011094/21-00.82

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

TERMO DE REFERÊNCIA

1. OBJETO

Contratação de empresa especializada para renovação das licenças do Antivírus para solução Kaspersky Endpoint Security for Business Advanced, com direito a atualizações e treinamento.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

Considerando que já existe em nosso parque computacional cerca de 2000 equipamentos com licenças de antivírus Kaspersky, uma mudança para outro software de antivírus ocasionaria um gasto desnecessário de tempo e custos, visto que necessitaria de uma grande quantidade de técnicos para conseguir implantar a nova solução em todos os computadores da JMU.

Sabendo-se que estas estão em via de expiração, necessita-se renová-las a fim de garantir o mesmo nível de segurança já praticado, além de realizar um upgrade no nível de suporte, com a finalidade de conseguir um apoio mais específico para situações críticas, dado a importância de se manter uma rede mais segura.

Além do exposto, ter uma equipe bem treinada é de suma importância para a necessidade de administração do software, principalmente na resolução de problemas pontuais que eventualmente venham a surgir, e possam ser resolvidos sem a necessidade de acionamento do suporte técnico. Diante do exposto, sabendo-se que é de praxe comercial que a mesma empresa que fornece as licenças, forneça também o serviço de suporte e o serviço de treinamento, e para evitarmos custos administrativos em fiscalizar diversas empresas, faz-se necessário que o objeto seja atendido em sua totalidade por uma única empresa.

Sendo assim, o emprego desta ferramenta de segurança possibilita monitorar e controlar o tráfego de dados que circula entre as redes internas e a Internet, garantindo a segurança e o bom funcionamento dos computadores da rede local (Intranet) contra ações de vírus e, ainda, permite a implantação de uma política de prevenção de riscos.

3. OBJETIVOS A SEREM ALCANÇADOS POR MEIO DA CONTRATAÇÃO

- Garantir que a DITIN implemente nível adequado de segurança da informação, no que tange às ameaças provenientes de vírus, antispyware e outos malwares;
- Garantir que as informações utilizadas em suas atividades de trabalho estejam protegidas contra ataques maliciosos;
- Proteger com acesso em tempo real as informações sobre malware, phishing, spam, vazamento e roubo de dados.
- Controlar o acesso de usuários e de outros aplicativos a processos, pastas e arquivos específicos. Realizar análise do aplicativo, controle de processos, controle de acesso ao registro e arquivo, bem como controle de DLL e chaves de registro.
- Controlar quais periféricos que podem ser conectados ao computador e como eles são usados.
- Aumentar a confidencialidade, integridade e disponibilidade das informações da DITIN;
- Capacitação e qualificação da equipe de TI da DITIN.

4. MODALIDADE E TIPO DE LICITAÇÃO

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.

5. PARCELAMENTO DO OBJETO E ADJUDICAÇÃO

Considerando o disposto no §1º do artigo 23 da lei 8666/93 onde as obras, serviços e compras efetuadas pela Administração serão divididas em tantas parcelas quantas se comprovarem técnica e economicamente viáveis. Os itens especificados estão fortemente integrados entre si, sendo necessária sua execução por uma mesma empresa para que não se configure conflito de competências quando da solicitação e/ou cobrança das atividades realizadas, além de reduzir a complexidade da gestão do contrato, reduzir seus custos de administração e reduzir os riscos operacionais e conflitos. Desta forma, os itens objeto do presente termo de referência serão agrupados em um único lote.

Assim sendo, a adjudicação será integralmente realizada a um único fornecedor.

6. ALINHAMENTO ENTRE A CONTRATAÇÃO DE FORNECIMENTO E O PLANEJAMENTO ESTRATÉGICO DA JMU

A análise, está em consonância com a necessidade de prover uma solução capaz de atender as demandas da JMU, de forma a atingir

os objetivos propostos por este projeto, em especial possibilitar a realização de análises em tempo exíguo para tomadas de decisão, viabilizando inclusive emissão de relatórios gerenciais e ampliação do conhecimento sistêmico organizacional.

Objetivo: Otimizar a infraestrutura e as soluções de tecnologia da informação e comunicação (TIC) para atender as necessidades da JMU.

Estratégia: Compatibilizar a infraestrutura e as soluções de TIC às necessidades da JMU.

Iniciativa: Aperfeiçoar a gestão e a proteção de dados e informações.

7. ESTUDOS

Os Estudos Técnicos Preliminares (Documento de Oficialização da Demanda – DOD, a Análise de Viabilidade da Contratação, a Sustentação do Contrato, a Estratégia para a Contratação e a Análise de Riscos) foram realizados pela equipe de Planejamento de conforme determinado o art. 12, § 1º, da Resolução nº 182/13, do CNJ.

8. RELAÇÃO ENTRE A DEMANDA PREVISTA E OS SERVIÇOS A SEREM CONTRATADOS

ITEM	QUANTIDADE	DESCRIÇÃO
1	2000 unidades	Renovação e upgrade de licenças – Kaspersky endpoint security for business advanced, pelo período de 36 meses.
2	36 meses	Serviço de Suporte Técnico com a Licitante para o item 1 (SOFTWARE KASPERSKY) por 36 meses
3	1 unidade	Serviço de Treinamento

9. ESPECIFICAÇÃO TÉCNICA

9.1.Requisitos do Demandante

ITEM	QUANTIDADE	DESCRIÇÃO
1	2000 unidades	Renovação e upgrade de licenças – Kaspersky endpoint security for business advanced, pelo período de 36 meses.

2	36 meses	Serviço de Suporte Técnico com a Contratante para o item 1 (SOFTWARE KASPERSKY) por 36 meses
3	1 unidade	Serviço de Treinamento

9.2. Requisitos Técnicos

9.2.1. ITEM 01 - Kaspersky endpoint security for business advanced

9.2.1.1. Características Gerais

9.2.1.1.1. Todas as licenças fornecidas terão validade de 36 (trinta e seis) meses para atualizações inerentes ao produto;

9.2.1.1.2. Deverão ser disponibilizadas atualizações tanto da base de dados do antivírus, quanto do software;

9.2.1.1.3. As atualizações deverão ser disponibilizadas através de site na Internet, ou através do próprio software;

9.2.1.1.4. Durante o período de validade da licença deverá ser permitida a atualização da solução para as versões mais recentes, sem ônus adicional para a CONTRATADA além daquele já cotado na proposta;

9.2.1.2. Servidor de Administração e Console Administrativa

9.2.1.2.1. Compatibilidade:

9.2.1.2.1.1. Microsoft Windows Server 2012 (Todas edições x64);

9.2.1.2.1.2. Microsoft Windows Server 2012 R2 (Todas edições x64);

9.2.1.2.1.3. Microsoft Windows Server 2016 x64;

9.2.1.2.1.4. Microsoft Windows Server 2019 x64;

9.2.1.2.1.5. Microsoft Windows 8 Professional / Enterprise x64;

9.2.1.2.1.6. Microsoft Windows 8.1 Professional / Enterprise x32;

9.2.1.2.1.7. Microsoft Windows 8.1 Professional / Enterprise x64;

9.2.1.2.1.8. Microsoft Windows 10 (Professional / Enterprise / Education x32);

9.2.1.2.1.9. Microsoft Windows 10 (Professional / Enterprise / Education x64).

9.2.1.2.2. Características:

9.2.1.2.2. 1. A console deve ser acessada via WEB (HTTPS) ou MMC;

9.2.1.2.2.2. Console deve ser baseada no modelo cliente/servidor;

9.2.1.2.2.3. Compatibilidade com Windows Failover Clustering ou outra solução de alta disponibilidade;

9.2.1.2.2.4. Deve permitir a atribuição de perfis para os administradores da Solução de Antivírus;

9.2.1.2.2.5. Deve permitir incluir usuários do AD para logarem na console de administração;

9.2.1.2.2.6. Console deve ser totalmente integrada com suas funções e módulos caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, Patch management e MDM;

9.2.1.2.2.7. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

9.2.1.2.2.8. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, login script e/ou GPO de Active Directory;

9.2.1.2.2.9. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

9.2.1.2.2.10. Deve armazenar histórico das alterações feitas em políticas;

9.2.1.2.2.11. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;

9.2.1.2.2.12. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;

9.2.1.2.2.13. A solução de gerencia deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

9.2.1.2.2.14. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

9.2.1.2.2.15. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

9.2.1.2.2.16. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;

9.2.1.2.2.17. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

9.2.1.2.2.18. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;

9.2.1.2.2.19. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

9.2.1.2.2.20. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;

9.2.1.2.2.21. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

9.2.1.2.2.22. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

9.2.1.2.2.23. A comunicação entre o cliente e o servidor de administração deve ser criptografada;

9.2.1.2.2.24. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

9.2.1.2.2.25. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

a) Nome do computador;

b) Nome do domínio;

c) Range de IP;

d) Sistema Operacional;

e) Máquina virtual.

9.2.1.2.2.26. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

9.2.1.2.2.27. Deve permitir, por meio da console de gerenciamento, extrair um artefato em quarentena de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

9.2.1.2.2.28. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

9.2.1.2.2.29. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

9.2.1.2.2.30. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

9.2.1.2.2.31. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;

9.2.1.2.2.32. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

9.2.1.2.2.33. Deve fornecer as seguintes informações dos computadores:

9.2.1.2.2.33.1. Se o antivírus está instalado;

9.2.1.2.2.33.2. Se o antivírus está iniciado;

9.2.1.2.2.33.3. Se o antivírus está atualizado;

9.2.1.2.2.33.4. Minutos/horas desde a última conexão da máquina com o servidor administrativo;

9.2.1.2.2.33.5. Minutos/horas desde a última atualização de vacinas;

9.2.1.2.2.33.6. Data e horário da última verificação executada na máquina;

9.2.1.2.2.33.7. Versão do antivírus instalado na máquina;

9.2.1.2.2.33.8. Se é necessário reiniciar o computador para aplicar mudanças;

9.2.1.2.2.33.9. Data e horário de quando a máquina foi ligada;

9.2.1.2.2.33.10. Quantidade de vírus encontrados (contador) na máquina;

9.2.1.2.2.33.11. Nome do computador;

9.2.1.2.2.33.12. Domínio ou grupo de trabalho do computador;

9.2.1.2.2.33.13. Data e horário da última atualização de vacinas;

9.2.1.2.2.33.14. Sistema operacional com Service Pack;

9.2.1.2.2.33.15. Quantidade de processadores;

9.2.1.2.2.33.16. Quantidade de memória RAM;

9.2.1.2.2.33.17. Usuário(s) logado(s) naquele momento, com informações de contato (caso disponíveis no Active Directory);

9.2.1.2.2.33.18. Endereço IP;

9.2.1.2.2.33.19. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;

9.2.1.2.2.33.20. Atualizações do Windows Updates instaladas;

9.2.1.2.2.33.21. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;

9.2.1.2.2.33.22. Vulnerabilidades de aplicativos instalados na máquina;

9.2.1.2.2.34. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

9.2.1.2.2.35. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

9.2.1.2.2.35.1. Alteração de Gateway Padrão;

9.2.1.2.2.35.2. Alteração de subrede;

9.2.1.2.2.35.3. Alteração de domínio;

9.2.1.2.2.35.4. Alteração de servidor DHCP;

9.2.1.2.2.35.5. Alteração de servidor DNS;

9.2.1.2.2.35.6. Alteração de servidor WINS;

9.2.1.2.2.35.7. Alteração de subrede;

9.2.1.2.2.35.8. Resolução de Nome;

9.2.1.2.2.35.9. Disponibilidade de endereço de conexão SSL;

9.2.1.2.2.36.Capacidade de configurar políticas móveis para que quando um computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

9.2.1.2.2.37.Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

9.2.1.2.2.38. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

9.2.1.2.2.39. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

9.2.1.2.2.40. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

9.2.1.2.2.41. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

9.2.1.2.2.42. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;

9.2.1.2.2.43. Capacidade de gerar traps SNMP para monitoramento de eventos;

9.2.1.2.2.44. Capacidade de enviar e-mails para contas específicas em caso de algum evento;

9.2.1.2.2.45. Listar em um único local, todos os computadores não gerenciados na rede;

9.2.1.2.2.46. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;

9.2.1.2.2.47. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente

9.2.1.2.2.48. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;

9.2.1.2.2.49. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

9.2.1.2.2.50. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo porém sem comprometer o desempenho do computador;

9.2.1.2.2.51. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a

utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

9.2.1.2.2.52. Permitir fazer uma verificação rápida ou detalhada de um dispositivo removível assim que conectado no computador, podendo configurar a capacidade máxima em GB da verificação;

9.2.1.2.2.53. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;

9.2.1.2.2.54. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

9.2.1.2.2.55. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

a) Nome do vírus;

b) Nome do arquivo infectado;

c) Data e hora da detecção;

d) Nome da máquina ou endereço IP;

e) Ação realizada.

9.2.1.2.2.56. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

9.2.1.2.2.57. Capacidade de listar updates nas máquinas com o respectivo link para download

9.2.1.2.2.58. Deve criar um backup de todos arquivos deletados em computadores para que possa ser restaurado através de comando na Console de administração;

9.2.1.2.2.59. Deve ter uma quarentena na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;

9.2.1.2.2.60. Capacidade de realizar resumo de hardware de cada máquina cliente;

9.2.1.2.2.61. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

9.2.1.3. Estações Windows

9.2.1.3.1. Compatibilidade:

9.2.1.3.1.1. Microsoft Windows 7 SP1 Professional/Enterprise/Ultimate;

9.2.1.3.1.2. Microsoft Windows 8 Professional/Enterprise;

9.2.1.3.1.3. Microsoft Windows 8.1 Professional/Enterprise;

9.2.1.3.1.4. Microsoft Windows 10 Professional/Enterprise.

9.2.1.3.2. Características:

9.2.1.3.2.1. Deve prover as seguintes proteções:

9.2.1.3.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

9.2.1.3.2.1.2. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);

9.2.1.3.2.1.3. Antivírus de E-mail (módulo para verificação de e-mails recebidos e enviados, assim como seus anexos);

9.2.1.3.2.1.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;

9.2.1.3.2.1.5. Firewall com IDS;

9.2.1.3.2.1.6. Autoproteção (contra-ataques aos serviços/processos do antivírus);

9.2.1.3.2.1.7. Controle de dispositivos externos;

9.2.1.3.2.1.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;

9.2.1.3.2.1.9. Controle de acesso a sites por horário;

9.2.1.3.2.1.10. Controle de acesso a sites por usuários;

9.2.1.3.2.1.11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;

9.2.1.3.2.1.12. Controle de execução de aplicativos;

9.2.1.3.2.1.13. Controle de vulnerabilidades do Windows e dos aplicativos instalados

9.2.1.3.2.2. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

9.2.1.3.2.3.As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

9.2.1.3.2.4. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

9.2.1.3.2.5. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

9.2.1.3.2.6. Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

9.2.1.3.2.7. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

9.2.1.3.2.8. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

9.2.1.3.2.9. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

9.2.1.3.2.10. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;

9.2.1.3.2.11. Capacidade de verificar somente arquivos novos e alterados;

9.2.1.3.2.12. Capacidade de verificar objetos usando heurística;

9.2.1.3.2.13. Capacidade de agendar uma pausa na verificação;

9.2.1.3.2.14. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;

9.2.1.3.2.15. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

9.2.1.3.2.16. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

9.2.1.3.2.16.1. Perguntar o que fazer, ou;

9.2.1.3.2.16.2. Bloquear acesso ao objeto;

9.2.1.3.2.16.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

9.2.1.3.2.16.2.2. Caso positivo de desinfecção:

9.2.1.3.2.16.2.2.1. Restaurar o objeto para uso;

9.2.1..3.2.16.2.3. Caso negativo de desinfecção:

9.2.1..3.2.16.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador

9.2.1..3.2.17. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

9.2.1..3.2.18. Capacidade de verificar e-mails recebidos e enviados nos protocolos POP3, POP3S, IMAP, NNTP, SMTP e MAPI;

9.2.1..3.2.19. Capacidade de verificar links inseridos em e-mails contra phishings;

9.2.1..3.2.20. Capacidade de verificar tráfego nos browsers: Internet Explorer, Firefox, Google Chrome e Opera;

9.2.1..3.2.21. Capacidade de verificação de corpo e anexos de e-mails usando heurística;

9.2.1..3.2.22. O antivírus de e-mail, ao encontrar um objeto potencialmente perigoso, deve:

9.2.1..3.2.22.1. Perguntar o que fazer, ou;

9.2.1..3.2.22.2. Bloquear o e-mail;

9.2.1..3.2.22.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

9.2.1.3.2.22.2.2. Caso positivo de desinfecção:

9.2.1.3.2.22.2.2.1. Restaurar o e-mail para o usuário;

9.2.1.3.2.22.2.3. Caso negativo de desinfecção:

9.2.1.3.2.22.2.3.1. Mover para quarentena ou apagar o objeto (de acordo com a configuração pré-estabelecida pelo administrador);

9.2.1.3.2.23. Caso o e-mail conter código que parece ser, mas não é definitivamente malicioso, o mesmo deve ser mantido em quarentena;

9.2.1.3.2.24. Possibilidade de verificar somente e-mails recebidos ou recebidos e enviados;

9.2.1.3.2.25. Capacidade de filtrar anexos de e-mail, apagando-os ou renomeando-os de acordo com a configuração feita pelo administrador;

9.2.1.3.2.26. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc), usando heurísticas;

9.2.1.3.2.27. Deve ter suporte total ao protocolo Ipv6;

9.2.1.3.2.28. Capacidade de alterar as portas monitoradas pelos módulos de Web e E-mail;

9.2.1.3.2.29. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

9.2.1.3.2.29.1. Perguntar o que fazer, ou;

9.2.1.3.2.29.2. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

9.2.1.3.2.29.3. Permitir acesso ao objeto;

9.2.1.3.2.30. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

9.2.1.3.2.30.1. Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

9.2.1.3.2.30.2. Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;

9.2.1.3.2.31. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;

9.2.1.3.2.32. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando-as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

9.2.1.3.2.33. Deve possuir módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;

9.2.1.3.2.34. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

9.2.1.3.2.35. Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (http://www.antiphishing.org/);

9.2.1.3.2.36. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

9.2.1.3.2.37. Deve possuir módulo IDS (Intrusion Detection System) para proteção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas;

9.2.1.3.2.38. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

9.2.1.3.2.38.1.Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

9.2.1.3.2.38.2. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

9.2.1.3.2.39. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

9.2.1.3.2.39.1. Discos de armazenamento locais;

9.2.1.3.2.39.2. Armazenamento removível;

9.2.1.3.2.39.3. Impressoras;

9.2.1.3.2.39.4. CD/DVD;

9.2.1.3.2.39.5. Drives de disquete;

9.2.1.3.2.39.6. Modems;

9.2.1.3.2.39.7. Dispositivos de fita;

9.2.1.3.2.39.8. Dispositivos multifuncionais;

9.2.1.3.2.39.9. Leitores de smart card;

9.2.1.3.2.39.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile, etc);

9.2.1.3.2.39.11. Wi-Fi;

9.2.1.3.2.39.12. Adaptadores de rede externos;

9.2.1.3.2.39.13. Dispositivos MP3 ou smartphones;

9.2.1.3.2.39.14. Dispositivos Bluetooth;

9.2.1.3.2.39.15. Câmeras e Scanners.

9.2.1.3.2.40. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;

9.2.1.3.2.41. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

9.2.1.3.2.42. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

9.2.1.3.2.43. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos,

etc.

9.2.1.3.2.44. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

9.2.1.3.2.45. Capacidade de limitar a execução de aplicativos por hash MD5 ou SHA256, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);

9.2.1.3.2.46. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

9.2.1.3.2.46.1. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

9.2.1.3.2.46.2. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

9.2.1.3.2.47. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

9.2.1.3.2.48. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

9.2.1.3.2.49. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;

9.2.1.3.2.50. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

9.2.1.3.2.51. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

9.2.1.3.2.52. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

9.2.1.3.2.53. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

9.2.1.3.2.54. Capacidade de integração com o Windows Defender Security Center.

9.2.1.3.2.55. Capacidade de integração com a Antimalware Scan Interface (AMSI).

9.2.1.3.2.56 Capacidade de detecção de arquivos maliciosos executados em Subsistema Windows para Linux (WSL).

9.2.1.4. Estações Mac OS X

9.2.1.4.1. Compatibilidade:

9.2.1.4.1.1. OS X 10.9 (Mavericks);

9.2.1.4.1.2.. OS X 10.10 (Yosemite);

9.2.1.4.1.3. OS X 10.11 (El Capitan);

9.2.1.4.1.4. macOS 10.12 (Sierra)

9.2.1.4.1.5. masOS 10.13 (High Sierra)

9.2.1.4.1.6. macOS 10.14 (Mojave)

9.2.1.4.1.7. macOS 10.15 (Catalina)

9.2.1.4.1.8. macOS 11.0 (Big Sur)

9.2.1.4.2. Características:

9.2.1.4.2.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

9.2.1.4.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possíbilidade de analisar endereços https;

9.2.1.4.2.3. Possuir módulo de bloqueio á ataques na rede;

9.2.1.4.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;

9.2.1.4.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;

9.2.1.4.2.6. Capacidade de controle de acesso a sites por endereços específicos e por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;

9.2.1.4.2.7. Possibilidade de importar uma chave no pacote de instalação;

9.2.1.4.2.8. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

9.2.1.4.2.9. Deve possuir suportes a notificações utilizando o Growl;

9.2.1.4.2.10. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

9.2.1.4.2.11. Capacidade de voltar para a base de dados de vacina anterior;

9.2.1.4.2.12. Capacidade de varrer a quarentena automaticamente após cada atualização de vacinas;

9.2.1.4.2.13. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: "Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

9.2.1.4.2.14. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

9.2.1.4.2.15. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

9.2.1.4.2.16. Capacidade de verificar somente arquivos novos e alterados;

9.2.1.4.2.17. Capacidade de verificar objetos usando heurística;

9.2.1.4.2.18. Capacidade de agendar uma pausa na verificação;

9.2.1.4.2.19. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

9.2.1.4.2.19.1. Perguntar o que fazer, ou;

9.2.1.4.2.19.2. Bloquear acesso ao objeto;

9.2.1.4.2.19.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

9.2.1.4.2.19.2.2. Caso positivo de desinfecção:

9.2.1.4.2.19.2.2.1. Restaurar o objeto para uso;

9.2.1.4.2.19.2.3. Caso negativo de desinfecção:

9.2.1.4.2.19.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

9.2.1.4.2.20. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

9.2.1.4.2.21. Capacidade de verificar arquivos de formato de email;

9.2.1.4.2.22. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

9.2.1.4.2.23. Capacidade de ser instalado, removido e administrado pela mesma console central de gerenciamento.

9.2.1.5. Estações de trabalho Linux

9.2.1.5.1 Compatibilidade:

9.2.1.5.1.1. Plataforma 32-bits:

9.2.1.5.1.1.1. Ubuntu 16.04 LTS

9.2.1.5.1.1.2. Red Hat® Enterprise Linux® 6.7

9.2.1.5.1.1.3. CentOS-6.7

9.2.1.5.1.1.4. Debian GNU / Linux 9.4

9.2.1.5.1.2. Plataforma 64-bits:

9.2.1.5.1.2.1. Ubuntu 16.04 e 18.04 LTS

9.2.1.5.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0

9.2.1.5.1.2.3. CentOS-6.7, 7.2, 8.0

9.2.1.5.1.2.4. Debian GNU / Linux 9.4, 10.1

9.2.1.5.1.2.5. OracleLinux 7.3, 8

9.2.1.5.1.2.6. SUSE® Linux Enterprise Server 15

9.2.1.5.1.2.7. openSUSE® 15

9.2.1.5.1.2.8. Amazon Linux AMI

9.2.1.5.2. Características:

9.2.1.5.2.1. Deve prover as seguintes proteções:

9.2.1.5.2.2. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

9.2.1.5.2.3. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos;

9.2.1.5.2.4. Rastreamento de atividades típicas de ataques de rede no tráfego de rede;

9.2.1.5.2.5. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento;

9.2.1.5.2.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados;

9.2.1.5.2.7. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

9.2.1.5.2.8. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

9.2.1.5.2.9. Capacidade de criar exclusões por local, máscara e nome da ameaça;

9.2.1.5.2.10. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

9.2.1.5.2.11. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

9.2.1.5.2.12. Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;

9.2.1.5.2.13. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

9.2.1.5.2.13.1. Alta;

9.2.1.5.2.13.2. Média;

9.2.1.5.2.13.3. Baixa;

9.2.1.5.2.13.4. Recomendado;

9.2.1.5.2.14. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

9.2.1.5.2.15. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

9.2.1.5.2.16. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

9.2.1.5.2.17. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

9.2.1.5.2.18. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

9.2.1.5.2.19. Capacidade de verificar objetos usando heurística;

9.2.1.5.2.20. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

9.2.1.5.2.21. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

9.2.1.6. Servidores Windows

9.2.1.6.1. Compatibilidade:

9.2.1.6.1.1. Microsoft Windows Server 2008 R2 Standard / Enterprise / Datacenter x64 SP1;

9.2.1.6.1.2. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter SP2;

9.2.1.6.1.3. Microsoft Windows Server 2008 Standard / Enterprise / Datacenter x64 SP2;

9.2.1.6.1.4. Microsoft Windows Server 2012 Standard / Foundation / Essentials / Datacenter x64;

9.2.1.6.1.5. Microsoft Windows Server 2012 R2 Standard / Foundation / Essentials / Datacenter x64;

9.2.1.6.1.6. Microsoft Windows Server 2016;

9.2.1.6.1.7. Microsoft Windows Server 2019.

9.2.1.6.2. Características:

9.2.1.6.2.1. Deve prover as seguintes proteções:

9.2.1.6.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

9.2.1.6.2.1.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;

9.2.1.6.2.1.3. Capacidade de verificar o tráfego de entrada de rede em busca de atividades típicas de ataques à rede. Ao detectar uma tentativa de ataque à rede que tem como alvo o servidor, bloqueia a

atividade de rede do computador atacante.

9.2.1.6.2.1.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

9.2.1.6.2.2. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

9.2.1.6.2.3. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

9.2.1.6.2.4. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

9.2.1.6.2.4.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

9.2.1.6.2.4.2. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

9.2.1.6.2.4.3. Leitura de configurações;

9.2.1.6.2.4.4. Modificação de configurações;

9.2.1.6.2.4.5. Gerenciamento de Backup e Quarentena;

9.2.1.6.2.4.6. Visualização de relatórios;

9.2.1.6.2.4.7. Gerenciamento de relatórios;

9.2.1.6.2.4.8. Gerenciamento de chaves de licença;

9.2.1.6.2.4.9. Gerenciamento de permissões (adicionar/excluir permissões acima);

9.2.1.6.2.5. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

9.2.1.6.2.6. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede

9.2.1.6.2.7. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);

9.2.1.6.2.8. Capacidade de automaticamente pausar e não iniciar tarefas agendadas caso o servidor esteja em rodando com fonte ininterrupta de energia (uninterruptible Power supply – UPS);

9.2.1.6.2.9. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;

9.2.1.6.2.10. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

9.2.1.6.2.11. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

9.2.1.6.2.12. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

9.2.1.6.2.13. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

9.2.1.6.2.14. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

9.2.1.6.2.15. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

9.2.1.6.2.16. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

9.2.1.6.2.17. Capacidade de verificar somente arquivos novos e alterados;

9.2.1.6.2.18. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);

9.2.1.6.2.19. Capacidade de verificar objetos usando heurística;

9.2.1.6.2.20. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

9.2.1.6.2.21. Capacidade de agendar uma pausa na verificação;

9.2.1.6.2.22. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

9.2.1.6.2.23. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

9.2.1.6.2.23.1. Perguntar o que fazer, ou;

9.2.1.6.2.23.2. Bloquear acesso ao objeto;

9.2.1.6.2.23.2.1. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

9.2.1.6.2.23.2.2. Caso positivo de desinfecção:

9.2.1.6.2.23.2.2.1. Restaurar o objeto para uso;

9.2.1.6.2.23.2.3. Caso negativo de desinfecção:

9.2.1.6.2.23.2.3.1. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

9.2.1.6.2.24. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

9.2.1.6.2.25. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

9.2.1.6.2.26. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

9.2.1.6.2.27. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

9.2.1.6.2.28. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros

9.2.1.6.2.29. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

9.2.1.6.2.30. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

9.2.1.7. Servidores Linux

9.2.1.7.1. Compatibilidade:

9.2.1.7.1.1. Plataforma 32-bits:

9.2.1.7.1.1.1. Ubuntu 16.04 LTS

9.2.1.7.1.1.2. Red Hat® Enterprise Linux® 6.7

9.2.1.7.1.1.3. CentOS-6.7

9.2.1.7.1.1.4. Debian GNU / Linux 9.4

9.2.1.7.1.2. Plataforma 64-bits:

9.2.1.7.1.2.1. Ubuntu 16.04 e 18.04 LTS

9.2.1.7.1.2.2. Red Hat Enterprise Linux 6.7, 7.2, 8.0

9.2.1.7.1.2.3. CentOS-6.7, 7.2, 8.0

9.2.1.7.1.2.4. Debian GNU / Linux 9.4, 10.1

9.2.1.7.1.2.5. OracleLinux 7.3, 8

9.2.1.7.1.2.6. SUSE® Linux Enterprise Server 15

9.2.1.7.1.2.7. openSUSE® 15

9.2.1.7.1.2.8. Amazon Linux AMI

9.2.1.7.2. Características:

9.2.1.7.2.1. Deve prover as seguintes proteções:

9.2.1.7.2.1.1. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;

9.2.1.7.2.1.2. Capacidade de verificação de tráfego HTTP / HTTPS e FTP e detecção de phishing e endereços da web maliciosos;

9.2.1.7.2.1.3. Rastreamento de atividades típicas de ataques de rede no tráfego de rede;

9.2.1.7.2.1.4. Capacidade de monitorar atividades maliciosas no sistema operacional com base em comportamento;

9.2.1.7.2.1.5. Capacidade de proteger arquivos nos diretórios locais com acesso à rede por protocolos SMB / NFS contra criptografia maliciosa remota;

9.2.1.7.2.1.6. Capacidade de gerenciar o acesso do usuário a dispositivos instalados ou conectados ao computador (por exemplo, armazenamento removível, discos rígidos, leitores de cartão inteligente ou módulos Wi-Fi). Isso permite a proteção do computador contra infecções quando esses dispositivos são conectados e evita a perda ou vazamento de dados;

9.2.1.7.2.2. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

9.2.1.7.2.3. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

9.2.1.7.2.3.1. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

9.2.1.7.2.3.2. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

9.2.1.7.2.3.3. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

9.2.1.7.2.3.4. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados;

9.2.1.7.2.4. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

9.2.1.7.2.5. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

9.2.1.7.2.6. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

9.2.1.7.2.7. Capacidade de verificar objetos usando heurística;

9.2.1.7.2.8. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

9.2.1.7.2.9. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

9.2.1.7.2.10. Deve possuir módulo de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

9.2.1.8. Smartphones e tablets

9.2.1.8.1. Compatibilidade:

9.2.1.8.1.1. Dispositivos com os sistemas operacionais:

9.2.1.8.1.1.1. Android 4.2 – 11

9.2.1.8.1.1.2. iOS 10.0 – 14.0 ou iPadOS

9.2.1.8.2. Características:

9.2.1.8.2.1. Deve prover as seguintes proteções:

9.2.1.8.2.1.1. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

9.2.1.8.2.1.2. Proteção contra adware e autodialers;

9.2.1.8.2.1.3. Todos os objetos transmitidos usando conexões wireless (porta de infravermelho, Bluetooth) e mensagens EMS, durante sincronismo com PC e ao realizar download usando o browser;

9.2.1.8.2.1.4. Arquivos abertos no smartphone;

9.2.1.8.2.1.5. Programas instalados usando a interface do smartphone

9.2.1.8.2.1.6. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

9.2.1.8.2.2. Deverá isolar em área de quarentena os arquivos infectados;

9.2.1.8.2.3. Deverá atualizar as bases de vacinas de modo agendado;

9.2.1.8.2.4. Capacidade de desativar por política:

a) Wi-fi;

b) Câmera;

c) Bluetooth.

9.2.1.8.2.5. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

9.2.1.8.2.6. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

9.2.1.8.2.7. Deverá ter firewall pessoal (Android);

9.2.1.8.2.8. Capacidade de tirar fotos quando a senha for inserida incorretamente;

9.2.1.8.2.9. Capacidade de enviar comandos remotamente de:

a) Localizar;

b) Bloquear.

9.2.1.8.2.10. Capacidade de detectar Jailbreak em dispositivos iOS;

9.2.1.8.2.11. Capacidade de bloquear o acesso a site por categoria em dispositivos;

9.2.1.8.2.12. Capacidade de bloquear o acesso a sites phishing ou malicioso;

9.2.1.8.2.13. Capacidade de configurar White e blacklist de aplicativos;

9.2.1.8.2.14. Capacidade de localizar o dispositivo quando necessário;

9.2.1.8.2.15. Permitir atualização das definições quando estiver em “roaming”;

9.2.1.8.2.16. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

9.2.1.8.2.17. Deve permitir verificar somente arquivos executáveis;

9.2.1.8.2.18. Deve ter a capacidade de desinfectar o arquivo se possível;

9.2.1.8.2.19. Capacidade de agendar uma verificação;

9.2.1.8.2.20. Capacidade de enviar URL de instalação por e-mail;

9.2.1.8.2.21. Capacidade de fazer a instalação através de um link QRCode;

9.2.1.8.2.22. Capacidade de executar as seguintes ações caso a desinfecção falhe:

a) Deletar;

b) Ignorar;

c) Quarentenar;

d) Perguntar ao usuário.

9.2.1.9. Gerenciamento de dispositivos móveis (MDM)

9.2.1.9.1. Compatibilidade:

9.2.1.9.1.1. Android 4.2 – 11

9.2.1.9.1.2. iOS 10.0 – 14.0 ou iPadOS

9.2.1.9.2. Características:

9.2.1.9.2.1. Capacidade de aplicar políticas de ActiveSync através do servidor Microsoft Exchange;

9.2.1.9.2.2. Capacidade de ajustar as configurações de:

9.2.1.9.2.2.1. Sincronização de e-mail;

9.2.1.9.2.2.2. Uso de aplicativos;

9.2.1.9.2.2.3. Senha do usuário;

9.2.1.9.2.2.4. Criptografia de dados;

9.2.1.9.2.2.5. Conexão de mídia removível.

9.2.1.9.2.3. Capacidade de instalar certificados digitais em dispositivos móveis;

9.2.1.9.2.4. Capacidade de, remotamente, resetar a senha de dispositivos iOS;

9.2.1.9.2.5. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

9.2.1.9.2.6. Capacidade de, remotamente, bloquear um dispositivo iOS;

9.2.1.9.2.7. Deve permitir configurar horário para sincronização do dispositivo com a console de gerenciamento;

9.2.1.9.2.8. Permitir sincronização com perfil do “Touch Down”;

9.2.1.9.2.9. Capacidade de desinstalar remotamente o antivírus do dispositivo;

9.2.1.9.2.10. Deve permitir fazer o upgrade do antivírus de forma remota sem a necessidade de desinstalar a versão atual;

9.2.1.9.2.11. Deve permitir criar perfis de políticas para out-of-office no caso de BYOD.

9.2.1.10. Criptografia

9.2.1.10.1. Compatibilidade

9.2.1.10.1.1. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;

9.2.1.10.1.2. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;

9.2.1.10.1.3. Microsoft Windows 7 Professional SP1 ou superior x86/x64;

9.2.1.10.1.4. Microsoft Windows 8 Enterprise x86/x64;

9.2.1.10.1.5. Microsoft Windows 8 Pro x86/x64;

9.2.1.10.1.6. Microsoft Windows 8.1 Pro x86/x64;

9.2.1.10.1.7. Microsoft Windows 8.1 Enterprise x86/x64;

9.2.1.10.1.8. Microsoft Windows 10 Enterprise x86/x64;

9.2.1.10.1.9. Microsoft Windows 10 Pro x86/x64.

9.2.1.10.2. Características

9.2.1.10.2.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

9.2.1.10.2.2. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

9.2.1.10.2.3. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

9.2.1.10.2.4. Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;

9.2.1.10.2.5. Permitir criar vários usuários de autenticação pré-boot;

9.2.1.10.2.6. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

9.2.1.10.2.7. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

9.2.1.10.2.8. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

9.2.1.10.2.9. Criptografar todos os arquivos individualmente;

9.2.1.10.2.10. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

9.2.1.10.2.11. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

9.2.1.10.2.12. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente. Nesta modalidade, os arquivos devem estar acessíveis para todas as máquinas gerenciadas pela mesma console de maneira transparente para os usuários;

9.2.1.10.2.13. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

9.2.1.10.2.14. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

9.2.1.10.2.15. Verifica compatibilidade de hardware antes de aplicar a criptografia;

9.2.1.10.2.16. Possibilita estabelecer parâmetros para a senha de criptografia;

9.2.1.10.2.17. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

9.2.1.10.2.18. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo

9.2.1.10.2.19. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

9.2.1.10.2.20. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

9.2.1.10.2.21. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;

9.2.1.10.2.22. Permite criar um grupo de extensões de arquivos a serem criptografados;

9.2.1.10.2.23. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

9.2.1.10.2.24. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.

9.2.1.10.2.25. Capacidade de deletar arquivos de forma segura após a criptografia;

9.2.1.10.2.26. Capacidade de criptografar somente o espaço em disco utilizado;

9.2.1.10.2.27. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;

9.2.1.10.2.28. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;

9.2.1.10.2.29. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;

9.2.1.10.2.30. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

9.2.1.10.2.31. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;

9.2.1.10.2.32. Capacidade de fazer “Hardware encryption”.

9.2.1.11. Gerenciamento de Sistemas

9.2.1.11.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;

9.2.1.11.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

9.2.1.11.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares

vulneráveis;

9.2.1.11.4. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;

9.2.1.11.5. Capacidade de gerenciar licenças de softwares de terceiros;

9.2.1.11.6. Capacidade de registrar mudanças de hardware nas máquinas gerenciadas;

9.2.1.11.7. Capacidade de gerenciar um inventário de hardware, com a possibilidade de cadastro de dispositivos (ex: router, switch, projetor, acessório, etc), informando data de compra, local onde se encontra, service tag, número de identificação e outros;

9.2.1.11.8. Possibilita fazer distribuição de software de forma manual e agendada;

9.2.1.11.9. Suporta modo de instalação silenciosa;

9.2.1.11.10. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

9.2.1.11.11. Possibilita fazer a distribuição através de agentes de atualização;

9.2.1.11.12. Utiliza tecnologia multicast para evitar tráfego na rede;

9.2.1.11.13. Possibilita criar um inventário centralizado de imagens;

9.2.1.11.14. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

9.2.1.11.15. Suporte a WakeOnLan para deploy de imagens;

9.2.1.11.16. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

9.2.1.11.17. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;

9.2.1.11.18. Capacidade de gerar relatórios de vulnerabilidades e patches;

9.2.1.11.19. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;

9.2.1.11.20. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;

9.2.1.11.21. Permite baixar atualizações para o computador sem efetuar a instalação

9.2.1.11.22. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;

9.2.1.11.23. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

9.2.1.11.24. Permite selecionar produtos a serem atualizados pela console de gerenciamento;

9.2.1.11.25. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;

9.2.1.11.26. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;

9.2.1.11.27. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;

9.2.1.11.28. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;

9.2.1.11.29. Deve permitir selecionar o idioma das aplicações que serão atualizadas;

9.2.1.11.30. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes.

9.2.2. ITEM 2 – Serviço de Suporte Técnico

9.2.2.1. Durante o período de 36 (trinta e seis) meses a contratada deverá fornecer suporte técnico para licitante seguindo as especificações abaixo:

9.2.2.2. Apoio às respostas a incidentes de segurança envolvendo Malware;

9.2.2.3. Suporte técnico para eventuais dúvidas ou problemas com a solução;

9.2.2.4. Acompanhamento nos chamados escalados para a fabricante em situações de falhas/problemas desconhecidos pelo suporte técnico da licitante ou bugs;

9.2.2.5. O atendimento deverá ser realizado via contato telefônico ou ferramenta de acesso remoto independentemente do tipo de incidente;

9.2.2.6. Suporte técnico 8x5 com a contratante, prestado unicamente à equipe de segurança da área de tecnologia da contratante, referente a problemas de funcionamento/configuração dos produtos fornecidos;

9.2.2.7. Número de chamados ilimitados;

9.2.2.8. Tempo de atendimento telefônico máximo de 2 horas, após a abertura do chamado técnico com a contratante.

9.2.2.9. Incidentes, chamados, e problemas escalados ao FABRICANTE deverão ter suporte 24x7 via web e telefone.

9.2.3. ITEM 3 - Serviço de Treinamento

9.2.3.1. A CONTRATADA deverá fornecer o serviço de treinamento de utilização, configuração e boas práticas do software de antivírus com carga horária de, no mínimo, 16 (dezesseis) horas ou superior para até 5 (cinco) colaboradores da CONTRATANTE que deverá ser realizado de forma remota;

9.2.3.2. O Treinamento deve abordar as versões dos softwares que estão sendo adquiridas pela CONTRATANTE;

9.2.3.4. O serviço de treinamento deverá ser executado em horário comercial.

9.4. Requisitos de Nível de Serviço - Item 2 (Suporte Técnico)

9.4.1. Os chamados técnicos serão categorizados nas severidades descritas abaixo, devendo ser atendidos nos prazos especificados (Tabelas I e II):

TABELA I - Severidade dos chamados técnicos	
Severidade	Descrição
ALTA	Serviços totalmente indisponíveis ou comprometimento de performance ou funcionalidade do serviço.
MÉDIA	Quando há um alerta no serviço/equipamento, mas ainda se encontra operacional.
BAIXA	Solicitação de configuração, manutenções preventivas, esclarecimentos técnicos relativos ao uso e aprimoramento do serviço/equipamento. Não haverá abertura de chamado com esta severidade em sábados, domingos e feriados.

TABELA II - Prazos para a solução do chamado			
PRAZOS	SEVERIDADES		
	ALTA	MÉDIA	BAIXA
Término do atendimento	2 horas	6 horas	3 dias úteis

9.4.2 . Serão considerados, para efeito do nível de serviço exigido:

9.4.2.1. Término do atendimento: Tempo decorrido entre a abertura do chamado pela CONTRATANTE e a solução definitiva da demanda pela CONTRATADA.

9.4.3. O atendimento da demanda só será considerado concluído após o aceite formal da equipe técnica da CONTRATANTE. Caso a CONTRATANTE não confirme a conclusão do atendimento, este permanecerá aberto. Nesse caso, a CONTRATANTE fornecerá informações sobre as pendências a serem resolvidas;

9.4.4. A severidade do chamado será informada pela CONTRATANTE no momento da sua abertura e seguirá o disposto na Tabela I;

9.4.5. A severidade poderá ser reclassificada pela CONTRATANTE. Caso isso ocorra, haverá nova contagem de prazo, conforme a nova severidade e seguirá os prazos dispostos na tabela II;

9.4.6. É vedado à CONTRATADA interromper o atendimento de severidade ALTA até que o equipamento/serviço esteja em pleno estado de funcionamento, mesmo que se estendam para períodos noturnos, sábados, domingos e feriados. Ainda assim, não haverá custos adicionais à CONTRATANTE;

9.4.7. É necessária autorização da CONTRATANTE para qualquer modificação na solução;

9.4.8. A CONTRATADA será a única responsável por todo e qualquer ato de seus empregados, credenciados e representantes, inclusive sobre danos causados à CONTRATANTE ou a terceiros, por negligência, imperícia, imprudência e/ou dolo, durante a

execução do contrato;

9.4.9. A CONTRATADA deverá ser parceira autorizada do fabricante estando apta e autorizada a fornecer o objeto, conforme Termo de Referência.

9.4.10. O não atendimento dos chamados nos prazos estipulados resultarão nas seguintes

9.4.10.1. Severidade alta: Glosa de 1,50% por hora de atraso, calculada sobre o valor mensal do serviço, até o limite de 24 horas. Ao final do prazo, a CONTRATANTE poderá considerar inexecução parcial do contrato;

9.4.10.2. Severidade média: Glosa de 0,75% por dia de atraso, calculada sobre o valor anual do serviço, até o limite de 72 horas. Ao final do prazo, a CONTRATANTE poderá considerar inexecução parcial do contrato;

9.5. Requisitos de capacitação

Não há

9.6. Requisitos Suporte Técnico e Atualização de Versão

Conforme o item 9.2.1.

9.7. Requisitos legais

Conforme Plano de Contratações de 2021

9.8. Requisitos de manutenção

9.8.1. 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, e obrigatoriamente, pelo fabricante da ferramenta ou empresa prestadora de serviços devidamente credenciada;

9.8.2. A garantia para o produto adquirido deverá contemplar a atualização de versão e suporte técnico, durante o período de garantia;

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

9.9. Requisitos Temporais

Não há

9.10. Requisitos Sociais, ambientais e culturais

Não se aplica, a infraestrutura já está preparada

9.11. Requisitos de arquitetura tecnológica

Não há

9.12. Requisitos de implantação

A contratada deverá instalar as licenças nas dependência do STM

9.13. Requisitos de garantia

Conforme item 9.2.1.

9.14. Requisitos de metodologia de trabalho

9.14.2. O produto fornecido será instalado e configurado em conformidade com o ambiente computacional da CONTRATANTE, sob a supervisão dos técnicos indicados por ela.

9.14.4. A CONTRATADA deverá instalar, configurar e testar a solução ofertada.

9.15. Requisitos de segurança da informação

9.15.1. O fornecedor deverá cumprir e garantir que seus profissionais estejam cientes, aderentes e obedeçam rigorosamente às normas e aos procedimentos estabelecidos na Política de Segurança da Informação do STM.

9.15.2. Deverá, ainda, manter sigilo, sob pena de responsabilidade civil, penal e administrativa, sobre todo e qualquer assunto de que tomar conhecimento em razão da execução do objeto deste processo de contratação, respeitando todos os critérios de sigilo, segurança e inviolabilidade, aplicáveis aos dados, informações, regras de negócio, documentos, entre outros.

9.15.3. As informações a serem tratadas de forma sigilosa, restrita e confidencial são aquelas que, por sua natureza, são consideradas como de interesse restrito ou confidencial, e não podem ser de conhecimento de terceiros, como por exemplo:

9.15.3.1. Dados, informações, códigos-fonte, artefatos, contidos em quaisquer documentos e em quaisquer mídias, não podendo, sob qualquer pretexto serem divulgadas, reproduzidas ou utilizadas por terceiros sob pena de lei, independentemente da classificação de sigilo conferida pelo STM a tais documentos;

9.15.3.2. Resultados, parciais ou totais, sobre produtos gerados;

9.15.3.3. Programas de computador, seus códigos-fonte e códigos-objeto, bem como suas listagens e documentações;

9.15.3.4. Toda a informação relacionada a programas de computador existentes ou em fase de desenvolvimento no âmbito do STM e rotinas desenvolvidas por terceiros, incluindo fluxogramas, estatísticas, especificações, avaliações, resultado de testes, arquivo de

dados, versões “beta” de quaisquer programas, dentre outros;

9.15.3.5. Documentos relativos à lista de usuários do STM e seus respectivos dados, armazenados sob qualquer forma;

9.15.3.6. Metodologias e ferramentas de serviços, desenvolvidas pelo STM;

9.15.3.7. Parte ou totalidade dos modelos de dados que subsidiam os sistemas de informações do STM, sejam eles executados interna ou externamente;

9.15.3.8. . Parte ou totalidade dos dados ou informações armazenadas nas bases de dados que subsidiam os sistemas de informações do STM, sejam elas residentes interna ou externamente;

9.15.3.9. Circulares e comunicações internas do STM;

9.15.3.10. Quaisquer processos ou documentos classificados como RESTRITO ou CONFIDENCIAL pelo STM.

10. LOCAL DE INSTALAÇÃO

10.1. A instalação da solução deverá ser feita na sede do Superior Tribunal Militar - Setor de Autarquias Sul, Praça dos Tribunais Superiores - Cep.: 70.098-900 - Brasília - DF

11. OBRIGAÇÕES DA CONTRATADA

11.1. Executar os serviços conforme especificações deste Termo de Referência e de sua proposta, com a alocação dos empregados necessários ao perfeito cumprimento das cláusulas contratuais, além de fornecer os materiais e equipamentos, ferramentas e utensílios necessários, na qualidade e quantidade especificadas neste Termo de Referência e em sua proposta.

11.2. Reparar, corrigir, remover ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços efetuados em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

11.3. Utilizar empregados habilitados e com conhecimentos básicos dos serviços a serem executados, em conformidade com as normas e determinações em vigor.

11.4. Apresentar os empregados devidamente uniformizados e identificados por meio de crachá, além de provê-los com os Equipamentos de Proteção Individual - EPI, quando for o caso.

11.5. Apresentar à CONTRATANTE, quando for o caso, a relação nominal dos empregados que adentrarão o órgão para a execução do serviço.

11.6. Responsabilizar-se por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere responsabilidade à CONTRATANTE.

11.7. Instruir seus empregados quanto à necessidade de acatar as normas internas da Administração.

11.8. Instruir seus empregados a respeito das atividades a serem desempenhadas, alertando-os a não executar atividades não abrangidas pelo contrato, devendo a CONTRATADA relatar à CONTRATANTE toda e qualquer ocorrência neste sentido, a fim de evitar desvio de função.

11.9. Relatar à CONTRATANTE toda e qualquer irregularidade verificada no decorrer da prestação dos serviços.

11.10. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos; nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

11.11. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação exigidas na licitação.

11.12. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

11.13. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento ao objeto da licitação, exceto quando ocorrer algum dos eventos arrolados nos incisos do § 1º do art. 57 da Lei nº 8.666, de 1993.

11.14. Assegurar à Contratante:

11.14.1. O direito de propriedade intelectual dos produtos desenvolvidos, inclusive sobre as eventuais adequações e atualizações que vierem a ser realizadas, logo após o recebimento de cada parcela, de forma permanente, permitindo à CONTRATANTE distribuir, alterar e utilizar estes sem limitações; e

11.14.2. Os direitos autorais da solução, do projeto, de suas especificações técnicas, da documentação produzida e congêneres, e de todos os demais produtos gerados na execução do contrato, inclusive aqueles produzidos por terceiros subcontratados, ficando proibida a sua utilização sem que exista autorização expressa da CONTRATANTE, sob pena de multa, sem prejuízo das sanções civis e penais cabíveis.

11.15. Deter instalações, aparelhamento e pessoal técnico adequado e disponíveis para a realização do objeto da licitação.

12. CONTRATANTE

12.1. Designar gestor que efetuará sua representação perante a CONTRATADA para determinação, avaliação, acompanhamento e aprovação dos serviços por ela realizados;

12.2. Colocar à disposição da CONTRATADA os equipamentos mínimos e documentação necessários para a realização das atividades quando estas forem executadas nas instalações do CONTRATANTE, com exceção das licenças de software necessárias

para os serviços, tais como licenças de ferramentas de desenvolvimento e outras, as quais deverão ser providenciadas pela própria CONTRATADA;

12.3. Prestar os esclarecimentos que venham a ser solicitados pela CONTRATADA, no que diz respeito ao contrato;

12.4. Efetuar os pagamentos devidos, observadas as condições estabelecidas no contrato;

12.5. Proporcionar à contratada todas as condições necessárias ao pleno cumprimento das obrigações decorrentes do objeto contratual, consoante estabelece a Lei Federal nº 8.666/1993 e suas alterações posteriores.

12.6. Fiscalizar a execução do objeto contratual, através de sua unidade competente, podendo, em decorrência, solicitar providências da contratada, que atenderá ou justificará de imediato.

12.7. Notificar a contratada de qualquer irregularidade decorrente da execução do objeto contratual.

12.8. Efetuar os pagamentos devidos à contratada nas condições estabelecidas neste Termo.

12.9. Aplicar as penalidades previstas em lei e neste instrumento.

13. SIGILO DAS INFORMAÇÕES

13.1. A CONTRATADA obriga-se, durante o curso do Contrato e após o seu término, ao mais completo e absoluto sigilo com relação a toda informação de qualquer natureza referente às atividades do CONTRATANTE, das quais venha a ter conhecimento ou venha a ter acesso por força do cumprimento do presente Contrato, não podendo sob qualquer pretexto, utilizá-las para si, invocar, revelar, reproduzir ou delas dar conhecimento a terceiros, responsabilizando-se em caso de descumprimento da obrigação assumida por eventuais perdas e danos e sujeitando-se às cominações legais, nos termos da Lei 4.595 de 31.12.1964 e demais leis correlatas;

13.2. “Informações Confidenciais" significam os dados ou informações confidenciais desenvolvidas ou adquiridas pelo CONTRATANTE ou pela Licitante vencedora e cuja divulgação ou utilização não autorizada, por qualquer das partes, poderá ser prejudicial a um ou a outro;

13.3. O CONTRATANTE e a Licitante vencedora tratarão sigilosamente todas as informações confidenciais, produtos e materiais que as contenham, não podendo ser copiados ou reproduzidos, publicados, divulgados ou de outra forma colocados à disposição, direta ou indiretamente, de qualquer pessoa, a não ser empregados e agentes do CONTRATANTE e/ou da Licitante vencedora que deles necessitem para desempenhar as suas funções no CONTRATANTE, sem que para tanto seja devido o consentimento prévio do CONTRATANTE ou comunicado da empresa vencedora;

13.4. As partes se obrigam a instruir sua equipe e prepostos a respeito das presentes disposições, as quais deverão ser observadas mesmo após o término ou cancelamento do futuro CONTRATO.

14. DIREITOS DE PROPRIEDADE, MARCAS, PATENTES E DIREITOS AUTORAIS

14.1. Quaisquer reproduções ou cópias de produtos e/ou bens e direitos cujos direitos de propriedade, marcas, patentes ou direitos autorais estiverem sob a responsabilidade da LICITANTE vencedora resultantes dos Serviços, incluindo documentação a eles correlata, em qualquer idioma, que forem desenvolvidos especificamente pela Licitante vencedora (para o CLIENTE) sob os dispositivos do futuro CONTRATO são de propriedade exclusiva do CONTRATANTE e deverão: (I) ser claramente designados como confidenciais, (II) incluir todas as marcas e indicações que façam referência ao proprietário, conforme apropriado, e (III) ter o mesmo grau de confidencialidade, proteção e legitimidade do original.

15. DA FISCALIZAÇÃO E ACOMPANHAMENTO

15.1. O acompanhamento e a fiscalização do contrato caberão à Equipe de Gestão do Contrato, que será instituída pelo Diretor-Geral, após a assinatura das partes;

15.2. No momento da assinatura do Contrato, a Contratada indicará um preposto para representá-la, sendo este responsável por acompanhar a execução do contrato e atuar como interlocutor principal junto ao Contratante, incumbido de receber, diligenciar, encaminhar e responder as questões técnicas, legais e administrativas referentes ao andamento contratual;

15.3. Assinado o contrato, o Diretor-Geral do Contratante instituirá a Equipe de Gestão da Contratação, composta por:

15.3.1. Gestor do Contrato: servidor com atribuições gerenciais, técnicas ou operacionais, relacionadas ao processo de gestão do contrato, para coordenar, supervisionar e controlar a execução do contrato, a fim de garantir o atendimento dos objetivos do Contratante;

15.3.2. Fiscal Demandante do Contrato: servidor representante da Diretoria de Tecnologia da Informação, competente para fiscalizar o contrato quanto aos aspectos funcionais da solução;

15.3.3. Fiscal Técnico do Contrato: servidor representante da Área da Diretoria de Tecnologia da Informação, competente para fiscalizar o contrato quanto aos aspectos técnicos da solução;

15.3.4. Fiscal Administrativo do Contrato, servidor representante da Área Administrativa, competente para fiscalizar o contrato quanto aos aspectos administrativos da execução, especialmente os referentes ao recebimento, pagamento, sanções, aderência às normas, diretrizes e obrigações contratuais.

15.4. A existência e a atuação da fiscalização pelo Contratante em nada restringe a responsabilidade, única, integral e exclusiva da Contratada, no que concerne à execução do contrato.

16. EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO

16.1. A Equipe de Planejamento desta contratação é composta pelos servidores Wilson Marques de Souza Filho (Integrante

Demandante), Márcio Coelho Marques (Integrante Técnico) e Luis Gustavo Costa Reis (Integrante Administrativo).

16.2. 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.

16.3. 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.

17. 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).

18. VIGÊNCIA DO CONTRATO

A vigência contratual será de 36 (trinta e seis) meses, podendo ser prorrogados na forma da lei, mediante termo aditivo, desde que mantendo as condições vantajosas para a administração até o limite previsto no art. 57, inciso II, da Lei nº 8.666/93;

19. PAGAMENTO

19.1. O pagamento será efetuado mediante a apresentação de nota fiscal, conforme instrução no link https://www.stm.jus.br/sistema-eletronico-informacoes/home-sei/usuario-externo/peticionamento-eletronico, acompanhada das informações quanto aos seus dados bancários e de cópia da nota de empenho, para atestação e posterior liquidação e pagamento da despesa pelo Contratante, em Brasília-DF, mediante ordem bancária creditada em conta corrente.

19.2. Informações sobre notas fiscais ou recibos encaminhados à Diretoria de Orçamento e Finanças (DORFI) para pagamento somente serão prestadas por intermédio do correio eletrônico dorfi@stm.jus.br ou pelo fax no (61) 3313-9516:

19.2.1. Na consulta, deverão ser informados o nome do interessado, com CNPJ ou CPF, o número da nota fiscal ou recibo e o número do protocolo no STM, com a respectiva data.

19.3. No caso de a Contratada ser optante pelo Sistema Integrado de Pagamento de Impostos e Contribuições das Microempresas e Empresas de Pequeno Porte (SIMPLES), ela deverá apresentar, juntamente com a nota fiscal, a devida comprovação, a fim de evitar a retenção na fonte dos tributos e contribuições.

19.4. No ato da efetivação do pagamento será efetuada a retenção na fonte dos tributos e contribuições, de acordo com a IN nº 1.234, de 11 de janeiro de 2012, da Secretaria da Receita Federal do Brasil e suas alterações.

19.5. Caso haja incorreção no faturamento, os documentos de cobrança serão devolvidos para regularização e pagos em até 72 horas, a contar da sua nova aceitação, não cabendo atualização financeira sob hipótese alguma.

19.6. O Superior Tribunal Militar reserva-se o direito de se recusar ao pagamento se, na ocasião prevista para a atestação, o objeto deste Termo de Referência não estiver de acordo com o licitado, proposto e contratado.

19.7. É vedado à Licitante vencedora, sob pena de rescisão contratual, negociar ou caucionar a nota de empenho recebida para fins de operação financeira, ainda que relacionada com o objeto deste edital.

19.8. 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 B 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.

20. DO REAJUSTE DE PREÇOS

20.1. Para os item 2, poderá haver reajuste anual de preços para as parcelas do contrato, de acordo com o Índice de Custo da Tecnologia da Informação (ICTI), do Instituto de Pesquisa Econômica Aplicada (IPEA), 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:

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

20.2. 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.

20.3. Por ocasião do pedido de reajuste, caberá à Contratada apresentar planilha dos cálculos, de acordo com fórmula do item 20.2.

20.4. 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.

20.5. 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.

20.6. O reajuste de que trata o Item 21.1 poderá sofrer alteração posterior, total ou parcial, decorrente da adoção, pelo Governo Federal, de medidas ou normas financeiras com força de lei.

21. RESCISÃO CONTRATUAL

21.1. A inexecução total ou parcial do contrato enseja a sua rescisão, conforme disposto nos arts. 77 a 80 da Lei no 8.666/93:

21.1.1. Os casos de rescisão contratual deverão ser formalmente motivados nos autos do processo, assegurado o contraditório e a ampla defesa.

21.2. A rescisão do contrato poderá ser:

21.2.1. Determinada por ato unilateral e escrito do Contratante, nos casos enumerados nos incisos I a XII, XVII e XVIII, do art. 78 da Lei nº 8.666/93;

21.2.2. Amigável, por acordo entre as partes, desde que haja conveniência para o Contratante;

21.2.3. Judicial, nos termos da legislação vigente sobre a matéria.

21.3. A rescisão administrativa ou amigável será precedida de autorização escrita e fundamentada da autoridade competente.

22. DESPESA ORÇAMENTÁRIA

22.1. A despesa ocorrerá à conta de dotação consignada à Justiça Militar da União pela Lei Orçamentária para o exercício de 2021, por meio dos seguintes Encargos do Plano de Ação (Código e Identificação) e emissão de respectivas Notas de Empenho:

25.1.1. As despesas decorrentes da presente contratação serão provenientes do Programa de Trabalho: MTGI; Elemento de Despesa 3.3.90.40 e Encargo: 52.01.06.06.000 - Software atualização de licenças - MTGI

23. ACRÉSCIMO OU SUPRESSÃO DO OBJETO

23.1. A critério da Administração, o objeto desta licitação poderá ser acrescido ou suprimido em até 25% do valor inicial contratado atualizado, observado o disposto no art. 65, §§ 1º e 2º, da Lei nº 8.666/93.

23.2. O acréscimo ou supressão contratual não poderá exceder os limites estabelecidos no § 1º do art. 65 da Lei nº 8.666/93, salvo a supressão decorrente de acordo celebrado entre as partes.

24. CONSIDERAÇÕES GERAIS

24.1. A equipe técnica envolvida na prestação dos serviços deverá possuir conhecimento e experiência conforme os requisitos técnicos para a prestação dos serviços descritos neste Termo de Referência;

24.2. A CONTRATADA, às suas expensas, deverá disponibilizar um profissional destacado para a gestão do relacionamento com a CONTRATANTE, o qual, além de possuir conhecimentos e capacidade profissionais necessários, deverá ter competência para resolver imediatamente todo e qualquer assunto relacionado com os serviços contratados;

24.3. A ausência ou omissão da fiscalização do CONTRATANTE não eximirá a CONTRATADA das responsabilidades oriundas deste contrato;

24.4. Todos os softwares e recursos computacionais utilizados pela CONTRATADA, necessários para o atendimento do objeto do contrato, deverão ser devidamente legalizados, em conformidade com as leis de Software (nº 9.609/98) e do Direito Autoral (nº 9.610/98);

24.5. Caso haja a necessidade de alocar equipamentos de informática nas dependências do CONTRATANTE, de propriedade da CONTRATADA, como computadores, switches, hubs, roteadores e impressoras, estes, obrigatoriamente, antes de conectar-se com a rede corporativa, deverão estar de acordo com a Política de Segurança da CONTRATANTE.

24.6. Caso haja necessidade de acessos remotos, por parte dos funcionários da CONTRATADA, o CONTRATANTE deverá ser informado, por escrito, da necessidade de utilização do referido meio e a CONTRATADA deverá ratificar que está de acordo com a Política de Segurança da Informação e o Termo de Confidencialidade, respectivamente;

25. SANÇÕES ADMINISTRATIVAS

Serão definidas pela SEPAD

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, 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.

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**
Márcio Coelho Marques	**Wilson Marques de Souza Filho**	**Luis Gustavo Costa Reis**
VALIDAÇÃO DO TERMO DE REFERÊNCIA		
Autoridade da Área Demandante - Ianne Carvalho Barros - Diretor da DITIN		

Documento assinado eletronicamente por **WILSON MARQUES DE SOUZA FILHO**, **COORDENADOR DE TECNOLOGIA**, em 23/09/2021, às 13:58 (horário de Brasília), conforme art. 1º,§ 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARCIO COELHO MARQUES**, **ANALISTA JUDICIÁRIA - Apoio Especializado - Análise de Sistemas**, em 23/09/2021, às 14:31 (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 23/09/2021, às 21:43 (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 **2338883** e o código CRC **188E0BA2**.