



MINISTÉRIO DA FAZENDA
SUPERINTENDÊNCIA DE SEGUROS PRIVADOS – SUSEP
DIRETORIA DE ADMINISTRAÇÃO
COORDENAÇÃO-GERAL DE TECNOLOGIA DA INFORMAÇÃO
PREGÃO Nº CGTI/05/2018
(Processo Administrativo n.º 15414.613061/2018-84)

1. DO OBJETO

Aquisição, ou renovação das licenças em uso, de software especializado para detecção e resposta a ameaças para *Endpoint* (ponto terminal) do tipo estação de trabalho e servidor, incluindo gerenciamento centralizado, licença de uso de software e garantia de atualização contínua, incluindo suporte técnico do desenvolvedor e/ou de seu representante técnico no Brasil, por um período de 36 (trinta e seis) meses.

Item	Descrição	Quantidade	Valor unitário	Valor Máximo Aceitável total
1	Licença de software para segurança de Endpoint para estação de trabalho, compatível com arquitetura de hardware 64 bits, para sistemas operacionais Microsoft Windows 7, Windows 8, Windows 10, Windows Server 2012 e Linux.	650	R\$ 86,99	R\$ 56.543,50
<p>1.1. CARACTERÍSTICAS MÍNIMAS DA CONSOLE DE GERENCIAMENTO (Administração centralizada por console único de gerenciamento);</p> <p>1.1.2. Conter configurações do Antivírus, AntiSpyware, Firewall, Proteção Contra Intrusos, controle de Dispositivos e Controle de Aplicações deverão ser realizadas para máquinas físicas e virtuais através da mesma console;</p> <p>1.1.3. Toda a solução deverá funcionar com agente único na estação de trabalho e nos servidores (físicos ou virtuais), a fim de diminuir o impacto ao usuário final.</p> <p>1.1.4. Mecanismo de comunicação em tempo real entre servidor e clientes, para entrega de configurações e assinaturas;</p> <p>1.1.5. Permitir a administração dos computadores dentro de uma estrutura de gerenciamento organizada por setores, unidades ou departamentos;</p> <p>1.1.6. O servidor de gerenciamento deverá possuir compatibilidade para</p>				

instalação nos sistemas operacionais Microsoft Windows Server 2012;

1.1.7. Possuir integração com LDAP, para importação da estrutura organizacional e autenticação dos Administradores;

1.1.8. Possibilidade de aplicar regras diferenciadas baseando na localidade lógica da rede;

1.1.9. Permitir que a localidade lógica da rede citada acima seja definida pelo conjunto dos seguintes itens: IP ou range de IP;

1.1.10. Possibilidade de aplicar regras diferenciadas por grupos de usuários e máquinas;

1.1.11. O servidor de gerenciamento deverá permitir o uso de banco de dados relacional Microsoft SQL Server 2012;

1.1.12. Possuir a funcionalidade e recursos para a criação e agendamento periódicos de backups da base de dados nativo da solução ou fornecer uma ferramenta para tal finalidade;

1.1.13. Possuir na solução replicação nativa do Banco de Dados entre os Servidores de Gerenciamento com opção de personalização do conteúdo a ser replicado (Assinaturas, Pacotes de Instalação, Políticas e Logs);

1.1.14. Possibilidade de instalação dos clientes em servidores, estações de trabalho e máquinas virtualizadas de forma remota via console de gerenciamento com opção de remoção da solução antivírus previamente instalada no parque da contratante (Symantec Endpoint Security), caso necessário.

1.1.15. Deve ter capacidade de remoção da solução citada no item anterior, a partir de um pacote único de instalação e desinstalação do próprio fabricante da solução.

1.1.16. A SOLUÇÃO ofertada deverá possuir ferramenta que permita analisar toda a rede e identificar os computadores que porventura não estejam com o Antivírus citado no item anterior instalado ou atualizado, de acordo com as políticas determinadas na console de administração;

1.1.17. Fornecer atualizações do produto e das definições de vírus e proteção contra intrusos durante toda a vigência do contrato;

1.1.18. Clientes definindo permissões para que somente o administrador possa alterar as configurações, desinstalar ou parar o serviço do cliente;

1.1.19. A console de gerenciamento deve permitir ao administrador travar separadamente os itens e cada subitens de acesso as configurações do cliente;

1.1.20. Capacidade de criação de contas de usuário com diferentes níveis de acesso de administração e operação;

1.1.21. Instalação e atualização do software sem a intervenção do usuário;

1.1.22. Possibilidade de configurar o bloqueio da desinstalação, desabilitar o serviço do cliente, importar e exportar configurações e abrir a console do cliente, por senha;

1.1.23. Suportar redirecionamentos dos logs para um servidor de Syslog;

1.1.24. A console de gerenciamento deve ser fornecida, no mínimo, em

língua portuguesa do Brasil ou inglesa.

1.2. CARACTERÍSTICAS MÍNIMAS DA ATUALIZAÇÃO DE VACINAS

1.2.1. Atualização incremental, remota e em tempo real, da vacina, da versão de cliente e do mecanismo de verificação (engine) dos clientes da rede;

1.2.2. Permitir eleger qualquer cliente gerenciado como um servidor de distribuição das atualizações, podendo eleger mais de um cliente para esta função;

1.2.3. Permitir criar planos de distribuição das atualizações via comunicação segura entre cliente e Servidores de Gerenciamento, Site do fabricante e Servidor de atualização interno;

1.2.4. Permitir políticas de atualização alternativas para que o cliente possa atualizar-se via internet, em caso de falha de comunicação (por determinado período configurável) com o servidor de atualização designado;

1.2.5. Nas atualizações das configurações e das definições de vírus não poderá utilizar login scripts, agendamentos, tarefas manuais ou outros módulos adicionais que não sejam parte integrante da solução e sem requerer reinicialização do computador ou serviço para aplicá-la.

1.2.6. Atualização automática das assinaturas dos servidores de gerenciamento e clientes via Internet, com periodicidade mínima diária;

1.2.7. Capacidade de voltar qualquer vacina e assinatura anterior armazenadas no servidor, utilizando opção e comando do Console podendo utilizar a arquitetura de grupos lógicos da console;

1.3. CARACTERÍSTICAS MÍNIMAS DA QUARENTENA

1.3.1. Possuir funcionalidades que permitam o isolamento (área de quarentena) de arquivos contaminados por códigos maliciosos que não sejam conhecidos ou que não possam ser reparados em um servidor central da rede;

1.3.2. Possibilidade de adicionar manualmente arquivos na quarentena do cliente com opção de restrições na console de gerenciamento;

1.3.3. Rastreamento agendado contra vírus com a possibilidade de selecionar uma máquina ou grupo de máquinas para rastrear com periodicidade mínima diária;

1.3.4. Rastreamento remoto contra vírus com a possibilidade de selecionar uma máquina ou grupo de máquinas para rastrear em tempo real;

1.4. CARACTERÍSTICAS MÍNIMAS DA CLIENTE GERENCIADO

1.4.1. Suportar máquinas com arquitetura 64-bit;

1.4.2. O cliente para instalação em estações de trabalho e servidores deverá possuir compatibilidade com os sistemas operacionais Microsoft Windows 7 ,8 e 10, além do 2012;

1.4.3. Deve possuir interface gráfica, no mínimo, em língua portuguesa do Brasil e inglesa.

1.4.4. Funcionalidade de Firewall e Detecção e Proteção de Intrusão

(IDS/IPS)

- 1.4.5. Suporte aos protocolos TCP, UDP e ICMP;
- 1.4.6. Reconhecimento dos tráficos DNS e DHCP com opção de bloqueio;
- 1.4.7. Possuir proteção contra exploração de buffer overflow;
- 1.4.8. Possuir proteção contra ataques de *Denial of Service (DoS)*, *Port-Scan* e *MAC Spoofing*;
- 1.4.9. Possibilidades de criação de assinaturas personalizadas para detecção de novos ataques;
- 1.4.10. Possibilidade de agendar a ativação da regra de Firewall;
- 1.4.11. Possibilidade de criar regras diferenciadas por aplicações;
- 1.4.12. Possibilidade de reconhecer automaticamente as aplicações utilizadas via rede baseado no fingerprint do arquivo;
- 1.4.13. Proteger o computador através da criação de uma impressão digital para cada executável existente no sistema, para que somente as aplicações que possuam essa impressão digital executem no computador;
- 1.4.14. Funcionalidade de *Whitelist* e *Blacklist* para o recurso de Impressão digital para os executáveis, possibilitando bloquear todos os executáveis da lista ou só liberar os executáveis da lista;
- 1.4.15. Permitir criação de zona confiável, permitindo que determinados IPs, protocolos ou aplicações se comuniquem na rede;
- 1.4.16. Bloqueio de ataques baseado na exploração da vulnerabilidade;
- 1.4.17. Permitir integração com navegadores WEB para prevenção de ataques;
- 1.4.18. Gerenciamento integrado à console de gerência da solução;

1.5. CARACTERÍSTICAS MÍNIMAS DA FUNCIONALIDADES DE ANTIVIRUS E ANTISPYWARE

- 1.5.1. Proteção em tempo real contra vírus, trojans, *worms*, *spyware*, *adwares* e outros tipos de códigos maliciosos.
- 1.5.2. Proteção AntiSpyware deverá ser nativa do próprio antivírus, ou seja, não dependente de plug-in ou módulo adicional;
- 1.5.3. As configurações do AntiSpyware deverão ser realizadas através da mesma console de todos os itens da solução;
- 1.5.4. Permitir a configuração de ações diferenciadas para cada subcategoria de riscos de segurança (Adwares, Discadores, Ferramentas de hacker, Acesso remoto, Spyware, Trackware e outros);
- 1.5.5. Permitir a configuração de duas ações, primária e secundária, executadas automaticamente para cada ameaça, com as opções de: somente alertar, limpar automaticamente, apagar automaticamente e colocar em quarentena;
- 1.5.6. Permitir a criação de listas de exclusões com informação da severidade, impacto e grau de remoção da ameaça nos níveis baixos, médio ou alto, onde os riscos

excluídos não serão verificados pelo produto;

1.5.7. Permitir que verificação das ameaças da maneira manual, agendada e em Tempo Real detectando ameaças no nível do *Kernel* do Sistema Operacional fornecendo a possibilidade de detecção de *Rootkits*;

1.5.8. Capacidade de realizar monitoramento em tempo real (real-time) por heurística correlacionando com a reputação de arquivos;

1.5.9. Capacidade de verificar a reputação de arquivos, correlacionando no mínimo as seguintes características:

1.5.9.1. Origem confiável;

1.5.9.2. Origem não confiável;

1.5.9.3. Tempo de existência do arquivo na internet;

1.5.9.4 Comportamento do arquivo;

1.5.9.5 Quantidade mínima de usuários que baixaram o arquivo da internet;

1.5.10. Programar intervalos de tempo para início de verificações agendadas de forma a reduzir impacto em ambientes virtuais.

1.5.11. Permitir configurar ações a serem tomadas na ocorrência de ameaças, incluindo Reparar, Deletar, Mover para a Área de Isolamento e Ignorar;

1.5.12. Verificação de vírus nas mensagens de correio eletrônico, pelo antivírus da estação de trabalho, suportando clientes Outlook (MAPI) e POP3/SMTP;

1.5.13. Possuir funcionalidades que permitam a detecção e reparo de arquivos contaminados por códigos maliciosos mesmo que sejam compactados;

1.5.14. A reparação automática dos danos causados deverá ser nativa do próprio antivírus, ou seja, não dependente de plug-in, execução de arquivo ou módulo adicional;

1.5.15. Capacidade de identificação da origem da infecção, para vírus que utilizam compartilhamento de arquivos como forma de propagação informando nome ou IP da origem com opção de bloqueio da comunicação via rede;

1.5.16. Possibilidade de bloquear verificação de vírus em recursos mapeados da rede, por senha;

1.5.17. Criar uma cópia backup do arquivo suspeito antes de limpá-lo;

1.5.18. Gerenciamento integrado à console de gerência da solução;

1.5.19. Possibilitar a criação de um disco (CD ou DVD) inicializável para verificação e remoção de ameaças sem a necessidade de carregar o Sistema Operacional do cliente;

1.5.20. Capacidade de executar varreduras em tempo real (real-time) contra ataques dirigidos às vulnerabilidades do navegador (browser);

1.6. CARACTERÍSTICAS MÍNIMAS DO RECONHECIMENTO DE NOVAS AMEAÇAS

1.6.1. Funcionalidade de detecção de ameaças desconhecidas que estão em memória por comportamento dos processos e arquivos das aplicações;

1.6.2. Não utilizar a assinatura de vírus para esta funcionalidade e fornecer assinatura periódicas da técnica de detecção;

1.6.3. Capacidade de detecção de *keyloggers* por comportamento dos processos em memória, com opção da sensibilidade distintas da detecção;

1.6.4. Reconhecer comportamento malicioso de modificação da configuração de DNS e arquivo Hosts;

1.7 CARACTERÍSTICAS MÍNIMAS DO CONTROLE DE DISPOSITIVOS E APLICAÇÕES

1.7.1. Gerenciar o uso de dispositivos USB e CD/DVD, através de controles de leitura/escrita/execução do conteúdo desses dispositivos e também sobre o tipo de dispositivo permitido (ex: permitir mouse USB e bloquear disco USB);

1.7.2. Permitir criar políticas de bloqueio de dispositivos baseadas na localização real da estação;

1.7.3. Gerenciamento integrado à console de gerência da solução;

1.7.4. Oferecer proteção para o sistema operacional, permitindo a definição de controles de acesso (escrita/leitura) para arquivos, diretórios, chaves de registro e controle de processos;

1.7.5. Permitir o bloqueio do uso de aplicações baseado em nome, diretório e hash da aplicação;

1.8 CARACTERÍSTICAS MÍNIMAS DA AUDITORIA DE INTEGRIDADE

1.8.1. Auditar periodicamente, em intervalos de minutos definidos pelo administrador, se o computador possui antivírus, firewall, AntiSpyware e patches instalados, ativos e atualizados, acionando o componente firewall para restringir o acesso à rede para aqueles computadores que não estiverem em conformidade com essa política;

1.8.2. Capacidade de iniciar a autocorreção do computador que falhou a auditoria, ou seja, corrigir os pontos onde a verificação especificada pelo administrador falhou;

1.9 CARACTERÍSTICAS MÍNIMAS DA PROTEÇÃO PARA AMBIENTES VIRTUALIZADOS

1.9.1. Capacidade de identificar automaticamente máquinas virtuais e físicas, possibilitando a criação de regras específicas por tipo de ambiente (virtual ou físico).

1.9.2. Suportar as mesmas funcionalidades existentes para o ambiente físico no ambiente virtual, contemplando os virtualizadores VMWare e Microsoft sem a necessidade de instalar outro agente, software, modulo e/ou plug-in;

1.9.3. Capacidade de verificar “templates” de máquinas virtuais, excluindo da operação de varredura todos os arquivos categorizados como confiáveis, existentes na máquina virtual utilizada como origem (templates);

1.9.4. Implementar funcionalidades para otimizar verificações em ambientes de VDI (Virtual Desktop Infrastructure);

1.10 CARACTERÍSTICAS MÍNIMAS DO SUPORTE A CLIENTES LINUX

1.10.1. Deve permitir a criação de pacotes de instalação a partir da console de

gerenciamento e fornecer link para download;

1.10.2. Gerenciamento integrado à console de gerência da solução;

1.10.3. Permitir a verificação das ameaças da maneira manual e agendada;

1.10.4. Permitir a criação de listas de exclusões para pastas e extensões de arquivos que não serão verificados pelo antivírus;

1.10.5. Permitir ações de reparar arquivo ou quarentena em caso de infecções a arquivos;

1.10.6. Deve permitir a configuração de parâmetros para otimizar a performance durante a verificação dos arquivos.

1.11. CARACTERÍSTICAS MÍNIMAS DOS RELATÓRIOS E MONITORAMENTO

1.11.1. Recursos do relatório e monitoramento deverão ser nativos da própria console central de gerenciamento;

1.11.2. Possibilidade de exibir a lista de servidores e estações que possuam o antivírus instalado, contendo informações como nome da máquina, usuário *logado*, versão do antivírus, versão do engine, data da vacina, data da última verificação e status (com vírus, desatualizada etc.);

1.11.3. Capacidade de Geração de relatórios, estatísticos e gráficos

1.12 IMPLANTAÇÃO (INSTALAÇÃO E CONFIGURAÇÃO)

1.12.1. A implantação (ou atualização de versão, caso a solução ofertada seja o Symantec Endpoint Security – a versão atualmente instalada é 12.1 RU6 MP1 Build 6318) da solução deverá ser realizada por técnicos da CONTRATADA, nas instalações da CONTRATANTE na cidade do Rio de Janeiro/RJ;

1.12.2. A implantação ou atualização da solução poderá ser realizada remotamente (via Rede *Wan* da Susep) nas representações regionais da CONTRATANTE localizadas nas seguintes cidades:

1.12.2.1. São Paulo – SP;

1.12.2.2. Brasília – DF;

1.12.2.3. Porto Alegre – RS.

1.12.3. Todos os custos referentes à implantação ou atualização da solução serão por conta da CONTRATADA, presencial na sede e presencial ou à distância nas regionais, cabendo à CONTRATANTE apenas a cessão dos computadores necessários às atividades e eventuais soluções de falhas de infraestrutura de rede;

1.12.4. A CONTRATADA deverá apresentar, previamente ao fornecimento de licenças, um plano de execução em um prazo máximo de 10 (dez) dias da assinatura do contrato, detalhando fases e prazos estimados;

1.12.5. Todos os passos necessários à instalação e à configuração da solução proposta deverão ser descritos no plano de execução, considerando a alocação mínima de 1 (um) técnico especializado, fornecido e mantido pela CONTRATADA.

1.12.6. A CONTRATADA terá o prazo de 30 (sessenta) dias corridos, excluídos os feriados nacionais, para concluir a instalação e a configuração da solução, findo o qual se

aplicarão as penalidades contratuais cabíveis;

1.12.7. Para efeito de emissão do Termo de Recebimento Definitivo, a instalação e a configuração dos softwares serão consideradas finalizadas com a aplicação em, no mínimo, 80% (oitenta por cento) do parque da CONTRATANTE e tendo sido validados pela equipe técnica da CONTRATANTE todos os procedimentos operacionais relativos ao processo como um todo;

1.12.8. A CONTRATANTE se reserva o direito de acompanhar e fiscalizar o cumprimento das obrigações contratuais pela CONTRATADA, verificando a aderência às especificações técnicas definidas, zelando pelo cumprimento de prazos e monitorando a qualidade;

1.12.9. A instalação deverá ser efetuada de forma a não comprometer o funcionamento dos sistemas, recursos ou equipamentos atualmente em operação na CONTRATANTE.

1.12.10. Havendo necessidade de interrupção de sistemas, recursos, equipamentos ou da rotina dos trabalhos de qualquer setor funcional em decorrência da instalação a ser efetuada, esta deverá estar devidamente planejada e ser necessariamente aprovada pela CONTRATANTE.

1.12.11. Para a execução do objeto contratado fica estabelecido o horário de funcionamento normal da CONTRATANTE.

1.12.12. É responsabilidade da Contratada a Migração (ou recriação) das regras e políticas já configuradas atualmente na solução utilizada pela Autarquia (Symantec Endpoint Security RU6 MP1 Build 6318).

1.12.13. É de responsabilidade da EMPRESA CONTRATADA a remoção da solução antiga de antivírus, atualmente instalada nos servidores e estações de trabalho da Susep. Havendo qualquer impossibilidade técnica de remover o produto antigo ou instalar produto novo de forma remota ou automatizada caberá à EMPRESA CONTRATADA encaminhar técnicos especializados ao local para proceder à migração.

1.12.14. Como parte integrante da instalação, imediatamente após a conclusão desta, deverá ocorrer operação assistida, em conjunto com os técnicos da CONTRATANTE, no intuito de capacitá-los minimamente a administrar a solução (8hs).

1.12.15. Esta operação assistida citada acima, deverá contemplar, no mínimo, os seguintes tópicos:

1.12.15.1. Instalação em ambientes Windows Linux;

1.12.15.2 Criação de pacotes de instalação;

1.12.15.3 Administração do servidor de gerenciamento, contemplando:

1.12.15.4. Migração (se for o caso);

1.12.15.5. Criação de regras e políticas;

1.12.15.6. Recuperação do banco de dados;

1.12.15.7. Configuração de antivírus;

1.12.15.8. Configuração de firewall;

1.12.15.9. Configuração de proteção para: Navegação; Arquivos compactados; Discos removíveis e E-mails.

1.12.15.10. Gerenciamento das funcionalidades via console de gerenciamento; Integração com o Microsoft Active Directory;

1.12.15.11. Atualização de softwares (tanto cliente quanto gerenciador) e vacinas.

1.13 ASSISTÊNCIA TÉCNICA DO PRODUTO

1.13.1. O fabricante da solução deverá manter sítio na internet em português do Brasil ou inglês que contenha os manuais e atualizações para download, FAQs, contatos e demais instruções necessárias para o uso e permanente atualização dos mesmos;

1.13.2. A CONTRATADA deverá fornecer todas as atualizações e novas versões dos softwares constantes da solução lançadas durante a vigência do contrato, sem ônus para a CONTRATANTE;

1.13.3. A CONTRATADA deverá fornecer versões dos softwares constantes da solução, compatíveis com qualquer nova versão de sistema operacional lançada (nas plataformas Microsoft Windows e Linux), assim que estas novas versões estejam disponíveis para uso, sem ônus para a CONTRATANTE;

1.13.4. As obrigações de manutenção (*software subscription*) deverão incluir atualizações de versões e pequenas atualizações de release, além de reparos de pequenos defeitos (*bug fixing patches*) assim que forem lançados no mercado;

1.13.5. A CONTRATADA deverá dispor de Central de Atendimento para resolução de problemas sobre o funcionamento apropriado da solução adquirida, via telefone e correio eletrônico;

1.13.6. Deverá ser provido serviço de atendimento a dúvidas técnicas (*helpdesk*) direto do fabricante, via sítio na internet, telefone e correio eletrônico;

1.13.7. A abertura de chamados e o atendimento junto à CONTRATADA e/ou ao fabricante deverão ser feitos em português, durante todo o prazo de vigência do contrato, através dos seguintes meios: Telefone fixo em horário comercial (prefixo 0800) ou Correio eletrônico.

1.13.8. A CONTRATADA deverá prover assistência técnica on-site nos limites do município do Rio de Janeiro/RJ, incluindo serviços de identificação e resolução de problemas, nos casos em o problema não seja solucionado pela Central de Atendimento.

1.13.9. A assistência técnica deverá oferecer, no mínimo, as seguintes características:

1.13.10. Atendimento via Central de Atendimento na modalidade 10x5, sendo 10 (dez) horas por dia (das 08:00h às 18:00h), 5 (cinco) dias na semana, exceto feriados e finais de semana;

1.13.11. Garantia de atendimento de número ilimitado de chamados;

1.13.12. Serão características da assistência técnica contratada:

1.13.13. Tempo máximo de espera para abertura do chamado após a comunicação do problema à Central de Atendimento: 02 (duas) horas;

1.13.14. Tempo máximo de retorno para avaliação do problema: 04 (quatro) horas;

1.13.15. Tempo máximo de primeira resposta após avaliação: 48 (quarenta e oito) horas, sem considerar finais de semana e feriados, a contar da hora de comunicação do incidente à Central

de Atendimento.

1.13.16. Este prazo acima poderá ser prorrogado desde que a CONTRATANTE aceite as justificativas apresentadas pela CONTRATADA que revelem a necessidade de dilação de prazo;

1.13.17. Os serviços de suporte técnico não terão qualquer ônus adicional para a CONTRATANTE.

1.13.18. Caso o problema verificado necessite ser escalado ao fabricante do produto adquirido, ou requeira o fornecimento de suporte on-site, o prazo para a sua primeira resposta não poderá ultrapassar, em qualquer situação, o tempo máximo de 48 (quarenta e oito) horas.

1.13.19. No caso de emergências em finais de semana ou feriados em que se necessite de assistência técnica e seja aberto chamado, o instante de abertura deste será considerado 08:00h do próximo dia útil, momento a partir do qual começarão a contar todos os demais prazos.

1.13.20. A CONTRATADA deverá responder por todas as despesas relativas a encargos trabalhistas, de seguro de acidentes, impostos, contribuições previdenciárias, passagens, diárias, hospedagem, alimentação e quaisquer outras que forem devidas e referentes aos serviços executados por seus empregados, em atividade de suporte, remoto ou on-site, uma vez que esses não têm qualquer vínculo empregatício com a CONTRATANTE;

2. JUSTIFICATIVA E OBJETIVO DA CONTRATAÇÃO

2.1. Com relação à segurança da informação, a Administração Pública Federal (APF) tem tomado medidas necessárias para implementação ou adequação da Segurança da Informação e Comunicações (SIC) em seus órgãos. Não somente o trato de assuntos e documentos sigilosos deve ser motivo de preocupação como também deve ser garantida a confiabilidade dos recursos tecnológicos utilizados para o trâmite dessas informações, onde se enquadram os “*Endpoint*” (em computação, *Endpoint* é jargão em língua inglesa utilizado para definir equipamentos de usuários finais ligados à rede local, notadamente estações de trabalho e computadores portáteis).

2.2. Apresenta-se, então, o desafio da área de Tecnologia da Informação (TI), em seu contexto Segurança Cibernética, de preservar a confidencialidade, a integridade e a disponibilidade dos dados, armazenados ou em trânsito, por seus meios computacionais.

2.3. Some-se a isto a publicação, em 07/10/2011, da Política de Segurança da Informação e Comunicações (Posic) da Susep que atribuiu à área de TI, em seu art. 49, a responsabilidade de “implantar ações técnicas para assegurar integridade, disponibilidade, confidencialidade e autenticidade de informações armazenadas em meio digital no âmbito da Susep”.

2.4. A COREI tem por atribuição regimental a adoção de medidas de segurança cibernética e esta aquisição visa a prevenir contaminação por vírus, *malwares* e suas variantes nos computadores (estações de trabalho e servidores de rede) na Susep pondo em risco os requisitos de SIC. Para isto, propõe-se como objeto de eventual certame licitatório a aquisição de solução integrada de segurança de *Endpoint*, incluindo instalação, atualização automática do software e das vacinas,

configuração, treinamento e assistência técnica, para equipamentos servidores de rede e estações de trabalho.

2.5. O quantitativo foi estimado com base no ambiente atual de TIC: Sede da Susep: 500 equipamentos; Representação Regional do Estado de São Paulo – SP: 50 equipamentos; Representação Regional do Estado do Rio Grande do Sul – Porto Alegre: 40 equipamentos e Escritório de Representação do Gabinete no Distrito Federal – Brasília: 10 equipamentos. O quantitativo foi estimado ainda com base em perspectiva de crescimento do parque computacional da CONTRATANTE de dez por cento (10%) aproximadamente ao longo do contrato.

2.6. Em 2015 foram adquiridas 650 licenças de uso do Symantec Endpoint Security, com validade de 36 meses, válidas de 21/09/2015 a 21/09/2018. Portanto, para não haver descontinuidade em nossa proteção, faz-se necessário renovar as licenças deste produto, cuja versão instalada é a 12.1 RU6 MP1 Build 6318, ou adquirir produto equivalente de outro fabricante.

3. CLASSIFICAÇÃO DOS BENS COMUNS

3.1. Verifica-se que os serviços pretendidos são oferecidos por diversos fornecedores no mercado de TIC. Desta forma, entendemos que o serviço é comum e, portanto, sugere-se como melhor opção a utilização da modalidade “Pregão” sendo, preferencialmente, em sua forma eletrônica e do tipo “Menor Preço”.

4. ENTREGA E CRITÉRIOS DE ACEITAÇÃO DO OBJETO.

4.1. O prazo de entrega e instalação dos bens é de 30 dias, contados do (a) assinatura do contrato, assim especificados:

4.1.1 Apresentação do plano de execução das fases de instalação e configuração em até 10 dias após a assinatura do contrato

4.1.2 Instalação e configuração em até 30 dias após a assinatura do contrato.

4.1.3 Como parte da instalação, imediatamente após a conclusão desta, deverá ocorrer operação assistida por parte da Contratada (8hs).

4.2. Os bens poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser substituídos no prazo de 10 (dez) dias, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

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

5. OBRIGAÇÕES DA CONTRATANTE

5.1. São obrigações da Contratante:

5.1.1. Receber o objeto no prazo e condições estabelecidas no Edital e seus anexos;

5.1.2. Verificar minuciosamente, no prazo fixado, a conformidade dos bens

recebidos provisoriamente com as especificações constantes do Edital e da proposta, para fins de aceitação e recebimento definitivo;

5.1.3. Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido;

5.1.4. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado;

5.1.5. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos no Edital e seus anexos;

5.1.6. A Administração não responderá por quaisquer compromissos assumidos pela Contratada com terceiros, ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

6. OBRIGAÇÕES DA CONTRATADA

6.1. A Contratada deve cumprir todas as obrigações constantes no Edital, seus anexos e sua proposta, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto e, ainda:

6.1.1. Efetuar a entrega do objeto em perfeitas condições, conforme especificações, prazo e local constantes no Edital e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: *marca, fabricante, modelo, procedência e prazo de garantia ou validade*;

6.1.2. *O objeto deve estar acompanhado do manual do usuário, com uma versão em português e da relação da rede de assistência técnica autorizada*;

6.1.3. Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990);

6.1.4. Substituir, reparar ou corrigir, às suas expensas, no prazo fixado neste Termo de Referência, o objeto com avarias ou defeitos;

6.1.5. Comunicar à Contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

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

6.1.7. Indicar preposto para representá-la durante a execução do contrato.

7. DA SUBCONTRATAÇÃO

7.1. *Não será admitida a subcontratação do objeto licitatório.*

8. ALTERAÇÃO SUBJETIVA

8.1. É admissível a fusão, cisão ou incorporação da contratada com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

9. CONTROLE DA EXECUÇÃO

9.1. Nos termos do art. 67 Lei nº 8.666, de 1993, será designado representante para acompanhar e fiscalizar a entrega dos bens, anotando em registro próprio todas as ocorrências relacionadas com a execução e determinando o que for necessário à regularização de falhas ou defeitos observados.

9.2. A fiscalização de que trata este item não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos, de conformidade com o art. 70 da Lei nº 8.666, de 1993.

9.3. O representante da Administração anotarará em registro próprio todas as ocorrências relacionadas com a execução do contrato, indicando dia, mês e ano, bem como o nome dos funcionários eventualmente envolvidos, determinando o que for necessário à regularização das falhas ou defeitos observados e encaminhando os apontamentos à autoridade competente para as providências cabíveis.

10. DAS SANÇÕES ADMINISTRATIVAS

10.1. Comete infração administrativa nos termos da Lei nº 8.666, de 1993 e da Lei nº 10.520, de 2002, a Contratada que:

10.1.1. Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

10.1.2. Ensejar o retardamento da execução do objeto;

10.1.3. Fraudar na execução do contrato;

10.1.4. Comportar-se de modo inidôneo;

10.1.5. Cometer fraude fiscal;

10.1.6. Não manter a proposta.

10.1.7. A Contratada que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

10.1.8. Advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;

10.1.9. Multa moratória de 0,5% (meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

10.1.10. Multa compensatória de 10 % (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

10.1.11. Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

10.1.12. Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

10.1.13. Impedimento de licitar e contratar com a União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;

10.1.14. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados;

10.1.15. Também ficam sujeitas às penalidades do art. 87, III e IV da Lei nº 8.666, de 1993, as empresas ou profissionais que:

10.1.16. Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no recolhimento de quaisquer tributos;

10.1.17. Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação;

10.1.18. Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

10.1.19. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 8.666, de 1993, e subsidiariamente a Lei nº 9.784, de 1999.

10.1.20. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

10.1.21. As penalidades serão obrigatoriamente registradas no SICAF.

Rio de Janeiro, 03 de agosto de 2018.