PODER JUDICIÁRIO
SUPERIOR TRIBUNAL MILITAR
PRSTM/DIREG/DITIN/COTEC

TERMO DE REFERÊNCIA

1. OBJETO

Contratação de empresa para aquisição de serviço de solução de proteção de perímetro com gerenciamento e suporte com garantia para 30 meses.

2. FUNDAMENTAÇÃO

A modernização dos recursos oferecidos ao público é uma realidade frente aos esforços executados pelo STM para manter seu parque tecnológico atualizado e preparado contra os ataques virtuais. É de suma importância para um órgão governamental possuir as últimas tecnologias existentes no mercado, para melhor prover serviços e para melhor prover serviços e para melhor atender ao público. A evolução tecnológica e a globalização têm influenciado de forma contundente a área de tecnologia da informação dos órgãos brasileiros, influência esta que independe do seu ramo de negócio, porte comercial ou estrutura organizacional. Essa evolução desencadeou e possibilitou a prática de crimes virtuais complexos que exigem soluções rápidas, práticas e especializadas. Para isso, as ferramentas de segurança da informação devem estar sempre à frente desta evolução. Para que isso seja possível, se toma indispensável a modernização de nosso sistema de segurança de informação, já que desatualizado, o órgão poderá se tornar refém de elementos mal intencionados, causando prejuízos incalculáveis à Justiça Militar da União - JMU.

É necessário também contar com o apoio de suporte técnico especializado, fornecido por empresa certificada pelo fabricante do software como apta a prestar suporte a ambientes corporativos críticos com comprovada excelência.

A experiência no uso da solução de firewall registra inúmeras situações em que o suporte técnico especializado mostrou-se imprescindível para manter os serviços no ar: problemas com novas características implementadas nas novas versões do software, bem como sua instalação e configuração, sempre demandam conhecimento especializado para resolução de eventuais problemas. A implementação de novas regras de segurança e tratamento de incidentes de segurança também motivaram, no passado, abertura de chamados técnicos junto ao suporte técnico especializado

3. OBJETIVOS A SEREM ALCANÇADOS POR MEIO DA CONTRATAÇÃO

3.1. Assegurar os níveis de serviço adequados à JMU no tocante a Segurança da Tecnologia da Informação;

3.2. Aumento do grau de satisfação dos usuários com os produtos e serviços fornecidos pela área de SI;

3.3. Redução dos riscos de interrupção dos serviços e sistemas em decorrência da ataques cibernéticos;

3.4. Melhoria da entrega dos serviços de SI aos usuários em decorrência da utilização de boas práticas dos processos de gerenciamento de serviços de TI;

3.5. Implantar processo estruturado e instrumentalizado de gerenciamento de incidentes de segurança da informação, em que as etapas de triagem, classificação, análise, resposta e comunicação sigam as melhores práticas de internacionais;

3.6. Criar bases históricas e estatísticas de incidentes, permitindo traçar tendências ou pontos que necessitam de aprimoramento;

3.7. Permitir a análise crítica dos logs de segurança de forma automatizada, tendo em vista a incapacidade humana de visualizar todas as centenas de eventos de segurança que ocorrem a cada segundo e em diferentes soluções;

3.8. Responder mais rapidamente aos ataques cibernéticos;

3.9. Possuir capacidade de identificação preventiva de ameaças emergentes e de eventuais vazamentos antes da divulgação pública;

3.10. Redução do tempo de restauração da operação normal dos serviços com o mínimo de impacto nos processos de negócios da CONTRATANTE, dentro dos Níveis Mínimos de Serviço (NMS) e prioridades acordados;

3.11. Melhoria da percepção do adequado gerenciamento de segurança de SI por parte da alta administração e dos usuários internos e externos, deixando transparente que há efetivo gerenciamento dos incidentes de segurança de tecnologia da informação;

3.12. Melhoria da disseminação de informações relacionadas à Segurança da Informação nos diversos níveis organizacionais;

3.13. Definição clara dos objetivos, produtos, prazos, custos, padrões de qualidade, responsabilidades das partes, além de indicadores de desempenho;

3.14. Incremento de qualidade no tratamento dos eventos de segurança;

3.15. Melhoria na identificação e tratamento de vulnerabilidades de segurança do ambiente de TI;

3.16. Investir no desenvolvimento de processos de trabalho seguros, ao invés de apenas investir em tecnologia;

3.17. Desenvolver resiliência e melhorar a capacidade da TI de enfrentar eventos adversos relacionados a cibersegurança.

4. ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO ESTRATÉGICO DA JMU OU DE TIC

Objetivo: 7 - Aperfeiçoamento da Tecnologia da Informação e Comunicação

Estratégia: - Aprimorar a infraestrutura de Tecnologia da Informação e Comunicação (TIC) para suporte às atividades administrativas e judiciais.

Iniciativa: - Elaborar e implementar programa para aprimorar a rede de dados e voz

5. JUSTIFICATIVA DA SOLUÇÃO ESCOLHIDA

Considerando a importância vital que os sistemas e serviços de TI adquiriram para a JMU e que se observa a constante diversificação e desenvolvimento de novas ameaças cibernéticas, são mandatórios a constante evolução, o aprimoramento dos mecanismos de segurança, bem como o desenvolvimento de equipes e de métodos de segurança cada vez mais complexos. Portanto, verifica-se que o atual modelo de contratações, por meio da compra de produtos e contratação de serviços de operação, não é suficiente para fazer frente à velocidade com surgem novos tipos de ameaças, e principalmente a velocidade com que o mercado de segurança evolui e lança novos produtos, o modelo para a contratação será a de aquisição de serviço de solução de proteção de perímetro com gerenciamento e suporte com garantia para 30 meses.

Tal modelo tem como principais vantagens a:

• Maior flexibilidade com relação à aquisição de produtos;

• Os serviços podem ser contratados sob demanda, conforme a necessidade e disponibilidade financeira do cliente;

• Maior velocidade de inserção de novas tecnologias;

• Utilização de profissionais altamente capacitados e especialistas em cibersegurança, que dificilmente atuariam em um único cliente de pequeno porte;

• Menor custo total de propriedade (Total Cost of Ownership – TCO), tendo em vista os custos de compra, operação e capacitação contínua a longo prazo.

6. ESPECIFICAÇÕES TÉCNICAS e demais requisitos

6.1. Requisitos de arquitetura tecnológica

6.1.1. Características gerais

6.1.1.1. É permitido a composição da solução ofertada entre diversos fabricantes, desde que não contemple solução de software livre;

6.1.1.2.A comunicação entre os appliances de segurança e o módulo de gerência deve ser através de meio criptografado;

6.1.1.3. Na data da proposta e durante a vigência do contrato, nenhum dos modelos ofertados poderá estar/ser listado no site do fabricante em listas de end-of-life, end-of-support e/ou end-of-sale;

6.1.1.4. Os equipamentos de rede fornecidos deverão permitir a operação plena com os protocolos IPv4 e IPv6, devendo atender ao selo “IPV6 Ready Logo Gold” encontrado no site https://www.ipv6ready.org/.

6.2. Capacidade e quantidades

A solução de segurança deve possuir a capacidade e as características abaixo:

6.2.1. Solução em alta disponibilidade de segurança de perímetro de próxima geração

6.2.1.1. Throughput NGFW de, no mínimo, 1.5 (um ponto cinco) Gbps, com as funcionalidades de firewall, controle de aplicação, filtro URL, IPS e anti-malware habilitadas e atuantes;

6.2.1.1.1. O Throughput é a quantidade de tráfego que um único equipamento é capaz de encaminhar, não havendo soma entre os membros do cluster;

6.2.2. Thoughput de IPS de, no mínimo, 4.5 (quatro ponto cinco) Gbps;

6.2.3. Suporte a, no mínimo, 8.000.000 (oito milhões) de conexões simultâneas;

6.2.4. Suporte a, no mínimo, 65.000 (sessenta e cinco) novas conexões por segundo;

6.2.5. Armazenamento de, no mínimo, 240GB SSD;

6.2.6. No mínimo, 08 (oito) interfaces de rede de 1GbE;

6.2.7. Suportar no mínimo, 04 (quatro) interfaces de rede de 10GbE SFP+, para expansão futura;

6.2.8. 01 (uma) interface do tipo console ou similar;

6.2.9. 01 (uma) interface dedicada para gerenciamento fora de banda (*out-of-band*);

6.2.10. Suportar, no mínimo, 2 instâncias de firewall virtual;

6.2.11. O Throughput e as interfaces solicitados neste item deverão ser comprovados através de datasheet público na internet. Não serão aceitas declarações de fabricantes informando números de performance e interfaces;

6.2.12. Todas as interfaces fornecidas nos appliances devem estar licenciadas e habilitadas para uso imediato, incluindo seus transceivers/transceptores;

6.2.13. Deve ser entregue solução em alta disponibilidade com no mínimo 02 (dois) equipamentos operando em cluster ativo/passivo ou ativo/ativo;

6.2.14. Não serão aceitos appliances virtualizados para os firewalls, somente equipamentos físicos.

6.3. Funcionalidade de firewall

6.3.1. A solução deve consistir de appliance de proteção de rede com funcionalidades de proteção de próxima geração;

6.3.2. As funcionalidades de proteção de rede que compõe a plataforma de segurança, podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação técnica;

6.3.3. O hardware e software que executem as funcionalidades de proteção de rede deve ser do tipo appliance. Não serão aceitos equipamentos servidores e sistema operacional de uso genérico;

6.3.4. A solução deve permitir a segregação entre o plano de dados de gerenciamento do plano de dados de rede;

6.3.5. Todos os equipamentos fornecidos devem ser próprios para montagem em rack 19", incluindo kit tipo trilho para adaptação se necessário e cabos de alimentação;

6.3.6. Os dispositivos de proteção de rede devem possuir pelo menos as seguintes funcionalidades:

6.3.6.1. Suporte a, no mínimo, 1024 VLAN Tags 802.1q, agregação de links 802.3ad, policy based routing ou policy based forwarding, roteamento multicast, DHCP Relay, DHCP Server e Jumbo Frames;

6.3.7. Realizar roteamentos unicast e multicast simultaneamente em uma única instância(contexto) de firewall;

6.3.8. Deve suportar os seguintes tipos de NAT:

6.3.8.1. Nat dinâmico (Many-to-1), Nat estático (1-to-1), Tradução de porta (PAT), NAT de Origem, NAT de Destino e suportar NAT de Origem e NAT de Destino simultaneamente;

6.3.9. Enviar logs para sistemas de monitoração externos, simultaneamente;

6.3.10. Prover mecanismo contra ataques de falsificação de endereços (IP Spoofing), através da especificação da interface de rede pela qual uma comunicação deve se originar. Não sendo aceito soluções que utilizem tabela de roteamento para esta proteção;

6.3.11. Para IPv4, deve suportar roteamento estático e dinâmico (RIPv2, BGP e OSPFv2);

6.3.12. Para IPv6, deve suportar roteamento estático e dinâmico (OSPFv3);

6.3.13. Deve suportar NAT64;

6.3.14. Suportar OSPF graceful restart;

6.3.15. Deve permitir a segregação entre o plano de dados de gerenciamento do plano de dados de rede;

6.3.16. A solução deve possuir mecanismo para dedicar processamento no equipamento de segurança para funções / ações de gerenciamento, mesmo que o equipamento esteja com alto processamento de CPU. Assim evitando a falta de acesso do administrador para qualquer mitigação de problema e aplicação de política para solução de problema. Entre as funções, deve suportar no mínimo: acesso SSH, FTP, WEB, alterações de política e comunicação SNMP;

6.3.17. Deve estar equipado com ferramenta de monitoração de pacotes de rede tipo sniffer para acompanhamento e visualização de tráfego de rede em tempo real, inclusive com a capacidade de aplicação de filtros personalizados. A ferramenta deve ter a opção de gravar o tráfego capturado em arquivos do tipo CAP, PCAP ou equivalente;

6.3.18. O Firewall deve ter a capacidade de operar de forma simultânea mediante o uso das suas interfaces físicas nos seguintes modos: transparente, mode sniffer (monitoramento e análise o tráfego de rede), camada 2 (L2) e camada 3 (L3);

6.3.19. Deve possuir sistema de monitoramento em tempo real do hardware via interface gráfica, interface Web HTTPS e linha de comando CLI;

6.4. Funcionalidade de filtro de conteúdo web

6.4.1. Controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

6.4.2. Controle de políticas por usuários, grupos de usuários, IPs e redes;

6.4.3. Deve de-criptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;

6.4.4. Suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

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

6.4.5.1. Deve ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

6.4.5.2. Reconhecer pelo menos 2.800 (Duas mil e oitocentos) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, *update* de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

6.4.6. A checagem de assinaturas deve determinar se uma aplicação está utilizando a porta padrão ou não;

6.4.7. Para tráfego criptografado (SSL), deve de-criptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

6.4.8. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo;

6.4.9. A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

6.4.10. Atualizar a base de assinaturas de aplicações automaticamente;

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

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

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

6.4.14. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações do órgão;

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

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

6.4.16.1. Permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

6.4.16.2. Deve ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

6.4.16.3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

6.4.16.4. Suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

6.4.16.5. Deve bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;

6.4.16.6. Suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs.

6.4.16.7. Suportar a criação de categorias de URLs customizadas;

6.4.16.8. Suportar a exclusão de URLs do bloqueio, por categoria;

6.4.16.9. Permitir a customização de página de bloqueio;

6.4.17. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

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

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

6.5. Funcionalidades de prevenção de ameaças

6.5.1. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS e suportar os

módulos de: Antivírus e Anti-Malware integrados no próprio equipamento de firewall;

6.5.2. Possuir capacidade de detecção de, no mínimo, 7.000 (sete mil) assinaturas de ataques pré-definidos;

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

6.5.4. Deve suportar granularidade nas políticas de Antivírus e Anti-malware, possibilitando a criação de diferentes políticas por endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

6.5.5. Detectar e bloquear a origem de portscans;

6.5.6. Bloquear ataques conhecidos, permitindo ao administrador acrescentar novos padrões de assinaturas e customizações;

6.5.7. Possuir assinaturas para bloqueio de ataques de buffer overflow;

6.5.8. Suportar o bloqueio de malware em, pelo menos, os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, IMAP, SMB e FTP;

6.5.9. Suportar bloqueio de arquivos por tipo;

6.5.10. Identificar e bloquear comunicação com botnets;

6.5.11. Deve suportar referência cruzada com CVE;

6.5.12. Registrar na console de monitoração as seguintes informações sobre ameaças identificadas:

6.5.12.1. O nome da assinatura e do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo de proteção;

6.5.13. Deve suportar a captura de pacotes (PCAP), em assinatura de IPS e Anti-Malware, através da console de gerência centralizada;

6.5.14. Os eventos devem identificar o país de onde partiu a ameaça;

6.5.15. Suportar rastreamento de vírus em arquivos pdf;

6.5.16. Deve suportar a inspeção em arquivos comprimidos (zip, gzip,etc.);

6.5.17. Possuir a capacidade de prevenção de ameaças não conhecidas;

6.5.18. Suportar a criação de políticas por Geo Localização, permitindo que o tráfego de determinado País/Países seja bloqueado;

6.5.19. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos;

6.5.20. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

6.5.21. Prevenir através do bloqueio efetivo do malware desconhecido (Dia Zero), oriundo da comunicação Web (HTTP e HTTPS) e E-mail (SMTP/TLS) via MTA durante análise completa do arquivo no ambiente sandbox, sem que o mesmo seja entregue parcialmente ao cliente.

6.5.22. O relatório das emulações deve conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

6.5.23. A solução deve ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

6.5.24. Implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL´s conhecidas;

6.5.25. A solução deve fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 7, Windows 8.1 e Windows 10, assim como Office 2010, 2013 e 2016;

6.5.26. 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 antes de entregar este arquivo para o cliente;

6.5.27. Implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

6.5.28. A funcionalidade de prevenção de ameaças avançadas deve ser habilitada de forma independente das outras funcionalidades de segurança;

6.5.29. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

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

6.5.31. Implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware

desconhecido: pdf, tar, zip, rar, seven-z, 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;

6.5.32. A solução deve permitir a criação de Whitelists baseado no MD5 do arquivo;

6.5.33. Para melhor administração da solução, a solução deve possibilitar as seguintes visualizações a nível de monitoração:

6.5.33.1. Número de arquivos emulados;

6.5.34. A solução deve possuir os indicadores abaixo referente ao último dia, última semana ou últimos 30 dias:

6.5.34.1. Arquivos scaneados;

6.5.34.2. Arquivos maliciosos;

6.6. Funcionalidades de controle de qualidade de serviço

6.6.1. Suportar a criação de políticas de QoS por:

6.6.1.1. Endereço de origem, endereço de destino e por porta;

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

6.6.2.1. Banda garantida, banda máxima e fila de prioridade;

6.6.2.2. Disponibilizar estatísticas RealTime para classes de QoS;

6.7. Funcionalidades de VPN

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

6.7.2. Suportar IPSec VPN;

6.7.3. Suportar SSL VPN;

6.7.4. A VPN IPSEc deve suportar:

6.7.4.1. 3DES, Autenticação MD5 e SHA-1, Diffie-Hellman Group 1, Group 2, Group 5 e Group 14, Algoritmo Internet Key Exchange (IKE), AES-XCBC, AES 128 e 256 (Advanced Encryption Standard) e Autenticação via certificado IKE PKI;

6.7.5. A VPN SSL deve suportar:

6.7.5.1. Permitir que o usuário realize a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

6.7.5.2. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

6.7.5.3. Deve ser capaz de informar se a senha do usuário da VPN SSL autenticado via Microsoft Active Directory está próxima a expirar;

6.7.5.4. Atribuição de endereço IP nos clientes remotos de VPN;

6.7.5.5. Atribuição de DNS nos clientes remotos de VPN;

6.7.5.6. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

6.7.5.7. Suportar leitura e verificação de CRL (certificate revocation list);

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

6.8. Solução de Gerenciamento e Relatórios

6.8.1. Deve possuir solução de gerenciamento e administração centralizado, possibilitando o gerenciamento de diversos equipamentos de proteção de rede desde que não sejam software livre;

6.8.2. O módulo de gerência deve ser capaz de gerenciar e administrar todas as soluções descritas neste termo;

6.8.3. Caso a solução possua licenças relacionadas a armazenamento, deve ser ofertado a de capacidade ilimitada;

6.8.4. O gerenciamento da solução deve possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

6.8.5. Centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

6.8.6. O gerenciamento da solução deve suportar acesso via SSH, cliente do próprio fabricante ou WEB (HTTPS);

6.8.7. O gerenciamento deve permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente

de administradores;

6.8.8. Deve possuir um mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

6.8.9. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

6.8.10. Cada regra deve, obrigatoriamente, funcionar nas versões de endereço IPv4 e IPv6 sem duplicação da base de objetos e regras e permitir a captura de pacotes, traffic shapping e utilização de mensagem de bloqueio customizada;

6.8.11. uportar validação de regras antes da aplicação;

6.8.12. Suportar validação das políticas, avisando quando houver regras que, ofusquem ou conflitem com outras (shadowing);

6.8.13. Deve possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;

6.8.14. Suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

6.8.15. Permitir a criação de certificados digitais para autenticação de usuários;

6.8.16. Deve possuir relatórios de utilização dos recursos por aplicações, URL, ameaças (IPS, Antivírus e Anti-Malware), etc;

6.8.17. Prover uma visualização sumarizada de todas as aplicações, ameaças (IPS, Antivírus, Anti-Malware), e URLs que passaram pela solução;

6.8.18. Deve ser possível exportar os logs em CSV;

6.8.19. Deve possibilitar a geração de relatórios de eventos no formato PDF;

6.8.20. Possibilitar rotação do log;

6.8.21. Suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

6.8.21.1. Resumo gráfico de aplicações utilizadas, principais aplicações por utilização de largura de banda, principais aplicações por taxa de transferência de bytes, principais hosts por número de ameaças identificadas, atividades de um usuário específico e grupo de usuários do AD/LDAP, incluindo aplicações acessadas, categorias de URL, URL/tempo de utilização e ameaças (IPS, Antivírus e Anti-Malware), de rede vinculadas a este tráfego;

6.8.22. Deve permitir a criação de relatórios personalizados;

6.8.23. Suportar enviar os relatórios de forma automática via:

6.8.23.1. E-mail em PDF ou HTML;

6.8.24. O gerenciamento centralizado deverá ser entregue como appliance virtual e dever ser compatível/homologado com/para VMWare ESXi;

6.8.25. Deve consolidar logs e relatórios de todos os dispositivos administrados;

6.8.26. Caso a solução possua módulo de relatórios estendida, deverá ser entregue junto com a solução;

6.8.27. Capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

6.8.28. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

6.8.29. Nas opções de Drill-Down, deve ser possível identificar o usuário que fez determinado acesso;

6.8.30. Permitir a integração e avaliação de todos os equipamentos de proteção de rede na gerência com os seguintes padrões regulatórios:

6.8.30.1. ISO 27001 e ISO 27002;

6.8.30.2. NIST 800-41.

6.8.31. Simular o impacto de segurança das alterações de configuração antes da instalação de acordo com a aderência aos padrões regulatórios apresentados no item anterior;

6.8.32. Permitir a customização do padrão regulatório da própria instituição;

6.8.33. Monitorar constantemente o status de conformidade da solução aos padrões regulatórios informados;

6.8.34. Destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados a gestão de conformidade manual;

6.8.35. Permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação;

6.8.36. Gerar relatórios regulamentares com base nas configurações de segurança em tempo real;

6.8.37. Permitir que os relatórios possam ser salvos, enviados e impressos;

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

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

6.8.39.1. Visualizar quantidade de tráfego utilizado de aplicações e navegação;

6.8.39.2. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

6.8.40. A solução deve possuir mecanismo para detectar login de administradores em horários irregulares;

6.8.41. Deve permitir a transferência de arquivos para upgrade dos firewalls via SCP, SFTP e interface de gerenciamento;

6.8.42. A solução deve ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

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

6.8.44. Criar certificados digitais para acesso dos usuários VPN;

6.8.45. Criar certificados digitais para VPNs Site-to-Site;

6.8.46. Caso a solução possua licenciamento relacionado a capacidade de criação de certificados, deve ser contemplado a capacidade ilimitada;

6.8.47. Permitir criações de políticas de acesso de usuários autenticada no Active Directory, de forma que reconheça os usuários de forma transparente;

6.8.48. Permitir a visualização de gráficos e mapa de ameaças;

6.8.49. Deve permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

6.8.50. Deve possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

6.8.51. A solução deve ser capaz de personalizar e criar regras de correlação;

6.8.52. A solução deve possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

7. REQUISITOS DE NÍVEL DE SERVIÇO (SUPORTE TÉCNICO)

7.1. Serviços Gerenciados de Segurança da Informação

7.1.1. Os serviços gerenciados de segurança compreendem o monitoramento, operação, suporte e gerenciamento dos ativos de segurança;

7.1.2. Toda e qualquer alteração de configuração e políticas da solução será realizada exclusivamente pela CONTRATADA;

7.1.3. A CONTRATADA deve ser responsável pelas atividades de planejamento, instalação, configuração, migração tecnológica, elaboração de documentação técnica e operação assistida dos serviços;

7.1.4. Os serviços devem ser prestados utilizando as soluções de segurança em hardware e/ou softwares fornecidas pela CONTRATADA;

7.1.5. Devem ser realizadas atividades de monitoramento de funcionamento e da capacidade dos serviços, resolução de problemas (*troubleshooting*), análise da efetividade de regras e configurações, instalação de *patches* e execução/revisão de procedimentos de *backup* e *restore* de configurações;

7.1.6. Deve ser realizada a criação de regras de proteção do tráfego de rede;

7.1.7. Esse serviço deverá ser realizado de forma local ou remota para assegurar que as operações diárias sejam realizadas em conformidade com os padrões pré-estabelecidos em regime 8x5, conforme a necessidade;

7.1.8. Realizar criação de regras de liberação ou bloqueio conforme solicitação da CONTRATANTE;

7.1.9. As execuções das atividades deverão ser monitoradas por um preposto da CONTRATANTE a fim de garantir a qualidade do serviço prestado;

7.1.10. A prestação dos serviços não gerará vínculo empregatício entre os empregados da CONTRATADA e da CONTRATANTE inexistindo qualquer relação entre as partes que possa caracterizar pessoalidade e subordinação direta, assim como não há dedicação de mão de obra exclusiva;

7.1.11. Todos os equipamentos e softwares necessários à prestação dos serviços devem ser novos, de primeiro uso e não constar, no momento da apresentação da proposta técnica, em listas de endofsale, endofsupport, endoflife ou similares do fabricante, ou seja, não podem ter previsão de descontinuidade de fornecimento, suporte ou vida;

7.1.12. A CONTRATADA deverá observar as melhores práticas de mercado para ambientes similares de forma a se obter uma uniformidade nos controles e padrões de segurança;

7.1.13. Gerar relatórios administrativos e técnicos, ambos customizáveis, em forma de textos e gráficos;

7.1.14. Para quaisquer solicitações que a CONTRATANTE solicitar para a CONTRATADA referente ao serviço prestado, a mesma deve seguir os prazos abaixo para iniciar a execução da solicitação:

Severidade	**Descrição**	**SLA**
1	Alteração de regras e políticas de segurança	Em até 1 hora
2	Alteração de configurações	Em até 1 hora e 30 minutos
3	Verificação de problemas de desempenho e/ou disponibilidade	Em até 3 horas
4	Verificação e filtragem de *logs*	Em até 1 hora
5	Esclarecimento de dúvidas/revisão de regras	Em até 24 horas

7.1.15. O descumprimento de quaisquer das obrigações assumidas importará na aplicação das seguintes penalidades:

Tempo decorrido entre o primeiro apontamento de indisponibilidade e a recuperação da disponibilidade do serviço	**Multa**
30 minutos	Sem aplicação de multa
60 minutos	0,5% do valor total mensal do respectivo item
120 minutos	1% do valor total mensal do respectivo item
180 minutos	1,5% do valor total mensal do respectivo item
240 minutos	2% do valor total mensal do respectivo item

7.2. Serviços de Monitoramento

7.2.1. Deverá monitorar os equipamentos da solução ofertada em regime 24x7x365;

7.2.2. O monitoramento deverá ser realizado através de dispositivos dedicados (hardware) para esta função, fornecidos pela CONTRATADA, de forma que coletarão as informações e enviarão de forma segura ao Centro de Monitoramento (SOC) da CONTRATADA;

7.2.3. Os dispositivos dedicados deverão coletar informações a respeito do desempenho dos elementos monitorados:

7.2.3.1. Utilização de CPU;

7.2.3.2.. Utilização de Memória RAM;

7.2.3.3. Utilização de Discos;

7.2.3.4. Vazão de dados (throughput) de rede;

7.2.3.5. Vazão de pacotes por segundo;

7.2.3.6. Conexões por segundo;

7.2.3.7. Conexões simultâneas;

7.2.4. Os dispositivos dedicados deverão ser capazes de verificar a disponibilidade dos elementos monitorados através de, no mínimo, as seguintes formas:

7.2.4.1.ICMP (ping);

7.2.4.2.SNMP (v1, v2 e v3);

7.2.4.3.Serviços TCP;

7.2.4.4.Serviços UDP;

7.2.5. Os dispositivos dedicados deverão ser capazes de coletar as informações de segurança (ameaças, ataques, intrusões, etc.) fornecidas pelos elementos monitorados e também do ambiente em questão, através de, no mínimo, as seguintes formas:

7.2.5.1.Syslog;

7.2.5.2.Syslog com TLS1.2;

7.2.5.3.Requisições SNMP;

7.2,5.4.Traps SNMP;

7.2.5.5.SSH;

7.2.5.6.REST API;

7.2.6.O monitoramento deverá ser capaz de coletar e reportar, minimamente, os seguintes itens da solução ofertada:

7.2.6.1.Estado das funcionalidades de segurança;

7.2.6.2.Estatísticas dos principais ataques, vírus e aplicações detectados;

7.2.6.3.Alertas de incidentes de segurança;

7.2.7.Os dispositivos dedicados deverão monitorar o domínio de broadcast do qual fazem parte, de forma a permitir detectar e registrar:

7.2.7.1.Novos dispositivos conectados (MAC address e endereço IP);

7.2.7.2.Mudanças de endereços IP de dispositivos conhecidos;

7.2.7.3.Ataques de ARP poisoning;

7.2.8.As informações monitoradas, detectadas ou coletadas deverão ser enviadas ao centro de monitoramento (SOC) sempre de forma criptografada e autenticada, utilizando protocolo TLS 1.2 (baseado em PKI);

7.2.9.O envio das informações criptografadas não deverá depender de túneis de VPN;

7.2.10.A comunicação do monitoramento deverá sempre ser realizada de forma unidirecional, onde apenas os dispositivos dedicados irão se comunicar com o centro de monitoramento (SOC);

7.2.11.O centro de monitoramento (SOC) não deve ter acesso direto aos dispositivos dedicados;

7.2.12.Em caso de perda de comunicação com o centro de monitoramento (SOC), os dispositivos dedicados deverão realizar armazenamento local (cache) das informações coletadas até que a comunicação seja reestabelecida, momento no qual irá enviar os dados históricos ao centro de monitoramento, de forma que não ocorram perdas de dados (gaps);

7.2.13.O centro de monitoramento (SOC) deve ser capaz de comunicar, automaticamente, os alertas através de, no mínimo, as seguintes formas:

7.2.13.1.E-mail;

7.2.13.2.Mensagem SMS;

7.2.14.O centro de monitoramento (SOC) deve possuir controle de acesso físico, onde apenas funcionários autorizados possuem acesso por meio de identificações biométricas;

7.2.15.O centro de monitoramento (SOC) deve possuir monitoramento através de vídeo 24x7 (CFTV), de forma a comprovar o seu funcionamento e o acesso de apenas funcionários autorizados;

7.2.16.O centro de monitoramento (SOC) deverá suportar a abertura de solicitações de atendimento através dos seguintes canais:

7.2.16.1.Número de telefone gratuito (0800);

7.2.16.2.E-mail;

7.2.16.3.Portal de atendimento WEB;

7.2.17.O centro de monitoramento (SOC) deverá contar com funcionários capacitados e altamente profissionais para a realização das atividades de monitoramento proativo, contendo, no mínimo, um profissional com certificado válido para cada

uma das competências abaixo:

7.2.17.1.ISO/IEC 27002;

7.2.17.2.Operação e administração avançada da solução ofertada;

7.2.17.3. Resposta a incidentes de segurança.

8.COMPROVAÇÕES PARA FINS DE HABILITAÇÃO

8.1. A LICITANTE deve possuir e apresentar tantos quantos ATESTADOS de CAPACIDADE TÉCNICA necessários para a devida comprovação do fornecimento, instalação e suporte dos produtos especificados nesse Termo de Referência devidamente conferidos por empresas públicas e/ou privadas, devendo também ser compatíveis em características e quantidades com o objeto desta Licitação;

8.2. Todas as especificações técnicas desse Termo de Referência devem ser comprovadas mediante documentação do próprio fabricante e deverá ser inclusa em anexo na proposta de preço indicando a página e parágrafo ou captura de tela de comprovação de cada um dos subitens dos requisitos técnicos;

8.3. A LICITANTE deve anexar à proposta de preço uma declaração que manterá em seu corpo funcional, durante todo o período de suporte contratado, equipe especializada contendo, no mínimo:

8.3.1. Três profissionais certificados em seu nível máximo na solução do fabricante do firewall ofertado;

8.3.2. Um profissional com certificação Certified Information Systems Security Professional (CISSP);

8.3.3. Um profissional com certificação PMP (Project Management Professional) em seu período de validade;

8.3.4. Um profissional com certificação CSAP (CompTIA Security Analytics Professional) em seu período de validade;

9. DOCUMENTOS A SEREM APRESENTADOS APÓS A INSTALAÇÃO DA SOLUÇÃO

9.1. A CONTRATADA deverá emitir um relatório referente a Lei Geral de Proteção de Dados (LGPD) de toda a solução ofertada, evidenciando quais aspectos da lei a solução está aderente. Esse relatório deve ser emitido por profissional com certificação de mercado específica para proteção de dados;

9.2. A CONTRATADA deverá emitir um laudo técnico com o resultado da análise de vulnerabilidades e teste de invasão da solução ofertada. Esse laudo deve ser emitido por profissional certificado em pelo menos uma das seguintes certificações:

9.2.1. OSCP – Offensive Security Certified Professional;

9.2.2. CEH – Certified Ethical Hacker;

9.2.3. CompTIA PenTest+;

9.2.4. CySA+ - CompTIA Cybersecurity Analyst;

9.3. Ao final, a CONTRATADA, deverá realizar testes de forma continuada e automatizada, por um período de 30 (trinta) dias, para avaliar o nível de segurança das camadas de segurança que protegem a rede DMZ e rede administrativa da CONTRATANTE, não sendo permitido o uso de ferramenta em software livre, suportando no mínimo as seguintes características:

9.3.1. Deve ser capaz de realizar simulações de ataques entre seus componentes distribuídos no ambiente da Contratante sem gerar nenhum impacto e penalidade no ambiente;

9.3.2. Deve informar os resultados das simulações de ataques e propor ações para mitigá-los;

9.3.3. Deve ser capaz de avaliar o nível de segurança do ambiente independentemente das soluções e tecnologias utilizadas pela Contratante;

9.3.4. A solução deve avaliar automaticamente as configurações de proteção contra ataques cibernéticos e relatar o nível de proteção alcançado por meio da infraestrutura de segurança cibernética existente no ambiente;

9.3.5. A solução deve simular ataques cibernéticos sem causar vulnerabilidades e/ou implantar serviços vulneráveis;

9.3.6. Deve utilizar cargas de ataques maliciosos de ambientes reais com o intuito de explorar vulnerabilidades e testar os controles de segurança;

9.3.7. Deve utilizar o framework do MITRE Attack para os sistemas operacionais Windows;

9.3.8. Deve simular ataques a aplicações Web através de HTTP e HTTPS;

9.3.9. Deve permitir a execução de simulações de ataques sob demanda da Contratante;

9.3.10. Deve atualizar a base de ataques de forma automática;

9.3.11. Deve permitir gerar e exportar relatórios nos formatos PDF e CSV;

9.3.12. A solução deve ser capaz de gerar relatórios executivos em formato de arquivo PDF sob demanda e também enviar automaticamente esses relatórios para endereços de e-mail definidos. Os relatórios executivos devem incluir as alterações no nível de segurança da Contratante e os detalhes das variações, incluindo detalhes do ataque que causam essa alteração;

9.3.13. A solução deve simular ataques cibernéticos via componentes de software distintos. Esses componentes de software devem ser instalados em diferentes segmentos lógicos e físicos na infraestrutura da organização ou na nuvem;

9.3.14. A solução deve avaliar o nível de segurança dos dispositivos de proteção em um caminho definido por um componente “atacante” e um componente “vítima”. A solução também deve avaliar, relatar e fornecer informações de correção para cada caminho diferente separadamente;3.1.27.14.Deve verificar de forma contínua a comunicação entre os componentes das soluções e alertar caso haja falha na comunicação;

9.3.15. Deve permitir a instalação em ambientes virtualizados utilizando VMWare ESXi e Microsoft Hyper-V;

9.3.16. O banco de dados de ataque da solução deve ser atualizado automaticamente;

9.3.17. A solução não deve ter limitações em termos de número de ataques ou técnicas de ataque;

9.3.18. Todos os componentes da solução devem ser capazes de funcionar em ambientes sem conectividade com a Internet. Deve haver procedimentos existentes para atualizar a solução nesses cenários de instalação;

9.3.19. Deve possuir parceria tecnológica com fabricantes das soluções de segurança ofertadas, garantindo que as ações para mitigação de ataques sejam específicas para aquele produto;

10. ELEMENTOS PARA GESTÃO DO CONTRATO

10.1. Papéis e Responsabilidades

10.1.1. Fiscal Demandante

10.1.1.1. Emitir o Termo de Recebimento Provisório.

10.1.1.2 Emitir o Termo de Recebimento Definitivo.

10.1.1.3 Avaliar a qualidade dos itens recebidos de acordo com os critérios de aceitação definidos no contrato.

10.1.1.4 Fiscalizar o contrato quanto do ponto de vista funcional da Solução de TI.

10.1.2. Fiscal Administrativo

10.1.2.1 Autorizar a CONTRATADA à emissão de Notas Fiscais e enviá-las para pagamento.

10.1.2.2. Decidir sobre o encaminhamento para a aplicação de penalidade ou o envio para correção dos desvios pela CONTRATADA.

10.1.2.3. Manter o histórico de gerenciamento do contrato, contendo registros formais de todas as ocorrências positivas e negativas da execução do contrato, por ordem histórica.

10.1.2.4. Encaminhar necessidades de mudanças no contrato a Administração.

10.1.3. Fiscal Técnico

10.1.3.1. Avaliar a qualidade dos produtos e/ou dos serviços entregues e das justificativas, quando houver, de acordo com os Critérios de Aceitação definidos em contrato.

10.1.3.2. Identificar a não conformidade entre o serviço ou material entregue e os termos contratuais.

10.2. DEVERES E RESPONSABILIDADES DA CONTRATANTE

10.2.1. Fornecer à CONTRATADA todos os elementos que se fizerem necessários à compreensão dos serviços a serem executados, informações técnicas e dados complementares que se tornem necessários å boa realização dos serviços, colaborando no seu estudo e interpretação.

10.2.2. Apresentar e dar ciência à CONTRATADA sobre as normas e políticas de segurança da informação instituídas.

10.2.3. Permitir o acesso dos profissionais da CONTRATADA, devidamente credenciados, às dependências do CONTRATANTE, bem como o acesso a dados e informações necessários ao desempenho das atividades previstas nesta contratação, ressalvados os casos de matéria sigilosa.

10.2.4. Analisar e responder, em tempo hábil, às solicitações formais da CONTRATADA. referentes aos esclarecimentos sobre os serviços contratados.

10.2.5. Notificar, por escrito, à CONTRATADA qualquer alteração de horário, métodos de trabalho, distribuição e variação dos quantitativos dos serviços controlados, com antecedência de 24 (vinte e quatro) horas.

10.2.6. Notificar, por escrito, à CONTRATADA, da aplicação da eventual multa.

10.2.7. Conferir os fornecimentos de licenças e os serviços executados, confrontando-os com as faturas emitidas pela CONTRATADA, no ato de entrega, recusando-as quando inexatas. incorretas, ou desacompanhadas dos documentos exigidos

neste contrato.

10.2.8. Efetuar os pagamentos oriundos da fiel execução deste contrato, na forma e prazos.

10.2.9. Exercer a fiscalização da execução dos serviços, através da equipe de fiscalização.

10.2.10. A fiscalização por parte do CONTRATANTE não exime, nem reduz a responsabilidade da CONTRATADA no cumprimento dos seus encargos.

10.3. DEVERES E RESPONSABILIDADES DA CONTRATADA

10.3.1. Formalizar a indicação de preposto da empresa, e substituto eventual, para o gerenciamento dos serviços técnicos e gestão administrativa do contrato, com poderes de representante legal para tratar dos assuntos relacionados ao contrato junto CONTRATANTE, em horário comercial, de segunda a sexta feira, sem ônus adicional para a CONTRATANTE.

10.3.2. Responder pela gestão de seus técnicos, coordenando as tarefas em execução.

10.3.3. Garantir a qualidade nas tarefas compatíveis com os padrões e normas estabelecidas pela empresa CONTRATANTE.

10.3.4. Garantir os prazos estipulados em Contrato.

10.3.5. Alocar os funcionários no projeto a ser desenvolvido.

10.3.6. Executar o objeto deste termo em prazo não superior ao máximo estipulado em Contrato

10.3.7. Manter sigilo dos dados e informações confidenciais a que tiverem acesso, de acordo com as Normas de Segurança para Acesso a Informação no âmbito do STM.

10.3.8. Respeitar as normas e procedimentos de segurança da CONTRATANTE, de acordo com as Políticas e Diretrizes de Segurança da Informação no âmbito do STM.

10.3.9. Manter os seus técnicos sujeitos às normas disciplinares da CONTRATANTE, porém sem qualquer vínculo empregatício com o órgão.

10.3.10. Iniciar a execução dos serviços logo após o recebimento da Ordem de Serviço.

10.3.11. Apresentar a CONTRATANTE, relação da equipe e respectiva qualificação profissional e comprovantes, exigidos em conformidade com este Contrato.

10.3.12. Manter durante a execução do contrato, compatibilidade com as obrigações por ela assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

10.3.13. Encaminhar, quando do término da Ordem de Serviço, minudente e circunstanciado relatório, acompanhado da respectiva fatura, relacionando.

10.3.14. Identificação dos serviços executados e concluídos, ou seja, aqueles entregues e aprovados pelo gerente técnico da CONTRATANTE.

10.3.15. Caso o serviço seja cancelado pela CONTRATANTE, esta pagará pelas atividades efetivamente concluídas e entregues pela CONTRATADA.

10.3.16. Responder por quaisquer perdas e danos causados diretamente aos equipamentos. softwares, informações e a outros bens de propriedade da CONTRATANTE. quando esses tenham sido ocasionados por seus técnicos durante a prestação dos serviços objeto desta contratação.

10.3.17. Responder pelas despesas relativas a encargos trabalhistas, de seguro de acidentes, impostos, contribuições previdenciárias e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, os quais não têm nenhum vínculo empregatício com a CONTRATANTE.

10.3.18. Efetuar os serviços conforme condições e especificações estabelecidas pela CONTRATANTE.

10.3.19. Prestar orientações técnicas aos técnicos da CONTRATANTE, através de metodologia interativa, de forma que haja a participação efetiva de todos nos debates, nas definições, pesquisas e na validação das soluções tecnológicas.

10.3.20. Submeter, ao final de cada fase do cronograma dos requisitos temporais, à apreciação e aprovação da equipe técnica da CONTRATANTE, os produtos definidos no OBJETO.

10.3.21. Arcar com despesas de transporte e hospedagem do corpo técnico da CONTRATADA.

10.3.22. As mudanças de parâmetro dos níveis de acordo de serviços, deverão ser formalizadas à CONTRATANTE.

10.3.23. Fornecer a seus técnicos todos os instrumentos necessários à execução dos serviços.

10.3.24. O fornecedor não poderá cobrar valores adicionais ao valor do contrato, tais como custos de deslocamento, alimentação, transporte, alojamento, trabalho em sábados, domingos, feriados ou em horário noturno, bem como qualquer outro valor adicional.

10.3.25. O fabricante deverá possuir suporte técnico, através de formulário da Web e contato telefonico 0800, disponíveis 24

horas por dia, sete dias por semana para o administrador de serviço, em idioma português.

11. ESTIMATIVA DE VOLUME DE BENS/SERVIÇOS

Inicialmente a aquisição contemplará apenas a sede do STM.

12. – ENTREGA, RECEBIMENTO, ACEITE E CANCELAMENTO

12.1. Requisitos de manutenção

12.1.1. O suporte técnico deve iniciar logo após a assinatura do termo de aceite dos serviços de instalação e configuração e deverá ser realizado de forma contínua durante 30 (trinta) meses, e obrigatoriamente, pelo fabricante da ferramenta ou empresa prestadora de serviços devidamente credenciada;

12.1.3. A atualização do produto deve fornecer upgrades para novas versões (ou patches) desenvolvidas durante o período de contratação;

12.1.4. O suporte técnico e garantia abrangem os seguintes serviços: acesso às novas versões do produto e suporte técnico para correção de problemas do produto (Bugs) em horário comercial

12.2 Requisitos Temporais

Etapa	Descrição	Prazo
1	Reunião de Kick off	Até 10 (dez) dias úteis após a assinatura do contrato
2	Apresentação do Plano Executivo de Implantação da Solução	Até 15 (quinze) dias após a assinatura do contrato
3	Apresentação do Plano de Continuidade de Negócios.	Até 15 (quinze) dias após a assinatura do contrato
4	Aprovação dos Planos de Continuidade de Negócios e Plano de Implantação da Solução.	Até 10 (dez) dias após a apresentação dos planos
5	Integração da solução contratada.	Até 15 (quinze) dias após a aprovação do plano executivo de implantação da solução
6	Migração da solução contratada.	Até 15 (quinze) dias após a aprovação do plano executivo de implantação da solução
7	Treinamento	Até 15 (quinze) dias após a aprovação do plano executivo de implantação da solução
8	Vigência do contrato	30 meses a partir da assinatura contratual

12.3. Demais condições especificadas pela Administração.

12.3.1. Prazos e condições de cancelamento

12.3.1.1. O recebimento provisório e definitivo do objeto não exclui a responsabilidade civil a ele relativa, nem a ético profissional, pela sua inexecução e possível cancelamento, dar-se-á se como não satisfeitas as seguintes condições:

12.3.1.1.1. Objeto de acordo com a especificação técnica contidas neste Termo de Referência e na Proposta Comercial vencedora;

12.3.1.1.2. Quantidades em conformidade com o estabelecido na Nota de Empenho;

12.3.1.1.3. Entrega no prazo, local e horários previsto neste Termo de Referência.

12.3.2 Demais condições especificadas pela Administração.

13. CONDIÇÕES DE PAGAMENTO

13.1. O pagamento deverá ser efetuado em 30 parcelas mensais,

13.2. Para efeitos de pagamento, a CONTRATADA deverá apresentar documento de cobrança constando, de forma discriminada a efetiva realização do objeto adquirido, informando o nome e numero do banco, a agência e o número da conta corrente em que o crédito deverá ser efetuado.

13.4. Deverá apresentar juntamente com o documento de cobrança a comprovação de que cumpriu as seguintes exigências, cumulativamente:

13.4.1. Certidão de regularidade com a Seguridade Social;

13.4.2. Certidão de regularidade com o FGTS;

13.4.3. Certidão de regularidade com a Fazenda Federal;

13.4.4. Certidão Negativa de Débitos Trabalhistas;

13.4.5. Certidão de regularidade com a Fazenda Estadual e Municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da Lei.

13.5 Os documentos de cobrança deverão ser entregues pela empresa CONTRATADA, no Setor de Protocolo do Superior Tribunal Militar.

Caso o objeto contratado seja faturado em desacordo com as disposições previstas no Edital e neste Termo de Referência ou sem a observância das formalidades legais pertinentes, a licitante vencedora deverá emitir e apresentar novo documento de cobrança, não configurando atraso no pagamento.

13.6. Após o atesto do documento de cobrança, que deverá ocorrer no prazo de até 05 (cinco) dias úteis contado do seu recebimento, o responsável deverá encaminhá-lo para pagamento.

13.7. Nos casos de eventuais atrasos de pagamento, desde que a Contratada não tenha concorrido de Alguma forma para o fato, a atualização financeira devida, entre a data que deveria ser efetuado o pagamento e a data correspondente ao efetivo pagamento, será calculada da seguinte forma, devendo a atualização prevista nesta condição ser incluída em nota fiscal a ser apresentada posteriormente:

AF = I x N x VP , onde:

AF = atualização financeira devida;

I = 0,0001644 (índice de atualização dia);

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

VP = valor do pagamento devido.

14. PROPRIEDADE, SIGILO E RESTRIÇÕES

14.1 Direito de propriedade

14.1.1. Os produtos e marcas objetos do presente Termo de Referência permanecem sob a titularidade de seus fabricantes/distribuidores por toda a extensão do período de duração do contrato, nos termos da Lei Nº 9.610 de 19 de fevereiro de 1998.

14.2. Condição de manutenção de sigilo

14.2.1. A CONTRATADA deverá tratar como confidenciais e zelar pelo sigilo de todos os dados, informações ou documentos que tomar conhecimento em decorrência do objeto desta contratação, bem como deverá submeter-se às normas e políticas de segurança do STM, devendo orientar seus empregados e/ou prepostos nesse sentido, sob pena de responsabilidade civil, penal e administrativa.

14.2.2. A CONTRATADA deverá assumir responsabilidade sobre todos os possíveis danos físicos e/ou materiais causados ao Órgão ou a terceiros, advindos de imperícia, negligência, imprudência ou desrespeito às normas de segurança.

14.2.3. A CONTRATADA deverá solicitar autorização formal da CONTRATANTE para a divulgação de quaisquer informações decorrentes da contratação ou da execução das atividades do contrato.

14.2.4. É vedada a veiculação de publicidade acerca do contrato, salvo se houver prévia autorização da CONTRATANTE.

14.2.5 A CONTRATADA estará sujeita às penalidades administrativas, civis e penais pelo descumprimento da obrigação assumida.

15. MECANISMOS FORMAIS DE COMUNICAÇÃO

Sempre que exigir-se, a comunicação entre o representante do STM e a Fornecedora deverá ser formal, considerando-se como documentos formais, além de documentos do tipo Ofício, as comunicações por correio eletrônico.

16. ADEQUAÇÃO ORÇAMENTÁRIA

A despesa ocorrerá à conta de dotação consignada à Justiça Militar da União pela Lei Orçamentária para o exercício de 2020, Encargo do Plano de Ação: **Solução de Segurança da Informação - Suporte e Garantia - MTGI**; Programa de Trabalho: MTGI; Natureza de despesa: 3.3.90.40; mediante emissão de nota de empenho.

17. SANÇÕES ADMINISTRATIVAS

Definidas pela SEPAD

18. MODALIDADE E TIPO DE LICITAÇÃO

18.1. Por se tratar de contratação de serviços comuns, nos termos do parágrafo único do art. 1º da Lei nº 10.520/02, o certame licitatório será realizado na modalidade Pregão, em sua forma eletrônica, do tipo menor preço global, de acordo com a Lei Federal nº 10.520/2002 e com os Decretos nºs 5.450/2005 subsidiariamente pela Lei n° 8.666/1993.

19. ADJUDICAÇÃO

Para efeito de adjudicação do objeto, será considerado o MENOR PREÇO GLOBAL, uma vez que a solução a ser fornecida é componente de uma única solução de TI, a qual não pode ser desmembrada sem que haja perda de produtividade e economia de escala.

20. GARANTIA DO CONTRATO

20.1. A Contratada prestará garantia destinada a assegurar a plena execução do contrato, no valor de R$, correspondente a 5% (cinco por cento) do valor do instrumento contratual, nos termos do art. 56 da Lei n.º 8.666/1993, em uma das seguintes modalidades:

20.1.1. caução em dinheiro ou títulos da dívida pública, devendo estes ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda;

20.1.2. seguro-garantia; ou

20.1.3. fiança bancária, devendo esta ser emitida por instituições autorizadas pelo Banco Central do Brasil, conforme entendimento previsto no Acórdão n° 2467/2017 – TCU/Plenário.

20.2. A Contratada deverá efetivar a prestação da garantia e apresentar o comprovante respectivo ao Fiscal do contrato no prazo de 30 (trinta) dias corridos, a contar da assinatura do contrato, sob pena de aplicação de multa moratória de 0,3% sobre o valor da garantia, por dia de atraso, limitado a 30 dias.

20.3. O atraso superior a 30 dias autoriza o Contratante a promover, discricionariamente, sem prejuízo das demais sanções cabíveis:

20.3.1. a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666/1993.

20.4. O valor da garantia não poderá ser decrescente em função da execução gradual do contrato, nem poderá a garantia estar condicionada a elementos externos à relação entre o Contratante e a Contratada.

20.5. Se a garantia for prestada na modalidade caução, a Contratada deverá:

20.5.1. caso a opção seja pela prestação em dinheiro, o respectivo depósito deverá ser feito na Caixa Econômica Federal (CEF), tendo como beneficiário o Contratante e como caucionário a Contratada; ou

20.5.2. caso a opção seja pela utilização de títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

20.6. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do art. 827 do Código Civil.

20.7. Se a garantia for prestada na modalidade de Seguro-Garantia, deverá ser observada a forma prevista na Circular nº 477, de 30 de setembro de 2013, da Superintendência de Seguros Privados (SUSEP).

20.8. A Contratada obriga-se a apresentar garantia complementar ou substitutiva da original, nos seguintes casos:

20.8.1. alteração do valor do contrato ou prorrogação de sua vigência, devendo ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação, a contar da assinatura do Termo Aditivo; ou

20.8.2. utilização do valor da garantia, total ou parcialmente, por qualquer motivo, a contar da data em que foi notificada.

20.9. A Contratada deverá efetivar a prestação da garantia complementar ou substitutiva prevista no item 8 e apresentar o comprovante respectivo ao Fiscal do contrato no prazo de 30 (trinta) dias corridos, sob pena de aplicação de multa moratória de 0,3% sobre o valor a ser complementado ou reposto, por dia de atraso, limitado a 30 dias.

20.10. O atraso superior a 30 dias, na prestação da garantia complementar ou substitutiva prevista no item 10, autoriza o Contratante a discricionariamente promover, sem prejuízo das demais sanções cabíveis:

20.10.1. a rescisão do contrato por descumprimento ou cumprimento irregular de suas cláusulas conforme dispõem os incisos I e II do art. 78 da Lei nº 8.666/1993.

20.11. Será considerada extinta a garantia:

20.11.1. com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do Contratante (Administração), mediante termo circunstanciado, de

que a Contratada cumpriu todas as cláusulas do contrato;

20.11.2. no prazo de 03 (três) meses após o término da vigência do contrato, caso o Contratante não comunique a ocorrência de sinistros, quando o prazo será ampliado, nos termos da comunicação.

21. VISTORIA

21.1. A Licitante poderá realizar Vistoria Técnica onde obterá a Declaração de Vistoria, expedida pelo STM, comprovando que tomou ciência dos serviços, características, condições especiais e dificuldades que possam existir na execução dos trabalhos, admitindo-se, consequentemente, como certo o prévio e total conhecimento dos serviços.

21.1.1. A visita técnica deverá ocorrer por horário marcado, e deverá ser agendada pela Licitante junto à COTEC, através do telefone 61 3313-9422, ou pelo email cotec@stm.jus.br,até o dia útil anterior à abertura da sessão.

22. VIGÊNCIA CONTRATUAL

22.1. O contrato decorrente deste Termo de Referência terá vigência por 30 (trinta) meses consecutivos, a partir da data de sua assinatura, podendo ser prorrogado por igual período, até o limite de 60 (sessenta) meses a critério das partes e mediante termo aditivo, observado o art. 57, II, da Lei no 8.666/1993.

22.2. Esse prazo de 30 (trinta) meses foi estipulado de modo a permitir as empresas realizarem a amortização dos equipamentos sem que os preços dos serviços sejam onerados além do necessário para a equalização dos investimentos efetuados.

22.4. Caso as partes não se interessem pela prorrogação do contrato, deverão manifestar sua vontade, no mínimo, 120 (cento e vinte) dias antes do término da vigência contratual.

23. REAJUSTE

23.1. Poderá haver reajuste anual de preços para as parcelas do contrato, de acordo com o Índice Geral de Preços de Mercado (IGPM), da Fundação Getúlio Vargas, ou outro índice que venha a ser adotado pelo Governo Federal, em substituição àquele, observado o interregno mínimo de um ano a partir da data da proposta:

23.1.1. o pedido de reajuste de preços deverá ocorrer antes da assinatura do termo de prorrogação contratual, sob pena de preclusão.

23.2 Para efeito de cálculo dos reajustes será utilizada a seguinte fórmula:

$$R = V \frac{I - IO}{IO}, \text{ onde:}$$

R = valor do reajustamento procurado;

V = valor contratual do serviço;

I = valor do índice relativo ao mês do reajuste, conforme definido no contrato;

IO = valor do índice inicial, correspondente ao mês da apresentação da proposta.

23.3 Por ocasião do pedido de reajuste, caberá à Contratada apresentar planilha dos cálculos, de acordo com fórmula do item **24.2**.

23.4 Caberá à Contratada, por ocasião do reajustamento de preços, apresentar faturas distintas, sendo uma correspondente aos preços iniciais contratados e outra, suplementar, relativa ao valor do reajustamento devido e pactuado pelas partes.

23.5 Ocorrendo o primeiro reajuste, os subsequentes só poderão ocorrer obedecendo ao prazo mínimo de um ano, a contar do início dos efeitos do último reajuste.

23.6 O reajuste de que trata o Item **23.1** poderá sofrer alteração posterior, total ou parcial, decorrente da adoção, pelo Governo Federal, de medidas ou normas financeiras com força de lei.

24. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

24.1. A Equipe de Planejamento desta contratação é composta pelos servidores Wilson Marques de Souza Filho (Integrante Demandante); Marcio Coelho Marques (titular), Claudio de Oliveira Melo (substituto) e; Luis Gustavo Costa Reis (titular) -Ubiratã Muniz da Silva (substituto).

24.2. A indicação do Integrante Administrativo consta do Documento de Oficialização da Demanda – DOD, de acordo com o inc. III, do § 5º, do art. 12, da Resolução nº 182, de 17 de outubro de 2013, do Conselho Nacional de Justiça.

24.3. A Equipe de Planejamento da Contratação foi instituída pelo Senhor Diretor-Geral, em conformidade com o inc. IV, do § 7º, do art. 12, da mesma Resolução.

25. EQUIPE DE APOIO À CONTRATAÇÃO

A Equipe de Apoio à Contratação é composta pelos integrantes da Equipe de Planejamento da Contratação e tem como finalidade subsidiar a Área de Licitações em suas dúvidas, respostas aos questionamentos, recursos e impugnações, bem como na análise e julgamento das propostas das licitantes (redação dada pelo inc. XI, do art. 2º, da Resolução nº 182/13, do CNJ).

26. FUNDAMENTO LEGAL

A elaboração deste Termo de Referência fundamenta-se no disposto na Lei nº 10.520, de 17 de julho de 2002, nos Decretos nº 5.450, de 31 de maio de 2005, e 7.892, de 23 de janeiro de 2013, na Resolução nº 182, de 17 de outubro de 2013, do Conselho Nacional de Justiça, e, subsidiariamente, na Lei nº 8.666, de 21 de junho de 1993.

27. ESTUDOS PRELIMINARES

São partes integrantes deste Termo de Referencia os Estudos Preliminares 1874271, 1838729, 1873230 e 1838731.

EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO		
Em cumprimento ao exposto no § 1º do art. 13 da Resolução nº 182, de 17 de outubro de 2013, do Conselho Nacional de Justiça, a Equipe de Planejamento da Contratação submete os Estudos Preliminares e o Termo de Referência à aprovação do Diretor de Tecnologia da Informação, titular da Área Demandante.		
INTEGRANTE TÉCNICO	**INTEGRANTE DEMANDANTE**	**INTEGRANTE ADMINISTRATIVO**
Marcio Coelho Marques (titular) Claudio de Oliveira Melo (substituto)	Wilson Marques de Souza Filho	Luis Gustavo Costa Reis (titular) - Ubiratã Muniz da Silva (substituto)

Documento assinado eletronicamente por **WILSON MARQUES DE SOUZA FILHO**, **COORDENADOR DE TECNOLOGIA**, em 16/10/2020, às 18:06 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **IANNE CARVALHO BARROS**, **DIRETOR DE TECNOLOGIA DA INFORMAÇÃO**, em 16/10/2020, às 18:17 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARCIO COELHO MARQUES**, **SUPERVISOR(A) DA SEÇÃO DE ADMINISTRAÇÃO E GERÊNCIA DE REDES E SEGURANÇA DA INFORMAÇÃO**, em 16/10/2020, às 19:04 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **UBIRATA MUNIZ DA SILVA**, **INTEGRANTE ADMINISTRATIVO**, em 19/10/2020, às 11:47 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site http://sei.stm.jus.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1971503** e o código CRC **A2775C3A**.

1971503v5