com o servidor de comando e controle);

3.9.5 Implementar atualização da base de assinaturas de forma automática, suportando, no mínimo, os seguintes intervalos:

3.9.5.1 Diária;

3.9.5.2 Dias da semana;

3.9.5.3 Dias do mês;

3.9.5.4 Intervalo de atualização (por exemplo: a cada 1 hora);

3.9.6 A solução de analisar e bloquear malware e/ou codigos maliciosos pelo menos os seguintes tipos de arquivos:

3.9.6.1 Bat;

3.9.6.2 Com;

3.9.6.3 Exe;

3.9.6.4 Dll;

3.9.6.5 Vsd;

3.9.6.6 Reg;

3.9.6.7 Jar;

3.9.6.8 Txt;

3.9.6.9 Swf;

3.9.6.10 Cmd;

3.9.6.11 Mpg;

3.9.6.12 Jse;

3.9.6.13 Midi;

3.9.6.14 Mp3;

3.9.6.15 Hlp;

3.9.6.16 Php;

3.9.6.17 Png;

3.9.6.18 Tif;

3.9.6.19 Wav;

3.9.6.20 Asf;

3.9.6.21 Htm;

3.9.6.22 Com;

3.9.6.23 Jpeg;

3.9.7 Possuir antivírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP e CIFS;

3.9.8 A solução de antivírus deve permitir o bloqueio de download de arquivos que excedam o tamanho pré-definido;

3.9.9 A solução deve atuar na prevenção de forma granular através de políticas por usuário / máquina ou Rede, sendo possível escolher um perfil diferente para cada regra;

3.9.10 A solução deve permitir criar regras de exceção de acordo com a proteção a partir do log visualizado na interface gráfica da gerencia centralizada;

3.9.11 A solução de inspeção de vírus não deverá possuir limitação para o tamanho dos arquivos inspecionados (a limitação é baseada na quantidade de memória/Disco), sendo ela capaz de customizar o tamanho do arquivo inspecionado, assim como a ação caso o tamanho seja excedido;

3.9.12 Implementar através da interface gráfica mecanismo de painel de controle onde seja possível a visualização de no mínimo as seguintes informações: sumário de

detecção e proteção, gráfico de top infecções, e gráfico da taxa de transferência de tráfego monitorado;

3.9.13 Implementar através da interface gráfica de administração, configuração de mecanismo de alerta onde seja possível configurar bloqueio/desbloqueio de uma comunicação do tipo callback;

3.9.14 Implementar geração de relatórios através da interface gráfica onde contenha, no mínimo, as seguintes informações, com recursos de navegação para baixo entre níveis (drill-down): tipo de malware, id de evento, extensão do arquivo inspecionado, severidade da ameaça, horário do último evento, IP de origem, IP de destino e nome do usuário infectado de acordo a base do Active Directory;

3.9.15 Implementar mecanismo de pesquisa por diferentes intervalos de tempo;

3.9.16 Implementar através da interface gráfica, pesquisa aos eventos já reconhecidos;

3.9.17 A solução de relatório deve apresentar via interface gráfica as seguintes informações no relatório:

3.9.17.1 Sumário executivo;

3.9.17.2 Relatório de servidores de callback;

3.9.17.3 Relatório de hosts infectados;

3.9.17.4 Atividade de malware e detalhes dos alertas.

3.9.18 A solução deve ser capaz de bloquear uma conexão até que a classificação da mesma seja completada;

3.9.19 Implementar através da interface gráfica, a criação de filtros para apresentação dos alertas visualizados;

3.9.20 A solução deve possuir na própria interface de gerencia, gráfico contento informações em tempo real sobre as atividades recentes de malwares detectados na solução, sendo que essas informações deverão ser apresentadas em Mapa geográfico por país, através de IP ou URL e principais e-mails que foram inspecionados;

3.9.21 Deve possuir visualização na própria interface de gerenciamento referente aos maiores incidentes através de hosts ou incidentes referentes a incidentes de vírus e bots;

3.9.22 A solução deve permitir de forma anônima compartilhar ou não informações sobre ataques ou arquivos maliciosos para o serviço na nuvem do Fabricante;

3.9.23 A solução deve permitir a criação de whitelist baseado no MD5 do arquivo;

3.9.24 Permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, etc.);

3.9.25 Em caso de falha no mecanismo de inspeção do antivírus, deve ser possível configurar se as conexões serão permitidas ou bloqueadas;

3.10 Requisitos técnicos de prevenção contra ameaças avançadas

3.10.1 A solução deverá prover as funcionalidades de inspeção de tráfego de entrada de malwares não conhecidos ou do tipo APT com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de call-backs;

3.10.2 Suportar os protocolos HTTP, SMTP assim como inspeção de tráfego criptografado através de HTTPS e TLS;

3.10.3 A solução deve ser capaz de inspecionar o tráfego criptografado SSL;

3.10.4 Deve ser possível determinar o tamanho máximo para inspeção de e-mail;

3.10.5 Deve ser possível determinar a quantidade de URL's a serem inspecionadas dentro de e-mail;

3.10.6 A solução deve possuir engine de DNS Trap, através da qual deve identificar hosts infectados tentando acessar o endereço de DNS inválido;

3.10.7 A solução deve identificar existência de malware em arquivos anexos a e-mails e URL´s conhecidas;

3.10.8 Implementar mecanismo de exceção, permitindo a criação de regras por usuário, VLAN, subrede e endereço IP;

3.10.9 A solução deve suportar a criação de exceções de inspeção, baseadas no endereço de e-mail de origem, endereço de e-mail de destino, e combinação do endereço de e-mail de origem e endereço de destino;

3.10.10 Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PFD com, no mínimo, 10 (dez) MB ;

3.10.11 A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, sendo eles:

3.10.11.1 Windows XP e Windows 7 assim como office 2003, 2010 e 2013;

3.10.12 A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas;

3.10.13 Todas as máquinas virtuais utilizadas na solução devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

3.10.14 A solução deve possuir nuvem de inteligência proprietária do fabricante, responsável em atualizar toda a base de segurança dos appliances através de assinaturas;

3.10.15 Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas ou qualquer outro mecanismo de redirecionamento de tráfego;

3.10.16 A solução deve suportar as seguintes topologias de implantação: inline, message transfer agent (MTA) e Mirror/TAP;

3.10.17 Implementar atualização automática da base de dados, suportando, no mínimo, agendamento diário, agendamento em determinados dias da semana, agendamento em determinados dias do mês;

3.10.18 A solução deve apresentar informações comportamental incluindo listagem de módulos e processos utilizados pelo malware e/ou código malicioso;

3.10.19 Toda análise deverá ser realizada na nuvem do fabricante;

3.10.20 Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

3.10.21 Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Sendo que essa ação deve ser realizada em um tempo inferior a 10 minutos e o bloqueio deve ser imediato, não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

3.10.22 Implementar a emulação, detecção e bloqueio de forma imediata não superior a 10 minutos de qualquer malware e/ou código malicioso detectado. A solução deve suportar, no mínimo, os seguintes tipos de arquivo: PDF, TAR, ZIP, RAR, 7Z, EXE RTF, CSV, SCR, XLS, XLSX, XLT, XLM, XLTX, XLSM, XLTM, XLSB, XLA, XLAM, XLL, XLW, PPT, PPTX, PPS, PPTM, POTX, POTM, PPAM, PPSX, PPSM, SLDX, SLDM, DOC, DOCX, DOT, DOCM, DOTX, DOTM, BAT, COM, EXE, DLL, VSD,

REG, JAR, TXT, SWF, CMD, MPG, JSE, MIDI, MP3, HLP, PHP, PNG, TIF, WAV, ASF, HTM, COM, JPEG;

3.10.23 A solução deve permitir criar regras de exceção de acordo com a proteção a partir do log visualizado na interface gráfica da gerencia centralizada;

3.10.24 Implementar através da interface gráfica mecanismo de painel de controle onde seja possível a visualização de no mínimo as seguintes informações: sumário de detecção e proteção, gráfico de top infecções, e gráfico do taxa de transferência de tráfego monitorado;

3.10.25 Implementar geração de relatórios através da interface gráfica onde contenha no mínimo as seguintes informações, com recursos de navegação para baixo entre níveis (drill-down): tipo de malware, id de evento, extensão do arquivo inspecionado, severidade da ameaça, horário do último evento, IP de origem, IP de destino e nome do usuário infectado de acordo a base do Active Directory;

3.10.26 Possuir mecanismo de pesquisa por diferentes intervalos de tempo;

3.10.27 Implementar através da interface gráfica, pesquisa aos eventos já reconhecidos;

3.10.28 A solução de relatório deve apresentar via interface gráfica as seguintes informações no relatório:

3.10.28.1 Sumário executivo;

3.10.28.2 Relatório de servidores de callback;

3.10.28.3 Relatório de hosts infectados;

3.10.28.4 Atividade de malware e detalhes dos Alertas.

3.10.29 A solução deve ser capaz de interromper uma conexão até que a classificação da mesma seja completada;

3.10.30 Implementar através da interface gráfica, a criação de filtros para apresentação dos alertas visualizados;

3.10.31 A solução deve possuir na própria interface de gerencia, gráfico contento informações em tempo real sobre as atividades recentes de malwares detectados na solução, sendo que essas informações deverão ser apresentadas em mapa geográfico por país, através de IP ou URL e principais e-mails que foram inspecionados;

3.10.32 A solução deve permitir a criação de whitelist baseada no MD5 do arquivo;

3.10.33 A solução deve possuir recurso de restrição de localização, permitindo que as emulações na nuvem sejam restritas ao tráfego de um país específico;

3.10.34 Para melhor administração da solução, a solução deve possibilitar as seguintes informações de monitoração:

3.10.34.1 Quantidade de maquinas virtuais que estão atuando;

3.10.34.2 Número de arquivos emulados;

3.10.35 A solução deve ser capaz de fazer atualizações em modo offline;

3.11 Solução de Firewall NGFW tipo appliance para Core da rede do Ed. Sede

3.11.1 Possuir tamanho máximo de 2U por equipamento;

3.11.2 O appliance de segurança, deverá possuir no mínimo, os seguintes throughputs **para condições reais de funcionamento em produção**:

3.11.2.1 05 (cinco) Gbps para a funcionalidade de Firewall;

3.11.2.2 800 (oitocentos) Mbps para a funcionalidade de IPS;

3.11.2.3 1,5 (um e meio) Gbps para a funcionalidade de VPN;

3.11.3 Cada appliance de segurança deve suportar, no mínimo, 3.000.000 (três milhões) de conexões simultâneas;

3.11.4 Cada appliance de segurança deve suportar, no mínimo, 100.000 (cem mil) novas conexões por segundo;

3.11.5 Possuir, no mínimo, 06 (seis) interfaces de rede 10/100/1000 RJ-45;

3.11.6 Possuir, no mínimo, 01 (uma) interface de rede 10/100/1000 RJ-45 dedicada para gerenciamento;

3.11.7 Possuir, no mínimo, 01 (uma) interface de rede 10/100/1000 RJ-45 para alta disponibilidade;

3.11.8 Possuir, no mínimo, 01 (uma) interface do tipo console ou similar;

3.11.9 Possuir disco rígido, no mínimo, 200 (duzentos) GB, com tecnologia SSD ou HDD;

3.12 Solução de Gerenciamento Centralizado

3.12.1 A solução de gerência deverá ser separada dos gateways de segurança onde irá gerenciar políticas de segurança de todos os firewalls e funcionalidades solicitadas neste projeto assim como logs e relatórios de forma unificada;

3.12.2 A solução de gerência poderá ser instalada em appliance dedicado do próprio fabricante, ou servidores de terceiros (Open Server), ou em ambiente virtualizado utilizando ambiente de virtualização VMware;

3.12.3 O hardware deve ser baseado em arquitetura aberta usando processadores Intel ou AMD a fim de manter flexibilidade e adaptação a novas ameaças sem impacto na performance.

3.12.4 A solução deverá permitir seu gerenciamento por: CLI (Command Line Interface) via SSH, WEB GUI utilizando protocolo HTTPS, e console proprietária;

3.12.5 Caso haja a necessidade de instalação de algum software para a administração da solução, o mesmo deve ser compatível com sistemas operacionais Windows ou Linux;

3.12.6 Deve possuir mecanismo de ajuda de comandos via SSH, facilitando a localização e parâmetros dos mesmos;

3.12.7 A solução de gerencia centralizada deverá ser composta por uma única console de gerenciamento, sem a necessidade de consoles adicionais para qualquer tipo de administração e análise de logs dos appliances e funcionalidades solicita neste termo;

3.12.8 Deve permitir a utilização de cores para facilitar a identificação de regras na interface gráfica;

3.12.9 Possibilitar a execução das seguintes tarefas: criação e administração de políticas de firewall e controle de aplicação; criação e administração de políticas de IPS, antivírus e antispyware, criação e administração de políticas de filtro de dados e filtro de URL, monitoração de logs, ferramentas de investigação de logs, debug e captura de pacotes;

3.12.10 Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, antivírus, antimalware) e URLs analisadas pelo firewall;

3.12.11 A solução de gerencia centralizada deverá possuir capacidade de analisar logs e eventos, com intuito de mitigar qualquer anomalia no ambiente, independentemente de o gateway de segurança ser alvo de ataque, causando elevado consumo de CPU e memória;

3.12.12 Possuir autoridade certificadora interna para geração de certificados;

3.12.13 Deve manter um canal de comunicação segura, com encriptação baseada em certificados, entre todos os componentes que fazem parte da solução de firewall, gerência, armazenamento de logs e emissão de relatórios;

3.12.14 A solução deve proporcionar a opção de adicionar alta disponibilidade de gerenciamento centralizado, utilizando um servidor de gerenciamento em standby que é automaticamente sincronizado com o servidor primário;

3.12.15 Deve permitir a definição de perfis de acesso à console de gerenciamento com permissões granulares: acesso de escrita, leitura, criação de usuários e alteração de configurações;

3.12.16 A autenticação dos usuários no console de gerenciamento deve permitir leitura de bases de usuários local ou RADIUS;

3.12.17 Possibilidade de efetuar alteração de política do firewall e aplicá-la posteriormente em horário pré-definidos, assim não impactando o ambiente durante o horario comercial;

3.12.18 A solução deve possuir mecanismo de verificação automática para detecção de erro humano na configuração da política de segurança evitando que regras como "any-any-accept" sejam aplicadas no ambiente, assim como conflito de regras, licença expirada e erro de configuração de interface. É permitido o fornecimento de solução de terceiros para prover esta funcionalidade;

3.12.19 Deve permitir a criação de regras por intervalo de tempo e/ou período (data e horário de início e fim de validade);

3.12.20 Para melhor analise e administração do ambiente de segurança, a solução deve prover em cada regra, a informação da utilização da mesma. Com, no mínimo, as seguintes informações:

3.12.20.1 Visualização do percentual e/ou contagem de utilização em relação a outras regras;

3.12.20.2 Informar a primeira e última vez que a regra foi utilizada, de acordo com a política estabelecida;

3.12.21 A solução deve incluir a opção de segmentar a base de regra utilizando rótulos ou títulos de seção para organizar melhor a política facilitando a localização e gestão do administrador;

3.12.22 A Gerencia deve possuir console de Log onde deve ter a capacidade de visualizar os logs de segurança em tempo real permitindo ao administrador realizar as devidas analises para resolução de problemas;

3.12.23 A solução de armazenamento de logs, deve ser capaz de exportar os logs para uma base de dados ou repositório externo;

3.12.24 A solução de gerencia, deverá prover fácil administração na aplicação das políticas para os gateways, sendo capaz de realizar o processo de alteração de regras e configuração de todas as soluções de segurança em uma única sessão, suportando inclusive alteração de configuração de gateways remotos, evitando qualquer tipo de retrabalho de configuração e aplicação de regra;

3.12.25 A solução deve permitir que em caso de falha da comunicação entre o appliance de segurança e a solução de armazenamento de logs, seja possível a retenção temporária dos logs no appliance de segurança.

3.12.26 A solução deve incluir monitoramento gráfico do status de gateways. A solução de monitoração deve apresentar ao administrador, no mínimo, os seguintes indicadores:

3.12.26.1 Informações de utilização de disco dos gateways gerenciados;

3.12.26.2 Todas as partições de disco e de espaço livre no disco rígido;

3.12.26.3 Informações de utilização de memória dos gateways gerenciados;

3.12.26.4 Informações de utilização de CPU dos gateways gerenciados;

3.12.26.5 Informações de conexões concorrentes e novas conexões dos gateways gerenciados;

3.12.26.6 Alerta quando um membro estiver desconectado do cluster;

3.12.26.7 Alerta de erro do módulo de aceleração de conexões e qualquer falha na perda de roteamento estático;

3.12.26.8 Informações do número de túneis ativos dos gateways gerenciados;

3.12.26.9 Nome da Politica aplicada nos Appliances de segurança;

3.12.26.10 Endereço IP de cada Gateway;

3.12.26.11 Versão do sistema operacional;

3.12.27 A ferramenta de monitoramento deve fornecer informações em tempo real e consolidado através de gráficos pré-configurados;

3.12.28 O sistema deverá ser capaz de criar query para visualização gráfica de consumo por interfaces, sendo mandatório a associação dos principais serviços de rede consumidos através das interfaces;

3.12.29 A solução de monitoração deverá possuir filtro para monitorar somente usuários de VPN ativos;

3.12.30 A solução deverá permitir configurar para cada tipo de regra ou evento pelo menos três das opções: log, alerta, enviar trap SNMP, envio de e-mail, execução de script definido pelo usuário;

3.12.31 Habilidade de realizar upgrade via SCP ou HTTPS via interface WEB;

3.12.32 Suportar rollback de configuração para a última configuração salva;

3.12.33 Solução deve ser capaz de reconhecer falhas e problemas de conectividade entre dois pontos conectados através de uma VPN, e registrar e alertar quando o túnel VPN está desconectado;

3.12.34 A filtragem de logs deve ser intuitiva, ou seja, através de uma palavra chave, sendo suficiente para que um analista com nenhum ou pouco conhecimento sobre a operação da ferramenta possa aplicar filtros utilizando apenas um único parâmetro para a busca. Não sendo aceito solução que precisam de criação de querys customizadas.

3.12.35 A solução dever ser capaz de criar filtro que permita a visualização de múltiplos logs como:

3.12.35.1 Top 10 endereços IP de origem;

3.12.35.2 Top 10 endereços IP de destino;

3.12.35.3 Principais acessos a determinados serviços;

3.12.35.4 Principais ações;

3.12.35.5 Principais funcionalidades de segurança utilizadas do Firewall;

3.12.35.6 Principais regras que foram utilizadas de acordo com o filtro criado;

3.12.35.7 Principais aplicações web utilizada de acordo com as funcionalidades de segurança disponíveis no Firewall;

3.12.36 Com intuído de melhorar a rapidez na pesquisa de eventos e abrangência de período de busca do log, a solução deve possuir logs indexados;

3.12.37 Deve suportar o formato CSV para exportação de relatórios;

3.12.38 Deve possuir logs de auditoria de gerenciamento detalhados, informando a configuração realizada, o administrador responsável pela alteração, a data e o horário da alteração;

3.12.39 A funcionalidade de visualização de logs deverá possibilitar a criação de filtros personalizados usando objetos pré-definidos (IP origem/destino, hosts, usuários, redes, grupos, portas, interfaces, categoria de ataques, entre outras) e funcionalidade de segurança que serão apresentados através de console gráfica para o administrador;

3.12.40 A solução de logs dever ter a capacidade criar múltiplos filtros customizados, sendo possível salvar em favoritos para visualizar em um momento posterior ou através de uma rotina constante;

3.12.41 A solução de logs deverá possibilitar a filtragem de eventos relacionados a ação do administrador. No mínimo: “login" e "logout” por timeout;

3.12.42 A solução de logs deve ser o repositório de logs dos firewalls, disponibilizando pesquisa interativa em qualquer campo destes logs, pelo menos através de termos: qualquer, bloquear, ontem, última hora, últimas 24 horas, última semana, último mês, último ano e questionar ao usuário;

3.12.43 A solução de logs deve permitir pesquisa de logs através de informações do código de protocolo IP e porta de origem;

3.12.44 A solução deve ser capaz de salvar registros gerados através de buscas de pesquisa, fazendo com que se torne simples na utilização futura;

3.12.45 A solução deve ser capaz de criar regras de exceção para assinaturas de IPS a partir do log apresentado na solução;

3.12.46 Para evitar grandes customizações da solução, a console de análise de logs, deve prover filtros pré-definidos de eventos com maior importância;

3.12.47 A solução de logs de gerencia deve suportar discos externos (storage) para aumentar capacidade de armazenamento;

3.12.48 A solução deve possuir licença perpétua, de forma que mesmo após o vencimento do contrato, não impossibilite a inserção de novas políticas e o acesso e alteração de configurações, não havendo necessidade de aquisição posterior de licenças.

3.13 Solução de Correlação de Eventos e Emissão de Relatórios

3.13.1 Deve incluir uma ferramenta do próprio fabricante ou solução de terceiros para correlacionar os eventos de segurança das funcionalidades adquiridas neste edita, sendo ele capaz de receber eventos de soluções mercado;

3.13.2 Deve permitir a criação de filtros com base em qualquer característica do evento, tais como: endereço IP de origem, endereço IP de destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem, país de destino, etc.

3.13.3 Disponibilizar informações gráficas, na linha tempo que informe o número de eventos ocorridos;

3.13.4 Disponibilizar recursos interativos de navegação nos eventos informados;

3.13.5 Disponibilizar relatório gráfico do percentual de eventos por CVE (Common Vulnerabilities and Exposures);

3.13.6 A solução deve exportar relatórios em, no mínimo, dois formatos a seguir: PDF, HTML, CSV e MHT;

3.13.7 A solução deve possibilitar a visualização geográfica dos eventos de segurança correlacionados;

3.13.8 A solução deve ser capaz de atribuir esses filtros para diferentes linhas do gráfico que são atualizadas em intervalos regulares, mostrando todos os eventos que corresponda a esse filtro. Permitindo ao operador a concentrar-se sobre os eventos mais importantes.

3.13.9 A solução deve prover, no mínimo, as seguintes funcionalidades para análise avançada dos incidentes:

3.13.9.1 Visualizar quantidade de tráfego utilizado por aplicações e navegação;

3.13.9.2 Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

3.13.9.3 Estatísticas com comparativo de período (hora, dia e mês);

3.13.10 Deve permitir a geração de relatórios com horários predefinidos, diários, semanais e mensais. Incluindo principais eventos, principais origens, principais destinos, principais serviços, principais origens e os seus principais eventos, principais destinos e seus principais eventos e principais serviços e seus principais eventos;

3.13.11 A solução deve incluir a opção de pesquisar dentro da lista de eventos, em detalhes para a investigação e analise dos eventos;

3.13.12 Deve mostrar a distribuição dos diferentes eventos filtrados por país em um mapa, onde devem estar inclusos os principais eventos por origem ou por destino de cada país;

3.13.13 Deve permitir ao administrador o agrupamento de eventos baseado em quaisquer características, incluindo vários níveis de alinhamento;

3.13.14 A solução de correlação deve possuir mecanismo para detectar login de administradores em horários irregulares;

3.13.15 Solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

3.13.16 Deve estar inclusa na lista de eventos a opção de gerar automaticamente gráficos ou tabelas com o evento, a origem e distribuição de destino.

3.13.17 Deve detectar ataques de negação de serviço e correlacionar eventos de todas as fontes;

3.13.18 Deve estar incluso horários predefinidos, diários, semanais e relatórios mensais. Incluindo Top eventos, Top origem, Top destinos, Top Serviços, Top origens e os seus principais eventos, Top destinos e seus principais eventos;

3.13.19 Deve suportar a programação de emissão de relatórios automáticos, suportando agendamentos, no mínimo, diário, semanal e mensal. Também deve permitir ao administrador definir a data e a hora que a solução inicia o processo de emissão do relatório;

3.13.20 Deve suportar a geração de relatório gerencial para apresentar aos executivos os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidades de eventos gerados e protegidos.

3.13.21 Deve possuir uma linha do tempo que permita ao administrador visualizar os eventos de forma correlacionada, através de hora, dia ou mês, permitindo a identificação sem qualquer criação de buscas, facilitando a rápida ação do administrador e minimizando os impactos na rede;

3.13.22 Deve implementar, ou utilizar solução de terceiros, no mínimo, com os seguintes tipos de correlação de eventos:

3.13.22.1 Compressão: Consiste em reduzir múltiplas ocorrências de um mesmo evento por um único evento, indicando quantas vezes o evento ocorreu durante o período de observação;

3.13.22.2 Filtragem: Consiste em suprimir um determinado evento, em função dos valores de um conjunto de parâmetros, previamente especificados;

3.13.22.3 Contagem: Capacidade de quantificar/contar a ocorrência de um mesmo evento;

3.13.22.4 Escalação: É a capacidade de um evento, através da análise de outros eventos ser considerado de maior importância ou severidade;

3.14 Serviços - Implantação das Soluções

3.14.1 A etapa de implantação e migração (remoção das ferramentas de segurança existentes e ativação das novas) deverá ocorrer nos locais de entrega dos produtos;

3.14.2 Compreende-se nesta etapa a instalação de sistemas, softwares e aplicativos da CONTRATANTE nos PRODUTOS fornecidos, bem como a migração de configurações dos equipamentos existentes na CONTRATANTE para os PRODUTOS fornecidos pela CONTRATADA ou estudo, planejamento e configuração inicial como a criação de regras e politicas dos equipamentos, visando a plena operação dos equipamentos, inclusive com a implementação de VPN entre sites;

3.14.3 Caberá à CONTRATANTE o acompanhamento da migração/configuração inicial, fornecimento de informações sobre os aplicativos e ferramentas existentes no ambiente, bem como a definição e concessão de janelas de intervenção;

3.14.4 A etapa de implantação e migração deve acontecer de forma gradual e transparente, de acordo com a conveniência da CONTRATANTE;

3.14.5 Durante a etapa de implantação e migração, os PRODUTOS fornecidos pela CONTRATADA serão colocados em plena operação, em condições reais de produção;

3.14.6 Durante esta etapa, a equipe da CONTRATADA deverá estar presente, nos horários de implantação e migração definidos entre a CONTRATANTE e a CONTRATADA;

3.14.7 As atividades de implantação e migração, de acordo com a necessidade, poderão ser executadas em horário comercial, período noturno ou final de semana;

3.14.8 A CONTRATADA deve garantir que a migração não irá alterar as versões ou o funcionamento dos serviços instalados na unidade objeto da migração, sem a prévia autorização da CONTRATANTE;

3.14.9 A CONTRATADA deverá, com a supervisão da CONTRATANTE, planejar e realizar a instalação dos softwares e a configuração dos novos equipamentos com total interoperabilidade operacional com ambiente atual da CONTRATANTE, sem impacto no ambiente de produção;

3.14.10 Durante a implantação e integração, a CONTRATADA deverá realizar, entre outras atividades: instalação de softwares, acompanhamento de migrações de regras e políticas, elaboração e execução de scripts, análise de performance, tunning, resolução de problemas, criação de regras e politicas, implementação de VPN site-to-site, identificação e solução de vulnerabilidades e implementação de segurança;

3.14.11 Se houver necessidade de disponibilização de elementos adicionais para o pleno funcionamento, integração e migração dos produtos ao ambiente da CONTRATANTE, estes deverão ser fornecidos pela CONTRATADA sem ônus adicional à CONTRATANTE;

3.14.12 Para implantação e migração devem ser consideradas as seguintes premissas:

3.14.13 Caberá à CONTRATADA a disponibilização de todos os recursos necessários, tais como hardwares, softwares, recursos humanos necessários à instalação dos PRODUTOS;

3.14.14 O fornecimento de toda e qualquer ferramenta, instrumento, material e equipamento de proteção, bem como materiais complementares, traslado, transporte, estada, embalagens, estritamente necessários à instalação, configuração e migração dos produtos são de inteira responsabilidade da CONTRATADA;

3.14.15 A CONTRATADA realizará adequação/configuração dos produtos fornecidos ao longo da etapa de migração e realização de novas configurações;

3.14.16 A CONTRATANTE deverá fornecer todas as licenças necessárias dos produtos ofertados e dos elementos adicionais que se fizerem necessários à instalação/migração e ao pleno funcionamento do ambiente de produção;

3.14.17 Ao final da implantação e migração deve-se permitir o gerenciamento/monitoração da disponibilidade dos produtos, customização de alertas, análise de desempenho, incluindo o tratamento de dados históricos e uso de console local e remota, pela CONTRATANTE;

3.15 HORAS DE SUPORTE

3.15.1 Os serviços estipulados deverão ser executados por uma única pessoa jurídica, sendo desta a total responsabilidade pelo cumprimento das obrigações assumidas;

3.15.2 Os serviços deverão ser executados sempre em conjunto com a equipe técnica da EMATER-DF, exclusivamente nas dependências da CONTRATADA.

3.15.3 Serviços deverão atentar ao horário de funcionamento, ou seja, de segunda a sexta-feira, das 08:00 às 17:00. Caso seja necessária intervenção em que ocorra a indisponibilidade de recursos de rede, o serviço deverá ser realizado fora do horário de expediente (após as 17 horas ou sábado/domingo);

3.15.4 Os serviços poderão ser utilizados para o planejamento de migração, validação de regras para migração, implantação de novas regras/funcionalidades, análise e mitigação de vulnerabilidades e/ou qualquer melhoria nas configurações de software da solução;

3.15.5 Os serviços serão solicitados através da emissão, por parte da Contratante, de Ordem de Serviço (conforme modelo a ser definido pela Contratada) onde será especificada a natureza das atividades a serem desempenhadas, incluindo os quantitativos de horas;

3.15.6 Após a execução dos serviços, a Contratada deverá apresentar relatório de execução de serviços onde conste a descrição do serviço executado, complexidade e quantidade de horas executadas;

3.15.7 A emissão da Nota Fiscal correspondente aos serviços realizados somente poderá ser realizada após o aceite da Ordem de Serviço, realizado por parte da Fiscalização do Contrato;

3.15.8 Os prazos para execução dos serviços são descritos a seguir:

3.15.9 Os serviços deverão ser executados dentro do quantitativos de horas especificado em cada Ordem de Serviço. Caso este prazo não seja alcançado, somente serão pagas as horas inicialmente acordadas na Ordem de Serviço;

3.15.10 As atividades deverão seguir as boas práticas do próprio Fabricante e quando necessário a Contratante pode solicitar, informando na Ordem de Serviço, a validação das tarefas pelo Fabricante;

3.15.11 Atividades relacionadas a problemas, correções, atualizações de firmware, indisponibilidade ou falhas nos equipamentos serão tratados como garantia e suporte, por isso não serão definidas como horas de serviço técnico especializado.

3.16 Serviços - Treinamento

3.16.1 A CONTRATADA fornecerá treinamento da solução de Firewall, deverá ter carga horária mínima de 24 (vinte e quatro) horas;

3.16.2 O mínimo de alunos em uma turma formada exclusivamente por servidores da EMATER é de 02 (dois) alunos, sendo possível que uma quantidade menor de servidores seja adicionada a uma turma formada com outros alunos indicados pela CONTRATADA;

3.16.3 O período de realização dos cursos será fixado pela EMATER em conjunto com a CONTRATADA, no prazo máximo de 90 (noventa) dias após a assinatura do contrato;

3.16.4 O treinamento deverá ser ministrado em local fornecido pela CONTRATADA ou em dependência da CONTRATANTE, de segunda a sexta-feira, das 08:00 às 12:00 ou das 14:00 às 18:00, à critério da EMATER, na cidade de Brasília-DF, de modo que o aluno possa praticar, ao menos, a configuração, o gerenciamento e a operação dos equipamentos e softwares que compõem a solução.

3.16.5 A CONTRATADA deverá emitir para o servidor participante, sem ônus para a CONTRATANTE, e no prazo máximo de 10 (dez) dias úteis após o término do treinamento, o certificado oficial de conclusão, no qual deverá constar o nome do treinando, a data, o local e a carga horária. A cópia desses certificados deverá acompanhar a nota fiscal/fatura para o devido pagamento.

3.16.6 Todo o material didático oferecido pela CONTRATADA para realização dos treinamentos deverá ser oficial do fabricante dos equipamentos e softwares, de primeiro uso, atualizados e poderão estar em inglês ou português.

4. DO QUANTITATIVO:

Descrição	Quantidade
Equipamento Firewall	1
Software de Gerenciamento	1
Serviço de Instalação e Configuração	1
Horas de suporte técnico	200h
Treinamento (pro aluno)	2

5. DO PRAZO, LOCAL DE ENTREGA E DO RECEBIMENTO:

5.1. Local de entrega: Parque estação biológica edifício sede EMATER-DF – Asa Norte – Brasília-DF. Cep. 70770-915 de segunda à sexta-feira, exceto feriados, entre 8h00m e 11h00m ou entre 13h00m e 16h00m.

5.2. Prazo para entrega: Os equipamentos deverão ser entregues em perfeita condição de uso **no prazo máximo de ate 60 (sessenta) dias após a emissão da nota de empenho**.

5.3. Recebimento provisório dos equipamentos e licenças: os equipamentos serão recebidos provisoriamente, por empregado ou comissão devidamente designada pela autoridade da EMATER-DF, desde que entregues em perfeitas condições de uso e em conformidade com as especificações exigidas pela CONTRATANTE em até 10 (dez) dias após a entrega;

5.4. Recebimento definitivo dos equipamentos e licenças: o recebimento definitivo ocorrerá em **até 10 (dez) dias** a contar da data do recebimento provisório dos equipamentos e licenças;

5.5. Recebimento definitivo do serviço de treinamento: o recebimento definitivo do serviço de treinamento ocorrerá em até 5 (cinco) dias a contar da data de recebimento dos certificados de conclusão;

5.6. Recebimento definitivo do objeto: o recebimento definitivo do objeto ocorrerá em até **10 (dez) dias** a contar da data de emissão do termo de aceite do serviço de instalação.

6. DA GARANTIA, MANUTENÇÃO PREVENTIVA E CORRETIVA E ASSISTÊNCIA TÉCNICA:

6.1. O período de Garantia Técnica deverá ser de, no mínimo, 36 (trinta e seis) meses e será contado a partir da data de aceite definitivo do(s) equipamento(s) ou software(s) a ser emitido pelo Fiscal de Contrato;

6.2. Durante o período de Garantia técnica deverá ser realizada a atualização dos softwares e do firmware de todos os equipamentos para as versões mais recentes, sem ônus adicional para a EMATER além daquele já cotado na proposta;

6.3. O registro dos chamados será realizado por meio de número telefônico/e-mail disponibilizado pela contratada ou por meio de sistema próprio para registro de chamados, disponibilizado na internet.

6.4. A garantia deve cobrir defeitos em componentes do hardware que incorram em mau funcionamento do equipamento. Em caso de defeito que impossibilite o conserto ou da inexistência de componentes para reposição, a Contratada deverá realizar a substituição do equipamento por outro (novo, de primeiro uso), não inferior e sem custo para a Contratante.

7. DA ESTIMATIVA DE CUSTO:

7.1. A estimativa de custo para aquisição dos equipamentos de informática é da ordem de **R$ 305.299,33 (trezentos e cinco mil, duzentos e noventa e nove reais e trinta e três centavos)**, conforme planilhas demonstrativas abaixo.

7.2. PLANILHA DEMONSTRATIVA:

LOTE 01 – Descritivo de Equipamentos e Valores					
Item	**Descrição**	**Unidade**	**Quant.**	**Preço Unitário**	**Total**
1.	Firewall	Equip.	01	R$ 146.703,33	R$ 146.703,33
2.	Software de Gerenciamento	Licença	1	R$ 92.370,00	R$ 92.370,00
3.	Serviço de Instalação e Configuração	Unid.	01	R$ 11.020,00	R$ 11.020,00
4.	Horas de suporte técnico	Horas	200	R$ 221,33	R$ 44.266,00
5.	Treinamento	Aluno	02	R$ 5.470,00	R$ 10.940,00
TOTAL					**R$ 305.299,33**

8. DO PAGAMENTO:

8.1. Para os itens 1, 2, 3 e 5 o pagamento deverá ser efetuado em até 30 dias após o recebimento definitivo de cada item, **em conformidade com a legislação vigente;**

8.2. Para o item 4 o pagamento deverá ser efetuado após em até 30 dias após o recebimento da nota fiscal/fatura referente à execução do serviço e utilização de horas de suporte;

8.3. O pagamento ficará condicionado à comprovação de regularidade junto à fazenda pública federal, estadual e municipal, assim como regularidade junto à receita federal (CND), fundo de garantia por tempo de serviço (FGTS), tribunal superior do trabalho (CNDT) e

apresentação de nota fiscal eletrônica conforme protocolo icms 42, de 3 de julho de 2009 e suas alterações;

8.4. As empresas com sede ou domicílio no distrito federal, com créditos de valores iguais ou superiores a R$ 5.000,00 (cinco mil reais), os pagamentos serão efetuados exclusivamente, mediante crédito em conta corrente, em nome do beneficiário junto ao banco de Brasília S/A – BRB. Para tanto, deverão apresentar o número da conta corrente e agência onde deseja receber seus créditos, de acordo com o decreto nº 32.767/2011;

8.5. Empresas de outros estados que não tenham filiais ou representações no Distrito Federal poderão indicar conta corrente de outro banco, conforme decreto n º 32.767/2011.

9. VIGÊNCIA DO CONTRATO

9.1. O Contrato terá vigência de 36 meses, **contados a partir da data de sua assinatura** podendo ser prorrogado até o prazo máximo estabelecido em lei.

10. DA CONDIÇÃO DE PARTICIPAÇÃO:

10.1. Como condição de habilitação da empresa licitante, esta deverá apresentar declaração atestando que não possui **em seu quadro societário**, servidor público da ativa ou empregado de empresa pública ou de sociedade de economia mista.

11. DAS OBRIGAÇÕES DA CONTRATADA:

11.1.A contratada deverá entregar os equipamentos em perfeitas condições de uso, em conformidade com as especificações do objeto, da legislação vigente visando sempre cumprir os prazos e datas estabelecidas neste Termo de Referência.

11.2.A contratada deverá possuir **representante comercial ou assistência técnica credenciada no Distrito Federal** para manutenção da garantia dos equipamentos**.**

11.3.A contratada deverá entregar os equipamentos em perfeita condição de uso, com as devidas mídias de instalação e licenças de uso autorizadas para uso nos equipamentos.

11.4. Efetuar a imediata substituição do objeto/equipamento ou acessório que apresentar defeitos, no prazo de 48h (quarenta e oito horas) do recebimento da notificação emitida pela contratante. Esse prazo poderá ser prolongado desde que devidamente justificado e acordado entre as partes.

11.5. Responder pelos danos causados à EMATER-DF e/ou a terceiros decorrentes da falha de equipamentos e/ou acessórios quando da sua montagem, ou mesmo pela culpa ou dolo de seus empregados ou prepostos quando da manutenção dos referidos equipamentos.

11.6. Cumprir as normas internas da EMATER-DF, bem como aquelas que regulam as ações de higiene e segurança do trabalho;

11.7. Responsabilizar-se por todas as despesas diretas ou indiretas tais como: salários, transportes, encargos sociais, fiscais, trabalhistas, previdenciários e de ordem de classe, indenizações e quaisquer outras que forem devidas aos seus empregados no cumprimento de suas obrigações;

11.8. Manter durante a execução do contrato todas as condições de habilitação e qualificação bem como as que comprovem sua compatibilidade com as obrigações assumidas;

11.9. A CONTRATADA deverá se responsabilizar pela qualidade dos materiais e serviços executados/fornecidos inclusive a promoção de readequações, sempre que detectadas impropriedades que possam comprometer a consecução do objeto contratado;

11.10. A CONTRATADA deverá permitir o livre acesso aos documentos e registros contábeis, aos servidores dos órgãos ou entidades públicas concedentes ou contratantes, bem como aos órgãos de controle interno e externo;

12. .DAS OBRIGAÇÕES DA CONTRATANTE:

12.1. Permitir o acesso aos empregados da empresa vencedora ao local de entrega dos equipamentos desde que devidamente identificados;

12.2. Informar à CONTRATADA e seus prepostos, tempestivamente, todas as providências necessárias ao bom andamento para a entrega dos equipamentos; prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA;

12.3. Comunicar prontamente a Contratada toda e qualquer anormalidade verificada nos equipamentos, bem como nos softwares fornecidos, e/ou nos serviços executados;

12.4. Efetuar o recebimento dos materiais conforme especificações do objeto e indicar o local para guarda dos mesmos;

12.5. Designar empregado ou comissão para fiscalização da entrega e da prestação da garantia do objeto desse Termo de Referência;

12.6. Rejeitar no todo ou em parte os objetos entregue em desacordo com as especificações contidas neste Termo de Referência;

12.7. Exercer a fiscalização dos bens e serviços, na forma prevista na Lei n° 8.666/93, inclusive do cumprimento das obrigações e encargos sociais e trabalhistas pela CONTRATADA, no que se refere à execução do contrato;

12.8. Verificar prazos, garantias, certidões e atestar notas fiscais;

12.9. Efetuar o pagamento em conformidade com a legislação vigente no Distrito Federal.

13. DAS PENALIDADES:

13.1. Pelo descumprimento de quaisquer cláusulas ou condições dispostas neste Termo de Referência, serão aplicadas as penalidades estabelecidas no Decreto nº 26.851/06 e

atualizações, que regulamenta a aplicação de sanções administrativas previstas na Lei nº 8.666/93 e alterações, facultada à EMATER-DF, a rescisão unilateral do contrato.

14. DO FORO:

14.1. Fica eleito o foro da Justiça do Distrito Federal para dirimir as dúvidas não solucionadas administrativamente oriundas do comprimento das obrigações estabelecidas.

15. DAS DISPOSIÇÕES FINAIS

15.1. Havendo irregularidades neste instrumento, entre em contato com a ouvidoria de combate a corrupção, no telefone 0800-6449060.

Brasília-DF, 19 de abril de 2017.

FABRÍCIO PORTES BRAGA
Responsável pela Elaboração

LÍVIA VERÍSSIMO MAGALHÃES
Revisado por

DANIELLA MOREIRA CARVALHO
Gerente de Compras, Material e Patrimônio