Projeto Básico SUPES 00942/2019

Título

Consulta Pública para Aquisição de Licenças, Manutenção e Suporte Técnico para Plaforma Corporativa de Proteção para Endpoints

1ª Versão

Vinculação com Documento de Oficialização de Demanda

Número DOD	Titulo da Demanda	Número do Item	Nome do Objeto	Descrição

1.0 Objeto

1.1.Contratação de licenças, manutenção, suporte técnico e atualização para plataforma corporativa de proteção para endpoints, que permita prevenção contra malwares (códigos maliciosos), para detecção e bloqueio de atividade maliciosa a partir de aplicações confiáveis e não-confiáveis, e que possuam recursos de investigação e remediação necessários para responder dinamicamente a alertas e incidentes de segurança em estações de trabalho e servidores.

2.0 Especificação do objeto a ser contratado

A solução a ser adquirida deverá atender todos os seguintes requisitos:

2.1 - Sobre o gerenciamento

2.1.1 - O gerenciamento centralizado da solução de proteção dos Endpoints deverá ser disponibilizado localmente no ambiente de Intranet da rede do Serpro (“On premise”), por meio de console (interface gráfica) e possuir as seguintes características:
2.1.1.1 - Exibir servidores e estações que possuam o agente da solução instalado, contendo, no mínimo, as seguintes informações:
2.1.1.1.1 - Nome da máquina;
2.1.1.1.2 - Nome e versão do sistema operacional;
2.1.1.1.3 - Endereço IP (IPV4 e IPV6) e endereço físico (MAC);
2.1.1.1.4 - Informações de login de usuário;
2.1.1.1.5 - Status do agente da solução;
2.1.1.1.6 - Versão do agente;
2.1.1.1.7 - Versões dos bancos de assinaturas ou equivalentes.
2.1.1.2 - Registrar e armazenar a data e hora, contendo o status da última tentativa de atualização e comunicação dos agentes com o servidor de gerenciamento.
2.1.1.3 - Permitir gerenciar os agentes da solução em uma árvore de diretórios personalizável pelo administrador da plataforma.
2.1.1.3.1 - A console deve permitir a criação, edição e remoção de grupos e subgrupos para realizar o agrupamento de agentes da solução.
2.1.1.3.2 - A console deve permitir o agrupamento de agentes da solução de forma automática utilizando o endereçamento de rede, pelo menos.
2.1.1.4 - Permitir o gerenciamento do servidor da solução por meio de Interface Gráfica de Usuário (GUI) instalável ou por navegador web por meio de protocolo HTTPS.

2.1.1.4.1 - No caso de GUI web, deverá ser compatível no mínimo com os seguintes navegadores:
2.1.1.4.1.1 - Google Chrome.
2.1.1.4.1.2 - Mozilla Firefox.
2.1.1.4.1.3 - Microsoft Internet Explorer.
2.1.1.5 - Possuir compatibilidade de armazenamento de dados em Banco de Dados padrão SQL (Structured Query Language).
2.1.1.6 - Permitir o armazenamento das informações coletadas nos agentes da solução em um banco de dados centralizado, devendo este ser fornecido de forma integrada à console de gerenciamento da solução ofertada sem custo adicional para o SERPRO.
2.1.1.7 - Permitir o gerenciamento centralizado dos arquivos infectados com códigos maliciosos e colocados em quarentena.
2.1.1.8 - Permitir a geração de relatórios ou gráficos que contenham as seguintes informações:
2.1.1.8.1 - Versões dos bancos de assinaturas (ou equivalentes) e dos componentes do agente instalado em cada máquina;
2.1.1.8.2 - Listagem dos códigos maliciosos que mais foram detectados;
2.1.1.8.3 - Listagem do total de códigos maliciosos encontrados;
2.1.1.8.4 - Listagem dos códigos maliciosos que infectaram determinada máquina;
2.1.1.8.5 - Listagem das máquinas que estão infectadas por determinado código malicioso;
2.1.1.8.6 - Listagem de máquinas com os bancos de assinaturas (ou equivalentes) desatualizados;
2.1.1.8.7 - Listagem de máquinas que mais sofreram infecções em um determinado período de tempo;
2.1.1.8.8 - Status da atividade do agente da solução;
2.1.1.8.9 - Listagem de códigos maliciosos não removidos, por máquina.
2.1.1.9 - Permitir a geração dos relatórios personalizados.
2.1.1.10 - Permitir a exportação dos relatórios gerados nos itens 2.1.1.8 e 2.1.1.9, em pelo menos três dos seguintes formatos: CSV, XLS, HTML e PDF.
2.1.1.11 - Possuir a capacidade de gerar registros/logs para auditoria por um período configurável.
2.1.1.12 - Possuir console de alertas e sumário do ambiente em relatório gráfico na própria console de gerenciamento, permitindo personalização, informando no mínimo:
2.1.1.12.1 - Quantitativo de agentes instalados e respectivos status;
2.1.1.12.2 - Visualização dos grupos de máquinas com maiores registros de infecção;
2.1.1.12.3 - Informação da base de assinatura do servidor de gerenciamento.
2.1.1.13 - Deve ser possível o uso de mecanismos que proporcionem alta disponibilidade para os servidores e banco de dados da solução.
2.1.1.14 - Possuir mecanismo para aplicação de políticas diferenciadas para as máquinas que acessarem a Internet a partir de uma rede externa.
2.1.1.15 - Permitir o acompanhamento do status das máquinas mesmo quando estas estiverem conectadas à Internet a partir de uma rede externa.
2.1.1.16 - A console de gerenciamento deve permitir a criação de usuários com diferentes perfis de acesso.
2.1.1.16.1 - Possibilitar a restrição dos níveis de acesso às políticas e às configurações da ferramenta;
2.1.1.16.2 - Possibilitar a restrição da visualização da estrutura de grupos de máquinas;
2.1.1.17 - Permitir a integração da base de usuários da solução com o a base de usuários corporativa através de protocolo LDAP.
2.1.1.18 - Permitir a gravação de registros de log das atividades dos usuários da console de gerenciamento, para fins de auditoria, tais como: login, logout e alteração de políticas,

no mínimo.
2.1.1.19 - Permitir a realização de backup dos componentes da solução de forma periódica e pré-agendada, possibilitando a plena restauração da plataforma de Endpoint em casos de desastre.

2.2 - Proteção para a plataforma Microsoft
2.2.1 - Compatibilidades:
2.2.1.1 - Estações de trabalho:
2.2.1.1.1 - Plataformas 32 bits: Windows 7 e superiores;
2.2.1.1.2 - Plataformas 64 bits: Windows 7 e superiores.
2.2.1.2 - Servidores:
2.2.1.2.1 - Plataformas 32 bits: Windows 2003 Server;
2.2.1.2.2 - Plataformas 64 bits: Windows 2003 Server e superiores.
2.2.1.2 - A compatibilidade com a plataforma Windows, de acordo com o especificado nos subitens dos itens 2.2.1.1 e 2.2.1.2, deve contemplar todas as edições disponibilizadas pelo fabricante do sistema operacional.
2.2.1.3 - A solução deve possuir compatibilidade com tecnologias de virtualização para os sistemas operacionais especificados nos subitens dos itens 2.2.1.1 e 2.2.1.2, permitindo o seu pleno funcionamento em máquinas virtualizadas de forma equivalente a máquinas reais.
2.2.1.3.1 - O agente da solução deverá ser suportado nas seguintes plataformas de virtualização:
2.2.1.3.1.1 - VMware;
2.2.1.3.1.2 - XEN;
2.2.1.3.1.3 - Hyper-V;
2.2.1.3.1.4 - Virtual Box.
2.2.1.3.2 - A solução, obrigatoriamente, deverá ofertar compatibilidade, nos testes de homologação, para todas as soluções acima (2.2.1.3.1.1 a 2.2.1.3.1.4).
2.2.1.4 - Para o sistema operacional Windows 2003 Server, será exigido no mínimo a compatibilidade com o módulo de proteção básico contra malwares, baseado apenas em assinaturas.
2.2.1.4.1 – Será permitido que seja ofertada outra versão da plataforma endpoint, com console separada, desde que seja do mesmo fabricante.
2.2.2 - Requisitos:
2.2.2.1 - Reconhecer e impedir a ação de código malicioso ao tentar executar funções que possam causar danos ao sistema, tais como:
2.2.2.1.1 - Alterações no registro do Windows;
2.2.2.1.2 - Alterações de código em programas e arquivos; e
2.2.2.1.3 - Modificação do navegador web (Browser Hijacking).
2.2.2.2 – Reconhecer e impedir ações provenientes de malwares classificados como: vírus, trojan, spyware, downloaders, adware, bot, fileless, worm, ransomware, rootkit e backdoor.
2.2.3 - Sobre a instalação da solução:
2.2.3.1 - Permitir a instalação do agente em estações de trabalho e servidores, pelos seguintes meios:
2.2.3.1.1 - Via console, a partir de um servidor de distribuição central ou de servidores distribuídos, por meio das estruturas da LAN e WAN;
2.2.3.1.2 - Por meio de navegador web ou mídia, em equipamentos standalone;
2.2.3.1.3 - Por meio de pacote de instalação pré-configurado, podendo ser utilizado em conjunto com scripts de inicialização.
2.2.3.2 - Permitir a remoção do agente em estações de trabalho e servidores via console

de gerenciamento da solução.
2.2.3.3 - Permitir que as seguintes ações sejam executadas após solicitação de senha específica da plataforma de endpoint:
2.2.3.3.1 - Desinstalar o agente;
2.2.3.3.2 - Desabilitar o agente;
2.2.3.3.3 - Parar e desabilitar o serviço da solução endpoint.
2.2.3.4 - Possibilitar a identificação de estações e servidores que ainda não possuam o agente instalado.
2.2.3.5 - Compatível com IPV4 e IPV6.
2.2.4 - Sobre as funcionalidades:
2.2.4.1 - Detectar, bloquear e remover códigos maliciosos localizados em diretórios e subdiretórios locais, mídias removíveis regraváveis, programas executáveis, setor de BOOT, em macro de arquivos de pacotes de escritórios e em mapeamentos de rede.
2.2.4.2 - Possuir tecnologia de detecção, bloqueio e remoção dos códigos maliciosos atualmente conhecidos, segundo a tipificação de malwares descrita na Cartilha do CERT.BR, no fascículo sobre Códigos Maliciosos.
2.2.4.3 – Detectar, bloquear e remover códigos maliciosos desconhecidos por meio de heurística e análise de comportamento.
2.2.4.4 - Detectar códigos maliciosos desconhecidos por meio de inteligência artificial (machine learning) com processamento local nos agentes da solução, sem necessidade de consulta a nuvem fora da Intranet.
2.2.4.5 - Possuir funcionalidades de HIPS (Host Intrusion Prevention System) e firewall de host integrados (gerenciados por console do mesmo fabricante da solução) e com opção de atualização automática dos bancos de assinaturas (ou equivalentes).
2.2.4.5.1 - Permitir a criação manual de regras personalizadas para as funcionalidades de firewall e HIPS.
2.2.4.6 - Permitir criação, remoção, manutenção e distribuição de listas de exclusão/reputação de arquivos legítimos identificados como códigos maliciosos (falsos positivos), e que sejam baseadas no nome (caminho completo) e/ou no hash, possibilitando a aplicação em toda a hierarquia de servidores e estações.
2.2.4.7 - Permitir programação de varreduras automáticas, tais como: conexão de pendrive, varredura ao iniciar o sistema operacional.
2.2.4.8 - Realizar varredura em tempo real para arquivos durante ações de leitura e escrita.
2.2.4.8.1 – Permitir customização para varredura caso ocorra uma única ação, tais como: leitura ou escrita.
2.2.4.9 - Permitir a execução de varredura manual por meio da interface gráfica do agente da solução.
2.2.4.10 - Permitir varredura remota a partir da console de gerenciamento contra códigos maliciosos com a opção de selecionar uma máquina ou um grupo de máquinas.
2.2.4.11 - Verificar código malicioso em arquivos compactados com no mínimo 3 (três) níveis de compactação e para os formatos ZIP e RAR, no mínimo.
2.2.4.12 - A proteção antispyware deverá ser realizada de forma integrada ao agente, caracterizando uma função nativa da solução.
2.2.4.13 - Possibilitar o acionamento da varredura de forma manual e pré-agendada:
2.2.4.13.1 - A varredura em tempo real deve possuir as opções de habilitar e desabilitar.
2.2.4.14 - Permitir execução automática das seguintes ações (primária e secundária), quando ocorrer a detecção de códigos maliciosos:
2.2.4.14.1 - Limpar;
2.2.4.14.2 - Apagar;
2.2.4.14.3 - Quarentenar;

2.2.4.14.3.1 - A quarentena consiste em algum mecanismo que inutilize a execução do código malicioso.
2.2.4.15 - Permitir a interrupção de tarefas do agente que estejam em andamento.
2.2.4.16 - O agente da solução deve gerar alertas, no momento da detecção, por mensagem na tela e registro na console de gerenciamento:
2.2.4.16.1 - A solução deve possuir opções para desativar ou ativar a mensagem a ser exibida na tela do usuário.
2.2.4.17 - O agente da solução deve gravar log registrando os eventos de detecção de código malicioso, tanto localmente como na console de gerenciamento.
2.2.4.18 - Permitir o controle de acesso a dispositivos externos, no mínimo de armazenamento e de conexão (3G/4G), conectados através da porta USB (e variantes) à estação ou servidor, por meio da definição centralizada de permissões, com a capacidade de replicação em toda a hierarquia de grupos de máquinas.
2.2.4.18.1 - A solução deve permitir o controle (bloqueio e registro em log), no mínimo, das ações de leitura e escrita nos dispositivos de armazenamento externo.
2.2.4.18.2 - Permitir criação de lista de exceção baseado no GUID e no Device ID.
2.2.4.18.3 - Permitir bloqueio baseado no GUID ou no Device ID.
2.2.4.19 - Permitir controle do uso da CPU no agente da solução quando o mesmo for executar suas tarefas de varredura, seja esta agendada ou manual.
2.2.4.20 - Possuir funcionalidade que permita o controle de execução de aplicativos de forma manual, através da inserção ou remoção de regras pelo administrador da solução possibilitando a aplicação em toda a hierarquia de servidores e estações.
2.2.4.20.1 - As regras devem permitir o controle dos aplicativos no mínimo por: nome (caminho completo ou apenas o nome do arquivo), extensão de arquivo, código hash e chaves de registro do windows.
2.2.4.20.1.1 - As ações a serem executadas neste controle devem ser, no mínimo, bloqueio e registro (log).
2.2.4.21 – Possuir mecanismo para blindagem de vulnerabilidades conhecidas do sistema operacional e de aplicativos cujos respectivos patches de correção não estejam aplicados ou não existam.
2.2.4.22 – Possuir funcionalidade de reputação de websites que efetue a análise e o bloqueio de páginas web suspeitas.
2.2.4.22.1 – Esta funcionalidade deverá ser compatível com os seguintes navegadores:
2.2.4.22.1.1 – Google Chrome;
2.2.4.22.1.2 – Microsoft Edge;
2.2.4.22.1.3 – Microsoft Internet Explorer;
2.2.4.22.1.4 – Mozilla Firefox.

2.2.5 - Sobre a Configuração:
2.2.5.1 - Bloquear o acesso às configurações do agente da solução para que as configurações estabelecidas pelo servidor de gerenciamento sejam mantidas.
2.2.5.2 - Bloquear a remoção do agente da solução por quaisquer usuários que não sejam o administrador do produto.2.2.5.2.1 - Permitir a remoção do agente da solução apenas com a utilização de senha definida por meio da Console de gerenciamento.
2.2.5.3 - Possuir a capacidade de aplicar mudança na configuração do agente da solução, para todos os endpoints, por grupo de máquinas e por máquina individualmente.
2.2.5.4 - Permitir o travamento das configurações, definições de permissões e paralisações do agente da solução, por máquina ou grupo de máquinas, somente pelo administrador da plataforma de proteção endpoint.
2.2.5.5 - Permitir que os servidores da solução imponham a configuração aos seus agentes/servidores de níveis mais baixos na respectiva hierarquia, mesmo que a

configuração local de um agente seja alterada com recursos administrativos da ferramenta.

2.2.6 - Sobre a atualização:
2.2.6.1 - Nas máquinas protegidas, as atualizações da engine (versão do agente), dos bancos de assinaturas e regras de todos os componentes deverão ser realizadas remotamente e em tempo real, sem a necessidade de utilização de login-scripts, agendamentos ou intervenção do usuário.
2.2.6.2 - Permitir atualização incremental dos bancos de assinaturas (ou equivalentes).
2.2.6.3 - As atualizações deverão ser possíveis mesmo com o uso de serviço de proxy.
2.2.6.4 - Permitir a atualização dos bancos de assinaturas dos agentes da solução (ou equivalentes) de forma hierárquica, a partir de máquinas distintas dos servidores de gerenciamento da solução.
2.2.6.5 - Permitir a programação de atualizações automáticas dos bancos de assinaturas (ou equivalentes) e regras de todos os componentes a partir de local predefinido da rede ou de fonte oficial do fabricante disponível na Internet, com frequência compatível ao surgimento de vacinas e horários definidos pelo administrador do produto, sem interrupção do usuário.
2.2.6.6 - Permitir realização de download para atualização da versão do agente, seus componentes e dos bancos de assinaturas (ou equivalentes) a partir da seleção de múltiplos repositórios (servidores da solução).
2.2.6.7 - Possuir mecanismo de "rollback" para atualização dos bancos de assinaturas (ou equivalentes), de forma centralizada, automática e operacionalizada por meio da console de gerenciamento.
2.2.6.7.1 - Permitir o gerenciamento, por meio da console, de no mínimo 02 (duas) versões distintas dos seguintes componentes:
2.2.6.7.1.1 - Engines (versões do agente);
2.2.6.7.1.2 - Bancos de assinaturas ou equivalentes.
2.2.6.8 - Possibilidade da eleição de estação de trabalho como fonte de atualização e de distribuição dos bancos de assinaturas (ou equivalentes), para máquinas ou grupos específicos.
2.2.6.9 - Permitir a instalação e atualização do agente e dos bancos de assinaturas mesmo com o servidor de gerenciamento inoperante, sem requerer outro software ou agente para esta finalidade.
2.2.6.10 - Permitir a atualização manual dos bancos de assinaturas dos servidores de gerenciamento e dos agentes da solução, quando não for possível atualizá-las remotamente ou quando for necessário.

2.3 - Proteção para plataforma Macintosh.
2.3.1 - Compatibilidades:
2.3.1.1 - Estações de trabalho:
2.3.1.1.1 - MacOS X Mavericks e superiores.
2.3.2 - Requisitos:
2.3.2.1 - Reconhecer e impedir a ação de software malicioso ao tentar executar ações sobre os arquivos.
2.3.2.2 - Permitir a instalação e atualização do agente e dos bancos de assinaturas mesmo com o servidor de gerenciamento inoperante, sem requerer outro software ou agente para esta finalidade.
2.3.3 - Sobre a instalação do produto:
2.3.3.1 - Permitir a instalação do agente de forma remota (via console) ou localmente (via mídia).

2.3.3.2 - Permitir interromper, desabilitar e desinstalar o produto somente com o privilégio de administrador do produto ou administrador local da máquina.
2.3.4 - Sobre as funcionalidades:
2.3.4.1 - Detectar, bloquear e remover códigos maliciosos localizados em diretórios, subdiretórios locais e programas executáveis.
2.3.4.2 - Possuir tecnologia de detecção, bloqueio e remoção dos códigos maliciosos atualmente conhecidos para esta plataforma.
2.3.4.3 - Permitir criação, remoção, manutenção e distribuição de listas de exclusão de arquivos legítimos identificados como códigos maliciosos (falsos positivos), e que sejam baseadas no nome (caminho completo) ou código hash, possibilitando a aplicação em toda a hierarquia de agentes da solução.
2.3.4.4 - Permitir programação de varreduras automáticas, tais como: conexão de pendrive, varredura ao iniciar o sistema operacional.
2.3.4.5 - Realizar varredura em tempo real, para arquivos criados, copiados, movidos, modificados e em execução.
2.3.4.6 - Permitir a execução de varredura manual.
2.3.4.7 - Permitir varredura remota a partir da console de gerenciamento contra códigos maliciosos com a opção de selecionar uma máquina ou um grupo de máquinas para serem rastreadas.
2.3.4.8 - Verificar códigos maliciosos em arquivos compactados para os formatos ZIP, GZIP e RAR, no mínimo.
2.3.4.9 - Programar obrigatoriamente as seguintes ações (primária e secundária), executadas automaticamente quando ocorrer a detecção de códigos maliciosos, como as opções definidas nos subitens:
2.3.4.9.1 - Limpar;
2.3.4.9.2 - Apagar;
2.3.4.9.3 - Quarentenar.
2.3.4.9.3.1 - A quarentena consiste em um mecanismo que deve inutilizar a execução do código malicioso.
2.3.4.10 - O agente da solução deve alertar, registrar e gravar os eventos de detecção de códigos maliciosos.
2.3.5 - Sobre a Configuração:
2.3.5.1 - Bloquear o acesso às configurações do agente da solução para que as configurações estabelecidas pelo servidor da solução sejam mantidas.
2.3.6 - Sobre a Atualização:
2.3.6.1 - Atualizar remotamente, o banco de assinaturas da solução, sem a necessidade de utilização de login-scripts nem intervenção do usuário.
2.3.6.2 - Permitir atualização incremental do banco de assinaturas da solução.
2.3.6.3 - Permitir a programação de atualizações automáticas do banco de assinaturas da solução, a partir de local predefinido da rede ou de site da Internet, com frequência compatível ao surgimento de vacinas e horários definidos pelo administrador do produto, sem interrupção do usuário.

2.4 - Proteção para plataforma Linux
2.4.1 - Compatibilidades:
2.4.1.1 - Estações de trabalho:
2.4.1.1.1 - Plataforma 64 bits:
2.4.1.1.1.1 - Ubuntu 16.04 e superior.
2.4.1.2 - Servidores:
2.4.1.2.1 - Plataforma 64 bits:
2.4.1.2.1.1 - RedHat 7 e superiores;

2.4.1.2.1.2 - CentOS 6 e superiores.
2.4.2 - Requisitos:
2.4.2.1 - Reconhecer e impedir a ação de software malicioso ao tentar executar ações sobre os arquivos.
2.4.2.2 - Permitir a instalação e atualização do agente e dos bancos de assinaturas mesmo com o servidor de gerenciamento inoperante, sem requerer outro software ou agente para esta finalidade.
2.4.3 - Sobre a instalação do produto:
2.4.3.1 - Permitir interromper, desabilitar e desinstalar o produto somente com o privilégio de administrador do produto ou administrador local da máquina.
2.4.4 - Sobre as funcionalidades:
2.4.4.1 - Detectar, bloquear e remover códigos maliciosos localizados em diretórios e subdiretórios locais, programas executáveis e setor de BOOT.
2.4.4.2 - Possuir tecnologia de detecção, bloqueio e remoção dos códigos maliciosos atualmente conhecidos para esta plataforma.
2.4.4.3 - Permitir criação, remoção, manutenção e distribuição de listas de exclusão de arquivos legítimos identificados como códigos maliciosos (falsos positivos), e que sejam baseadas no nome (caminho completo) ou código hash, possibilitando a aplicação em toda a hierarquia de servidores e agentes da solução.
2.4.4.4 - Permitir programação de varreduras automáticas do sistema.
2.4.4.5 - Realizar varredura em tempo real, para arquivos criados, copiados, movidos, modificados e em execução.
2.4.4.6 - Permitir a execução de varredura manual.
2.4.4.7 - Permitir varredura remota a partir da console de gerenciamento contra códigos maliciosos com a opção de selecionar uma máquina ou um grupo de máquinas para serem rastreadas.
2.4.4.8 - Verificar códigos maliciosos em arquivos compactados para os formatos ZIP, GZIP, e RAR, no mínimo.
2.4.4.9 - Possibilitar acionamento de função de verificação de ocorrência de código malicioso das seguintes formas:
2.4.4.9.1 - Em tempo real;
2.4.4.9.2 - Manual;
2.4.4.9.3 - Pré-agendada.
2.4.4.10 - Programar obrigatoriamente uma das seguintes ações, executadas automaticamente quando ocorrer a detecção de códigos maliciosos, como as opções definidas nos subitens:
2.4.4.10.1 - Limpar;
2.4.4.10.2 - Apagar;
2.4.4.10.3 - Quarentenar.
2.4.4.10.3.1 - A quarentena consiste em um mecanismo que deve inutilizar a execução do código malicioso.
2.4.4.11 - O agente da solução deve registrar e gravar os eventos de detecção de código malicioso.
2.2.4.12 - Possuir funcionalidades de HIPS (Host Intrusion Prevention System) e firewall de host integrados (gerenciados por console do mesmo fabricante da solução) e com opção de atualização automática dos bancos de assinaturas (ou equivalentes).
2.2.4.12.1 - Permitir a criação manual de regras personalizadas para as funcionalidades de firewall e HIPS.
2.4.5 - Sobre a Configuração:
2.4.5.1 - Bloquear o acesso às configurações do agente da solução para que as configurações estabelecidas pelo servidor da solução sejam mantidas.

2.4.5.2 - Bloquear a remoção e a paralisação do agente da solução por usuários que não sejam o administrador do produto ou administrador local da máquina.
2.4.5.2.1 - Deve ser solicitada senha específica da solução para permitir a remoção do produto.
2.4.6 - Sobre a Atualização:
2.4.6.1 - Atualizar remotamente, o banco de assinaturas da solução, sem a necessidade de utilização de login-scripts nem intervenção do usuário.
2.4.6.2 - Permitir atualização incremental do banco de assinaturas da solução.
2.4.6.3 - Permitir a programação de atualizações automáticas do banco de assinaturas da solução, a partir de local predefinido da rede ou de site da Internet, com frequência compatível ao surgimento de vacinas e horários definidos pelo administrador da solução, sem interrupção do usuário.
2.4.6.4 - Possuir mecanismo de "rollback" para atualização da base de assinaturas da solução.

2.5 – Criptografia de dados armazenados
2.5.1 - A funcionalidade de criptografia poderá ser fornecida através de solução integrada à solução de endpoint ou separada, desde que essa funcionalidade seja fornecida pelo mesmo fabricante da solução de endpoint;
2.5.2 - Deve possibilitar tanto o uso de criptografia em nível de pastas e arquivos quanto a criptografia total de disco;
2.5.3 - Deve possibilitar a criptografia de mídias removíveis;
2.5.4 - Deve possibilitar o gerenciamento centralizado dos recursos criptografados e das chaves de criptografia;
2.5.5 - Deve possuir recursos para recuperação de chaves pelo administrador da solução;
2.5.6 - Deve ser compatível com os sistemas operacionais Windows, MacOS e Linux.

2.6 – Recurso de EDR
2.6.1 - A funcionalidade de EDR (Endpoint Detection and Response) poderá ser fornecida através de solução integrada à solução de endpoint ou separada, desde que essa funcionalidade seja fornecida pelo mesmo fabricante da solução de endpoint;
2.6.2 - A funcionalidade de EDR deve permitir o monitoramento e registro das atividades das máquinas, possibilitando as seguintes ações:
2.6.2.1 - Registro das ações realizadas por arquivos no sistema operacional e sistema de arquivos da máquina;
2.6.2.2 - Registro das portas de comunicação abertas e do tráfego gerado por arquivos executados em uma máquina;
2.6.2.3 - Realizar o armazenamento dos eventos detectados em uma base de dados centralizada;
2.6.2.4 - Possibilitar a análise e correlação dos eventos detectados;
2.6.2.5 - Possibilitar a emissão de relatórios e alertas dos eventos identificados;
2.6.2.6 - Possibilitar a tomada de medidas de reação para a contenção de ameaças, tais como: apagar, quarentenar e isolar arquivos suspeitos, bem como realizar rollback de arquivos infectados.

2.7 – Proteção para estações de trabalho VDI
2.7.1 - A funcionalidade de proteção da infraestrutura de estações de trabalho virtualizadas (tecnologia VDI - Virtual Desktop Infraestructure) poderá ser fornecida através de solução integrada à solução de endpoint ou separada, desde que essa funcionalidade seja fornecida pelo mesmo fabricante da solução de endpoint;
2.7.2 - A solução para a proteção de VDI deverá permitir o uso de Agente Mínimo (light

agent), que centraliza funções como varredura de arquivos comuns e download de assinaturas, ocupando menos recursos de processamento de CPU, memória RAM e espaço em disco em comparação ao que é utilizado por um agente completo da solução em uma máquina física;
2.7.2.1 - O Agente mínimo que será utilizado nas estações de trabalho virtuais deverá fornecer pelo menos as seguintes funcionalidades de proteção, para todas os sistemas operacionais suportados:
2.7.2.1.1 - Antimalware e antispyware baseado em assinatura;
2.7.2.1.2 - Firewall;
2.7.2.1.3 - HIPS (IPS de Host);
2.7.2.1.4 – Permitir a criação manual de regras personalizadas para as funcionalidades de firewall e HIPS.
2.7.3 - O agente mínimo da solução para o uso na infraestrutura de VDI deverá ser compatível pelo menos com os seguintes sistemas operacionais:
2.7.3.1 - Windows 7 e superiores;
2.7.3.2 - Ubuntu 16 e superiores;
2.7.4 - A solução de proteção para estações de trabalho virtuais (VDI) deverá ser compatível pelo menos com as seguintes plataformas de virtualização:
2.7.4.1 - Citrix XenDesktop 7.11 e superiores;
2.7.4.2 - Red Hat Virtualization 4.2 e superiores;
2.7.4.3 – VMware Horizon 7.6 e superiores;

2.8 – Licenciamento da solução
2.8.1 - A contabilização de licenças será realizada por nó (estação de trabalho/servidor) da rede local.
2.8.1.1 – Para a proteção de estações de trabalho VDI (item 2.7) a contabilização de licenças deverá ser baseado por núcleo (processadores) das máquinas hospedeiras (máquinas físicas). Ou seja, o licenciamento ocorrerá pela quantidade de processadores utilizados para cada máquina física (Host) do ambiente de VDI.
2.8.2 - A tabela a seguir apresenta o volume de licenças estimadas:

1º ANO		2º ANO		3º ANO		4º ANO	
Licenças	Manutenção	Licenças	Manutenção	Licenças	Manutenção	Licenças	Manutenção
25.000	-	2.000	25.000	3.000	27.000	3.000	30.000

2.8.3 - Descrição da manutenção e atualização:
2.8.3.1 - Manutenção: Consiste em correções de erros de software identificados durante a utilização dos produtos, bem como a elucidação de dúvidas e investigação de supostos erros.
2.8.3.2 - Atualização: consiste no fornecimento gratuito de novas versões e releases no decorrer da vigência do contrato e atualização de assinaturas e engines.
2.8.4 - Prazos e Locais de Entrega
2.8.4.1 - A empresa vencedora terá até 10 (dez) dias corridos a partir da assinatura do contrato, para fornecer 1 (um) certificado de licenciamento emitido pelo fabricante e o software de instalação da solução. Observando a necessidade da disponibilização dos instaladores da solução para realização dos testes de homologação antes da adjudicação.

2.8.4.1.1 - Esse certificado será entregue no Protocolo Geral do SERPRO, no endereço SGAN - Quadra 601 - Módulo G – Brasília.
2.8.5 - Da manutenção:
2.8.5.1 - Durante a vigência do contrato, o atendimento ao SERPRO para este serviço será realizado por telefone, podendo também ser realizado por e-mail e, quando solicitado, se dará de forma presencial (on-site) em um dos locais a seguir, a ser definido pelo SERPRO no momento da abertura do chamado, cito: Recife/PE, Av. Parnamirim, 295 Parnamirim CEP 52.060-000, ou em Brasília, no endereço SGAN 601 MÓDULO G Asa Norte - Brasília/DF CEP 70.836-900.

3.0 Níveis de serviço e sancionamentos

3.1. Deverá ser prestado remotamente ou *on-site* pela CONTRATADA serviço de suporte técnico e manutenção, inerente a contratação, destinado a resolver defeitos, problemas de desempenho, sanar dúvidas relacionadas com a instalação, configuração, *upgrade* e uso dos softwares.

3.2 Período de Atendimento e Níveis de Severidade

3.2.1. O atendimento pela CONTRATADA será prestado 24 (vinte e quatro) horas por dia durante os 7 (sete) dias da semana, incluindo feriados, de acordo com o nível de severidade definido para cada caso:

Severidade		Descrição	Tipo de Atendimento	Tempo de Atendimento	Tempo de Solução
1	**Crítica**	Chamados referentes à situação de emergência ou problemas críticos, caracterizados pela existência de sistema parado.	Remota (*) ou on-site	No máximo 2 (dois) horas corridas após a abertura do registro chamado, incluindo percurso do técnico até as instalações do SERPRO.	No máximo 4 (quatro) horas corridas após a abertura do chamado, para aplicar a solução ou a medida de contorno.
2	**Alta**	Chamados associados a situações de alto impacto, referentes ao uso do produto.	Remota (*) ou on-site	No máximo 2 (dois) horas corridas após o registro da abertura do chamado, incluindo percurso do técnico até as instalações do SERPRO.	No máximo 6 (seis) horas corridas após a abertura do chamado, para aplicar a solução ou a medida de contorno.

3	**Média**	Chamados referentes a situações de baixo impacto ou para aqueles problemas que se apresentem de forma intermitente.	Remota	No máximo 4 (quatro) horas corridas após a abertura do registro do chamado.	No máximo 8 (oito) horas corridas após a abertura do chamado, para aplicar a solução ou a medida de contorno.
4	**Baixa**	Chamados para formular perguntas com o objetivo de sanar dúvidas quanto ao uso ou à implementação do produto.	Remota	No máximo 12 (doze) horas corridas após a abertura do registro do chamado.	No máximo 24 (vinte e quatro) horas corridas para concluir o chamado após a abertura do chamado.
***Exceção das situações em que sejam necessárias intervenções físicas.**					

3.2.2. **Sistema Parado** é a situação em que há impossibilidade total de uso de um serviço prestado ao SERPRO, em razão de defeito em um ou mais produtos fornecidos pela CONTRATADA.
3.2.3. **Tempo de Atendimento** é o prazo máximo para início do atendimento a partir da abertura do chamado na CONTRATADA.
3.2.4. **Tempo de Solução** é o prazo máximo para que a CONTRATADA aplique uma correção definitiva ou solução de contingência para o problema reportado a partir do início do atendimento.
3.2.5. Quando necessário, a CONTRATADA deverá assistir *on-site* na instalação e uso dos software(s) ofertado(s), fornecendo orientações para diagnóstico de problemas e ajuda na interpretação de *traces*, *dumps* e *logs*. Nos casos de defeitos não conhecidos, as documentações enviadas pelo SERPRO (tais como: *traces*, *dumps* e *logs*) deverão ser encaminhadas aos laboratórios do fabricante a fim de que sejam fornecidas as devidas correções.
3.2.6. Em quaisquer casos e quando necessário, a CONTRATADA deverá fornecer informações sobre as correções a serem aplicadas ou a própria correção.

3.2.7. Em qualquer hipótese (e ainda que não seja o fabricante dos softwares) a CONTRATADA deverá possuir acesso para suporte técnico de 1º, 2º e 3º níveis junto ao fabricante. Para todos os efeitos da contratação em espécie, vigoram os seguintes conceitos:
3.2.7.1. **Suporte Técnico Primeiro Nível:** equipe treinada e certificada pelo fabricante para atender diretamente os usuários em demandas referentes a diagnóstico e tratamento de problemas, configuração e administração do ambiente e esclarecimento de dúvidas em geral.
3.2.7.2. **Suporte Técnico Segundo Nível:** equipe multidisciplinar treinada, certificada e com grande experiência em ambientes críticos e complexos, que exigem alta disponibilidade.
3.2.7.3. **Suporte Técnico Terceiro Nível:** equipe do fabricante, devido à necessidade de retaguarda nas tecnologias suportadas.

3.3 Chamados, Registros e Início de Prazos
3.3.1. Será aberto um chamado para cada problema reportado.

3.3.2. A abertura do chamado na CONTRATADA pelo SERPRO poderá ser realizado por meio de telefone ou WEB.
3.3.2.1. Atendimento por meio de canal telefônico gratuito 0800, 24 (vinte e quatro) horas por dia, 7(sete) dias por semana.
3.3.2.2. Chamado técnico por meio de site na Internet, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.
3.3.3. Os prazos para atendimento de chamados de qualquer severidade serão considerados a partir da hora em que o chamado é aberto, isto é, registrado na CONTRATADA, recebendo dela uma identificação para acompanhamento, controle e histórico.

3.4. Prazos para primeiro atendimento
3.4.1. Chamados de Severidade 1 – CRÍTICA
3.4.1.1. Os chamados de Severidade 1 serão atendidos remotamente ou *on-site* em no máximo 2 (dois) horas corridas após a abertura do registro do chamado, incluindo o percurso do técnico até as instalações do SERPRO, e contarão com esforço concentrado da CONTRATADA para aplicar a solução ou a medida de contorno em até 4 (quatro) horas corridas após a abertura do registro do chamado.
3.4.1.2. O atendimento de Severidade 1 não poderá ser interrompido até o completo restabelecimento dos serviços envolvidos, mesmo que se estenda por períodos noturnos e dias não úteis.
3.4.1.3. O atendimento de Severidade 1, quando remoto, poderá sofrer intervenções físicas em casos de exceção das situações.

3.4.2. Chamados de Severidade 2 – ALTA
3.4.2.1. Os chamados de Severidade 2 serão atendidos remotamente ou *on-site* em no máximo 2 (dois) horas corridas após a abertura do registro do chamado, incluindo o percurso do técnico até as instalações do SERPRO, e contarão com esforço concentrado da CONTRATADA para aplicar a solução ou a medida de contorno em até 6 (seis) horas corridas após a abertura do registro do chamado.
3.4.2.2. Os chamados de severidade 2 não poderão ser interrompidos até o completo restabelecimento dos serviços envolvidos, mesmo que se estenda por períodos noturnos e dias não úteis.
3.4.3.3. O atendimento de Severidade 2, quando remoto, poderá sofrer intervenções físicas em casos de exceção das situações.

3.4.3. Chamados de Severidade 3 – MÉDIA
3.4.3.1. Os chamados de Severidade 3 serão atendidos remotamente em no máximo 4 (quatro) horas corridas após a abertura do registro do chamado, e contarão com esforço concentrado da CONTRATADA para aplicar a solução ou a medida de contorno em até 8 (oito) horas corrida após a abertura do registro do chamado.
3.4.3.2. Os chamados classificados com Severidade 3 serão atendidos em horário comercial, ou seja, das 08h00min às 17h00min, de segunda-feira a sexta-feira, horário de Brasília.
3.4.3.3. Caso o problema não possa ser resolvido remotamente, a CONTRATADA deverá colocar à disposição do SERPRO um especialista devidamente habilitado e credenciado, que trabalhará o tempo que for necessário para a solução do problema, cujo ônus financeiro de tal providência será da CONTRATADA.

3.4.4. Chamados de Severidade 4 – BAIXA

3.4.4.1. Os chamados de Severidade 4 serão atendidos em no máximo 12 (doze) horas corridas após o registro da abertura do chamado e deverão ser concluídos em até 24 (vinte e quatro) horas corridas após a abertura do registro do chamado.
3.4.4.2. Os chamados classificados com Severidade 4 serão atendidos em horário comercial, ou seja, das 08h00min às 17h00min, de segunda-feira a sexta-feira, horário de Brasília.

3.5. Monitoramento do Atendimento dos Chamados
3.5.1. Todos os chamados serão controlados por sistema de informação da CONTRATADA.
3.5.2. Para efeito de acompanhamento das providências e do tempo decorrido desde a sua abertura, o SERPRO será informado sobre cada abertura e fechamento de chamado efetuado por força da presente contratação.
3.5.3. O fechamento do chamado poderá se dar quer pela aplicação da correção definitiva do produto ou da solução de contingência que possibilite a operação do sistema.
3.5.4. A disponibilização de medida corretiva definitiva poderá, a critério da CONTRATADA, vir a ser incorporada em futuras versões do software.
3.5.5. Antes do fechamento de cada chamado a CONTRATADA consultará o SERPRO para validar o fechamento do chamado.
3.5.6. Um chamado fechado sem anuência do SERPRO ou sem que o problema tenha sido de fato resolvido, será reaberto e os prazos serão contados a partir da abertura original do chamado, inclusive para efeito de aplicação das sanções previstas.
3.5.7. A CONTRATADA deverá cadastrar pelo menos 03 (três) pessoas, indicadas pelo SERPRO e apenas essas pessoas estarão autorizadas a abrir e fechar os chamados.

3.6. Penalidades
3.6.1. Pelo descumprimento dos níveis de serviços acordados, o SERPRO aplicará as sanções abaixo à CONTRATADA, a qual sujeitar-se-á ao pagamento de multas escalonadas tendo como base o valor total do contrato, a menos que haja justificativa formal apresentada pela CONTRATADA e aceita pelo SERPRO:
3.6.1.1. **Severidade 1 (Crítica):** 0,05% (cinco centésimos por cento) do valor TOTAL do contrato, por hora ou fração de hora de atraso.
3.6.1.2. **Severidade 2 (Alta):** 0,04% (quatro centésimos por cento) do valor TOTAL do contrato, por hora ou fração de hora de atraso.
3.6.1.3. **Severidade 3 (Média):** 0,03% (três centésimos por cento) do valor TOTAL do contrato, por hora ou fração de hora de atraso.
3.6.1.4. **Severidade 4 (Baixa):** 0,01% (um centésimos por cento) do valor TOTAL do contrato, por hora ou fração de hora de atraso.

3.6.2. Pelo descumprimento do prazo da entrega das licenças, estabelecido no item 2.7.4. será aplicada multa no valor de 0,3% (zero vírgula três por cento) do valor total do contrato por dia de atraso, não podendo ultrapassar o limite máximo de 10% (dez por cento) do valor do contrato.

3.6.3. O percentual total de multa não poderá sob hipótese alguma ser superior a 20% (vinte por cento) do valor total do contrato.

3.7. Relatórios sobre a prestação dos serviços
3.7.1. A CONTRATADA mensalmente deverá entregar um relatório constando os acionamentos técnicos efetuados no período, por regional, com o mínimo de informações

de número de acionamento, descrição da ocorrência, severidade, data e hora de abertura do chamado, data e hora do início do atendimento, data e hora de conclusão e descrição da resolução adotada. O relatório deverá ser entregue mesmo quando não houver chamados no período.
3.7.2. A entrega dos relatórios mensais será condição necessária para o SERPRO realizar o ateste da nota fiscal e/ou fatura, para fins de pagamento dos serviços executados.

3.8. Os serviços, via web, deverão estar disponíveis 24 x 7 com a disponibilidade mensal, no mínimo, de **98,5%** (noventa e oito vírgula cinco por cento).
3.8.1. O tempo de interrupção para efetuar atividades de manutenção planejadas, atualizações de sistemas operacionais e atualizações de softwares envolvidos na prestação do serviço não serão computadas no cálculo geral de disponibilidade do serviço. As atividades de manutenção programada serão previamente comunicadas e acordadas entre as partes.
3.8.2. Pelo descumprimento da disponibilidade estabelecida no item 3.8. será aplicada multa no valor de 1% (um por cento) do valor total do contrato.

3.9. Os registros dos chamados, com as respectivas soluções de contorno, ficarão disponíveis por 365 dias para consulta, via site disponibilizado pela CONTRATADA.

4.0 Especificação de valores e forma de pagamento

4.1 - FORMA DE PAGAMENTO:
4.1.1 - O pagamento das licenças adquiridas será efetuado em parcela única, no 20o (vigésimo) dia corrido do mês subsequente às aquisições.
4.1.2 - O pagamento da Manutenção se dará mensalmente, no 20o (vigésimo) dia corrido do mês subseqüente à sua execução.
4.1.3 - Para a efetivação do pagamento o Serpro deverá receber os certificados de uso de software emitido pelo fabricante do produto, de acordo com os reportes realizados, bem como a nota fiscal e/ou fatura, relacionando as licenças reportadas e os valores referentes ao mês de manutenção, que deverá ser entregue em duas vias, no Protocolo Geral do Serpro, sito no SGAN - Quadra 601 - Módulo G - Brasília - DF.
4.1.3.1 - As notas fiscais deverão ser emitidas de acordo com os dados abaixo:
Razão Social : Serviço Federal de Processamento de Dados - Serpro
Endereço: SGAN - Quadra 601 - Módulo G - Asa Norte - Brasília/DF - CEP 70830-900
CNPJ : 33.683.111/0002-80
Inscrição estadual: 07.334.743/002-94

5.0 Justificativa da contratação

6.0 Seleção do fornecedor

6.1. A contratação será realizada na Modalidade de Pregão, na forma eletrônica conforme disposto no Art. 32, inciso IV, da Lei 13.303/2016 c/c Lei n° 10.520/2002.
6.2. Será considerada vencedora do processo licitatório a empresa que apresentar proposta com o menor preço global.
6.3. Apresentar Atestado de Capacidade Técnica de acordo com Cláusula editalícia padrão do SERPRO.

7.0 Justificativa para aceitação de preços

Não se aplica

8.0 Gerenciamento contratual

8.1. Obrigações da CONTRATADA
8.2. Ter publicado na Internet a especificação dos softwares ofertados.
8.3. Fornecer a documentação técnica, em português e/ou inglês, necessária à instalação, ao uso, à administração, ao controle, à monitoração e à operação dos softwares adquiridos.
8.4. Caso haja atualização de release, a CONTRATADA deverá manter o funcionamento do ambiente durante a vigência do contrato ininterruptamente.
8.5. Os produtos deverão ser entregues em um conjunto de mídias originais de instalação e configuração com suporte a site de recuperação de desastres, além de documentação técnica, completa e atualizada, contendo os manuais, guias de instalação e outros pertinentes, em mídia eletrônica ou por meio de download ou acesso ao site do fabricante na internet.
8.6. Caso o acesso ao conteúdo dos sites necessitem de cadastramento de pessoas, deverá ser previsto o cadastramento para no mínimo 20 (vinte) pessoas.
8.7. A CONTRATADA deverá garantir que, quando da descontinuidade de um produto e lançamento de outro, o SERPRO passará a ter direito de uso do produto mais recente (sucessor) e a documentação completa sem custos adicionais durante a vigência do Contrato.
8.8. A manutenção deverá incluir o acesso, livre de qualquer ônus, ao website e à base de conhecimento da solução ofertada, bem como ao seu repositório de programas contendo correções, atualizações recentes, "drivers", programas de controle e informações.
8.8.1. Nos casos em que as manutenções necessitarem de paradas das soluções, o CONTRATANTE deverá ser imediatamente notificado para que se proceda a aprovação da manutenção ou para que seja agendada nova data, a ser definida pelo CONTRATANTE, para execução das atividades de manutenção.
8.9. Correrá por conta exclusiva da CONTRATADA a responsabilidade pelo deslocamento de sua equipe aos locais de prestação dos serviços, bem como as despesas de transporte, frete e seguro correspondente, quando acionado pelo SERPRO e não resolvido pelo Telesuporte.
8.10. O SERPRO poderá fazer uso das licenças em seus servidores em qualquer uma das suas regionais e sede, respeitando a quantidade de processadores e a modalidade de cada licença adquirida.
8.11. A instalação das licenças deverá ocorrer de forma automática para as estações do SERPRO e de seus clientes, de forma que as mesmas não fiquem sem conexão com o respectivo servidor de atualização e que não gere impacto para o SERPRO e seus clientes.
8.12. Caso haja migração das licenças, todo o processo dar-se-á sem ônus para o SERPRO.
8.13. A CONTRATADA prestará toda orientação técnica necessária para a perfeita utilização dos produtos, para obtenção do máximo desempenho destes durante o período de vigência do contrato, conforme definido abaixo:
8.13.1. Identificar e corrigir problemas de funcionamento.
8.13.2. Manutenção evolutiva para integração das soluções.
8.13.3. Apoio nas definições do produto para composição de soluções.
8.13.4. Apoio na customização do produto para composição de soluções.
8.13.5. Avaliações, diagnósticos e proposições de soluções de melhoria em ambiente de produção.
8.14. Deverá ser fornecido um serviço a nível mundial de monitoramento proativo para ameaças de segurança que encaminhe notificações técnicas via e-mail.

8.15. A CONTRATADA deverá elaborar um cronograma de execução para os serviços de Suporte Técnico em até 03 (três) dias úteis após a data da assinatura do contrato, previamente acordado com a fiscalização do SERPRO, para o bom andamento dos serviços.
8.16. O reporte das licenças ocorrerá por demanda.
8.16.1. O instrumento utilizado para o reporte de novas licenças será a emissão de Ordem de Fornecimento de Bens (OF) e pelos demais instrumentos de Gestão de Contratos do SERPRO, sem a necessidade de aditivação do contrato, para esse fim.
8.16.2. Durante a vigência do contrato, o SERPRO não se obriga a reportar as quantidades totais de produtos e serviços previstos, sendo estas quantidades utilizadas como referência de preços unitários, o que permitirá ao SERPRO variar o volume de reporte a seu critério.

8.17. Do Repasse de Conhecimento
8.17.1. Como parte integrante do processo de instalação e configuração, a empresa vencedora deverá realizar o repasse de conhecimento presencial necessário para administrar, configurar, operar e gerenciar todas as licenças ofertadas.
8.17.2. O Repasse de Conhecimento para a Solução de Proteção de Estação de Trabalho e Servidores e para a Solução de Gestão e Análise de Ambiente será prestado sem ônus para o SERPRO e deverá ser ministrado para 24 (vinte e quatro) empregados, no total, a serem indicados pelo SERPRO, conforme descrito a seguir:
8.17.2.1. O Repasse de Conhecimento para a Solução de Proteção de Estação de Trabalho e Servidores será prestado sem ônus para o SERPRO e deverá ser ministrado para 12 (doze) empregados a ser realizado em Recife – PE, conforme definição do SERPRO.
8.17.3. A duração do repasse de conhecimento será de 40 (quarenta) horas semanais e 8 (oito) horas por dia, ou seja, serão necessárias 40 (quarenta) horas para cada uma das duas turmas. O repasse de conhecimento técnico deve contemplar os conhecimentos relativos a arquitetura, a instalação, a configuração e o gerenciamento, de acordo com as necessidades a serem indicadas pelo SERPRO.
8.17.4. Todas as despesas com material, equipamentos, instrutores, deslocamento de instrutores e demais itens serão de responsabilidade da CONTRATADA e sem ônus para o SERPRO.
8.17.5. A CONTRATADA deverá prover toda a logística e todo o material necessário à execução do repasse de conhecimento teórica e prática, ou seja, instalações adequadas, equipamentos, manuais e apostilas didáticas.
8.17.6. O repasse de conhecimento deverá ser realizado utilizando conteúdo teórico e prático, por meio de laboratório preparado com as ferramentas solicitadas para esta capacitação, cujas funcionalidades foram solicitadas nas especificações técnicas.
8.17.7. A CONTRATADA deverá disponibilizar, em até 30 (trinta) dias após a data da assinatura do contrato, um cronograma com a data de início do repasse, o qual deverá ser aprovado pelo SERPRO.
8.17.7.1. Todo o material deverá ser fornecido ao SERPRO com um mínimo de 15 (quinze) dias corridos de antecedência do início de cada repasse para avaliação prévia de seu conteúdo.
8.17.8. O SERPRO deverá comunicar formalmente a CONTRATADA, com antecedência mínima de 5 (cinco) dias, a ocorrência de fato impeditivo para a realização do repasse de conhecimento.
8.17.9. O repasse de conhecimento deverá ser executado por profissionais capacitados pelo fabricante dos softwares ofertados. O conteúdo programático deverá ser o oficial do fabricante

das licenças. A CONTRATADA poderá subcontratar empresas especializadas, que possuam autorização do fabricante, sendo que o profissional deverá ser devidamente capacitado.
8.17.10. Deverá ser emitido certificado e entregue para cada participante que obtiver 70% (setenta por cento) de frequência, em até 10 (dez) dias corridos após o término do repasse de
conhecimento.
8.17.11. Ao final do repasse de conhecimento, o SERPRO fará uma avaliação na qual a CONTRATADA deverá obter no mínimo 70% (setenta por cento) de conceitos "bom" ou "ótimo".
8.17.11.1. Caso não seja alcançado o mínimo exigido, conforme descrito no item 8.16.11, haverá a necessidade de realização de outro repasse de conhecimento.
8.17.12. A CONTRATADA deverá iniciar o repasse de conhecimento em até 03 (três) meses após a data de assinatura do contrato..

9.0 Considerações gerais

N/C.

Anexos

Nenhum Anexo encontrado.