Secretaria de Estado da Segurança Pública

ESTADO DE GOIÁS
SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA
GERÊNCIA DE TELECOMUNICAÇÕES

TERMO DE REFERÊNCIA

1. OBJETO

1.1. **Registro de Preços para eventual aquisição de licenças de software antivírus incluindo garantia, atualização de versão e suporte técnico por 30(trinta) meses** para proteção de estações de trabalho e servidores de aplicações conectados na Rede Corporativa da SSPGO.

2. JUSTIFICATIVAS

2.1. A Gerência de Telecomunicações da SSPGO tem entre suas principais atribuições:

2.1.1. "Gestão de Segurança da Informação, definição de Política de Segurança, controle de acesso, análise e correção de vulnerabilidades em aplicações e rede corporativa."

2.1.2. "Gerência e Configuração de Servidores de Virtualização, Antivírus, Firewall, Anti-Spam, Filtro de Conteúdo Web e Sistema de Prevenção de Intrusão (IPS)."

2.1.3. "Análise e especificação de ferramentas, equipamentos e serviços de TI e de Telecomunicações para aquisição ou contratação. "

Para o correto atendimento destas atribuições é necessário a implantação de infraestrutura técnica visando garantia de sigilo e integridade dos dados contra acesso indevido, fornecendo segurança para estações de trabalho, dispositivos móveis e servidores de aplicações, sejam físicos ou virtuais, conectados na Rede Corporativa da Instituição.

2.2. A Lei Geral de Proteção de Dados Pessoais (LGPD) - LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, que entrará em vigor a partir de Agosto de 2020, torna obrigatório a definição de mecanismos formais que visem auxiliar no controle sobre o tratamento de dados nas instituições conforme abaixo:

"Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

"Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios."

"Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito."

"Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término."

2.3. De acordo com a norma internacional ISO IEC 27001:2006, que trata da certificação para Sistemas de Gestão de Segurança da Informação e apresenta entre seus conceitos fundamentais os três atributos básicos da informação: confidencialidade, integridade e disponibilidade, é necessário que esta Gerência, responsável pela Infraestrutura de TI da SSPGO, no exercício de suas atribuições institucionais, promova e mantenha ações que permitam identificar, analisar e qualificar riscos que possam comprometer as informações que trafegam e que são acessadas por seus usuários finais.

2.4. Em decorrência disso, é fundamental a definição de estratégias que unifiquem os propósitos desses pilares da Segurança da Informação. Dentre as medidas de segurança que garantem a proteção e a preservação das informações da Instituição, destaca-se a utilização de uma ferramenta de detecção e de prevenção de contaminações ou ataques de programas maliciosos, como vírus e malwares em geral, que possam vir a comprometer os dados e informações do negócio.

2.5. Uma solução de antivírus corporativo é uma solução de combate à vírus e malwares, com definições de políticas, regras de segurança e tarefas que permitem uma gestão centralizada, com instalação e atualização de vacinas de forma automatizada com proteção abrangente em vários tipos de dispositivos e computadores e com um controle e visão gerencial unificados por meio de relatórios e notificações em tempo real.

2.6. A solução de antivírus corporativo permite manter todo o ambiente computacional protegido contra contaminações por vírus provenientes de mídias removíveis como pendrives ou discos rígidos portáteis, pelo recebimento de mensagens de correio eletrônico, através de acessos às estações de trabalho, à internet e acesso por meio de notebooks e outros dispositivos móveis similares e contaminados por vírus.

2.7. Esta aquisição busca evitar o acesso indevido e roubo de informações no ambiente de TI da SSPGO de tal forma que o serviço fim da Instituição seja prestado ao cidadão de forma segura e confiável.

2.8. Atualmente a SSPGO possui solução de antivírus ativa. No entanto a mesma não permite mais atualizações, está obsoleta e deixa o ambiente vulnerável a ameças de vírus, exigindo a substituição devido a novos tipos de ataques que já não consegue tratar adequadamente.

2.9. Justifica-se a duração contratual pelo período de 30(trinta) meses devido ao alto impacto e alta complexidade de ativação dos serviços na rede corporativa. Tal ativação implica na remoção do atual antivírus e instalação do novo em 5.000(cinco mil) estações de trabalho que estão conectadas à rede da SSPGO, necessitando a mobilização das equipes de infraestrutura de TI e atendimento ao usuário, gerando custo técnico e operacional em trabalho a ser executado durante meses devido a características técnicas, fatores estes que fazem com que o processo de ativação seja demorado. Por isso, períodos curtos de contratos podem acarretar altos custos para substituição da arquitetura sempre que for necessário a mudança do serviço.

3.QUANTIDADES E VALORES

Quantidades e Valores Estimados

Item	Código	Descrição	QTD	Valor Unitário	Valor Total
1	64597	Licença de software antivírus incluindo garantia, atualização de versão e suporte técnico por 30(trinta) meses	5.000	R$ 45,84	R$ 229.212,50

Item	Código	Descrição	QTD	Valor Unitário	Valor Total
O valor total estimado do contrato pelo período de 30(trinta) meses é de R$ 229.212,50 (Duzentos e vinte e nove mil, duzentos e doze reais e cinquenta centavos).					

4. ESPECIFICAÇÕES

4.1. Possuir uma única console de gerenciamento para gestão e configurações do antivírus, antispyware, firewall, detecção de intrusão, controle de dispositivos, controle de aplicações e criptografia de discos;

4.2. A solução deverá ter a capacidade de remoção do atual antivírus instalado e ser capaz de instalar de forma remota o agente do antivírus pela console de gerenciamento, e caso não tenha a capacidade de realização a remoção completa, a contratada deverá remover a atual solução utilizando scripts, softwares de terceiros, ou mesmo de forma manual;

4.3. O produto deverá possuir no mínimo os seguintes módulos e funcionalidades:

4.3.1. Console de gerenciamento fornecendo funcionalidades de gestão e configurações de políticas;

4.3.2. Módulos para estações físicas, notebooks e servidores;

4.3.3. Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;

4.3.4. Módulo para dispositivos móveis no mínimo para tablets e smarthpones com sistema operacional iOS e Android;

4.3.5. Utilizar o conceito de heurística;

4.3.6. Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit);

4.3.7. Oferecer tecnologia nativa no intuito de eliminar ameaças que sequestram dados, do tipo ransomware;

4.3.8. Oferecer inventário de softwares;

4.3.9. Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção;

4.3.10. Oferecer proteção por base de assinaturas (vacinas).

4.4. CONSOLE DE GERENCIAMENTO

4.4.1. Instalação e configuração:

4.4.1.1. Deve ser fornecido como um appliance virtual ou executável para instalação em servidores Windows. Deverá suportar no mínimo os seguintes Hypervisors:

4.4.1.1.1. VMWare vSphere;

4.4.1.1.2. Citrix XenServer; XenDesktop, VDI-in-a-Box;

4.4.1.1.3. Microsoft Hyper-V;

4.4.1.1.4. Red hat Enterprise Virtualization;

4.4.1.1.5. Kernel-based Virtual Machine ou KVM;

4.4.1.1.6. Oracle VM;

4.4.1.2. Deverá ser fornecido com base de dados embutida e proprietária ou com possibilidade de utilização de banco de dados SQL ou Oracle. *Licenças do BD utilizado deverão ser fornecidas;*

4.4.1.3. Permitir instalação remota via console WEB de gerenciamento para ambientes virtual VMWare ou Citrix;

4.4.1.4. O mecanismo de varredura deverá estar disponível para download separadamente;

4.4.1.5. A solução deverá permitir a inclusão de um módulo de balanceamento para casos em que vários servidores tenham a mesma função (para alta disponibilidade, recuperação de desastres, performance, dentre outras necessidades);

4.4.1.6. Deve ser totalmente em português.

4.4.2. Características Gerais:

4.4.2.1. Licenciamento flexível;

4.4.2.2. Arquitetura simples de atualização, com um simples clique deve ser possível atualizar todas funções e serviços;

4.4.2.3. Permitir que o administrador escolha qual o pacote será atualizado;

4.4.2.4. As notificações devem ser destacadas como item não lido e notificar o administrador por e-mail;

4.4.2.5. No mínimo enviar notificações para as seguintes ocorrências:

4.4.2.5.1. Problemas com licenças;

4.4.2.5.2. Alertas de surto de vírus;

4.4.2.5.3. Máquinas desatualizadas;

4.4.2.5.4. Eventos de antimalware.

4.4.3. Painel para Monitoramento:

4.4.3.1. Baseado em “portlets” configuráveis com no mínimo as seguintes especificações:

4.4.3.1.1. Nome;

4.4.3.1.2. Tipo de relatório;

4.4.3.1.3. Alvo do relatório;

4.4.3.2. Deverá disponibilizar “portlets” para qualquer serviço de segurança, máquinas físicas, virtuais, dispositivos móveis.

4.4.4. Inventário da Rede:

4.4.4.1. Possuir no mínimo as integrações abaixo:

4.4.4.1.1. Múltiplos domínios do Active Directory;

4.4.4.1.2. Múltiplos VMWare vCenters;

4.4.4.1.3.Múltiplos Citrix Xen Servers;

4.4.4.2. Possuir a possibilidade de definição de sincronização com o Active Directory em horas;

4.4.4.3. Descoberta de rede para máquinas em grupo de trabalho;

4.4.4.4. Possuir busca em tempo real pelo menos com os seguintes filtros:

4.4.4.4.1. Nome;

4.4.4.4.2. Sistema Operacional;

4.4.4.4.3. Endereço IP;

4.4.4.5. Possibilitar a instalação remota e desinstalação remota do antivírus;

4.4.4.6. Possibilitar a configuração de pacotes de instalação do produto de antivírus;

4.4.4.7. Possuir tarefas remotas e configuráveis de scan;

4.4.4.8. Possuir tarefa de reinicialização remota de estação ou servidor;

4.4.4.9. Assinar políticas para no mínimo os níveis:

4.4.4.9.1. Computador;

4.4.4.9.2. Máquina Virtual;

4.4.4.9.3. Grupo de Endpoints;

4.4.4.9.4. Usuário do AD;

4.4.4.9.5. Grupo do AD;

4.4.4.10. Possuir a propriedade detalhada de objetos gerenciados para:

4.4.4.10.1. Nome;

4.4.4.10.2. IP;

4.4.4.10.3. Sistema Operacional;

4.4.4.10.4. Grupo;

4.4.4.10.5. Política Assinada;

4.4.4.10.6. Último status de malware.

4.4.5. Políticas:

4.4.5.1. Modelo único para todos os equipamentos, sejam físicos ou virtuais;

4.4.5.2. Cada serviço de segurança deve ter seu modelo configurável de política com opções específicas de ativar/desativar;

4.4.5.3. Deverá configurar as funcionalidades como escaneamento do antivírus, firewall de duas vias de detecção de intrusão, controle de acesso a rede, controle de aplicação,

controle de acesso web, localização de dispositivo (Mobile), autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade.

4.4.6. Relatórios

4.4.6.1. Deverá apresentar as seguintes funcionalidades:

4.4.6.1.1. Relatório para cada serviço de segurança;

4.4.6.1.2. Facilidade de usar e visualização simplificada;

4.4.6.1.3. Agendamento, com opção de envio por e-mail para qualquer destinatário conforme escolha do administrador;

4.4.6.1.4. Filtros de agendamento de relatórios;

4.4.6.1.5. Arquivo com todas as instâncias de relatório agendados;

4.4.6.1.6. Exportar o relatório nos formatos .pdf e/ou .csv;

4.4.6.1.7. Oferecer possibilidade de criar relatórios de maneira dinâmica no *dashboard* da solução.

4.4.7. Quarentena:

4.4.7.1. Restauração remota, com configuração de localidade e deleção;

4.4.7.2. Criação e exclusão para arquivos restaurados.

4.4.8. Usuários:

4.4.8.1. Deverá apresentar no mínimo as seguintes funcionalidades:

4.4.8.1.1. Administração baseada em regras;

4.4.8.1.2. Disponibilizar tipos de usuários pré-definidos com no mínimo:

4.4.8.1.2.1. Administrador – Gerente dos componentes da solução;

4.4.8.1.2.2. Administrador de rede - Gerente dos serviços de segurança;

4.4.8.1.2.3. Relatório – Monitorar e criar relatórios;

4.4.8.1.3. Deverá ser possível customizar um tipo de usuário;

4.4.8.1.4. Deverá permitir a integração do usuário com o Active Directory para autenticação da console de gerenciamento.

4.4.9. Logs:

4.4.9.1. Registrar as ações do usuário na console de gerenciamento;

4.4.9.2. Detalhar cada ação do usuário;

4.4.9.3. Permitir busca complexa baseada em ações do usuário, intervalos de tempo.

4.4.10. Certificado de Segurança:

4.4.10.1. Deverá prover o acesso via HTTPS;

4.4.10.2. Deverá permitir a importação de certificados digitais;

4.4.10.3. O gerenciamento e a comunicação com dispositivos móveis deve ser feito de forma segura utilizando certificados digitais.

4.5. PROTEÇÃO PARA ESTAÇÕES DE TRABALHO E SERVIDORES FÍSICOS

4.5.1. Deverá apresentar no mínimo:

4.5.1.1. Deverá permitir a configuração do scan do antivírus do cliente como:

4.5.1.1.1. Scan local;

4.5.1.1.2. Scan local/remoto;

4.5.1.1.3. Scan remoto;

4.5.1.2. Deverá permitir a instalação customizada do antivírus com no mínimo:

4.5.1.2.1. Instalar o antivírus sem o controle de acesso a internet; (Windows Desktop)

4.5.1.2.2. Instalar o antivírus sem o módulo de firewall; (Windows Desktop)

4.5.1.3. Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho:

4.5.1.3.1. Windows 10 64Bits;

4.5.1.3.2. Windows 8.1 64Bits;

4.5.1.3.3. Windows 8 64Bits;

4.5.1.3.4. Windows 7 64Bits;

4.5.1.3.5. Windows XP (SP3) apenas o módulo de antivírus;

4.5.1.4. Deverá suportar no mínimo os seguintes sistemas operacionais para servidores:

4.5.1.4.1. Windows Server 2012R2;

4.5.1.4.2. Windows Server 2012;

4.5.1.4.3. Windows Server 2008 R2;

4.5.1.4.4. Windows Server 2008;

4.5.1.4.5. Windows Server 2003 R2 apenas o módulo de antivírus;

4.5.1.4.6. Windows Server 2003 com SP1 apenas o módulo de antivírus;

4.5.1.5. Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux:

4.5.1.5.1. Red Hat Enterprise Linux;

4.5.1.5.2. Cent OS 5.6 ou superior;

4.5.1.5.3. Ubuntu 10.04 LTS ou superior;

4.5.1.5.4. SUSE Linux Enterprise Sever 11 ou superior;

4.5.1.5.5. OpenSUSE 11 ou superior;

4.5.1.5.6. Debian 5.0 ou superior.

4.5.2. Gerenciamento e Instalação Remota

4.5.2.1. Deverá permitir ao administrador customizar a instalação;

4.5.2.2. A instalação deverá ser possível executar com no mínimo das seguintes maneiras:

4.5.2.2.1. Executar o pacote de antivírus diretamente na estação de trabalho;

4.5.2.2.2. Instalar remotamente, distribuído via console de gerencia web;

4.5.2.3. Deverá ser possível ter um relatório com as estações instaladas e as faltantes da instalação;

4.5.2.4. A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações:

4.5.2.4.1. Nome;

4.5.2.4.2. IP;

4.5.2.4.3. Sistema Operacional;

4.5.2.4.4. Política Aplicada;

4.5.2.5. Através da console o administrador poderá ser capaz de enviar uma política única para configurar o antivírus;

4.5.2.6. A console de gerenciamento deverá incluir sessão de log com as seguintes informações:

4.5.2.6.1. Login;

4.5.2.6.2. Edição;

4.5.2.6.3. Criação;

4.5.2.6.4. Log-out;

4.5.2.7. Ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits;

4.5.2.8. Deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;

4.5.2.9. O agente utilizado na sincronização deve ser incluído no cliente do antivírus e não ser necessário a distribuição em um agente separado.

4.6. PROTEÇÃO PARA ESTAÇÕES E SERVIDORES VIRTUAIS

4.6.1. Proteção de antivírus dedicado para ambientes virtuais

4.6.1.1. Deverá ter a disponibilidade de ser integrado com o VMWare e oferecer a escaneamento sem instalar o produto na máquina virtual;

4.6.1.2. A console de gerenciamento central da solução deverá ter a possibilidade de integrar com múltiplos vCenters da VMWare;

4.6.1.3. Deverá proteger em tempo real e agendado as máquinas virtuais Linux;

4.6.1.4. O produto deverá oferecer agente para virtualização dos seguintes produtos:

4.6.1.4.1. Citrix Xen Server;

4.6.1.4.2. Microsoft Hyper-V;

4.6.1.4.3. VMware ESXi;

4.6.1.4.4. Red Hat Virtualization;

4.6.1.4.5. Oracle VM;

4.6.1.4.6. KVM.

4.6.2. Funções Gerais

4.6.2.1. Deverá ter métodos de detecção de vírus, spyware, rootkits e outros mecanismos de segurança;

4.6.2.2. Deverá reportar o estado atual das VMs no mínimo, protegida/desprotegida;

4.6.2.3. Requisitos Mínimos do Sistema

4.6.2.3.1. Plataformas de Virtualização:

4.6.2.3.1.VMware vSphere ESX 5.0 ou superior;

4.6.2.3.2. VMware vCenter Server 4.1 ou superior;

4.6.2.3.3. Xen Server 5.5 ou superior;

4.6.2.3.4. Citrix VDI-in-a-Box 5, ou superior;

4.6.2.3.5. Microsoft Hyper-V Server 2008 R2, 2012, ou superior;

4.6.2.3.6. Oracle VM 3.0 ou superior;

4.6.2.3.7. Red Hat Enterprise Virtualization 3.0 ou superior;

4.6.2.3.2. Requisitos do Sistema

4.6.2.3.2.1. Sistemas Operacionais desktops:

4.6.2.3.2.1.1. Windows 10 64Bits;

4.6.2.3.2.1.2. Windows 8.1;

4.6.2.3.2.1.3. Windows 8;

4.6.2.3.2.1.4. Windows 7;

4.6.2.3.2.1.5. Windows XP (SP3) – Instalação apenas do módulo de antivírus.

4.6.2.3.2.2. Sistemas Operacionais Servidores:

4.6.2.3.2.1. Windows Server 2012 R2;

4.6.2.3.2.2. Windows Server 2012;

4.6.2.3.2.3. Windows Server 2008 R2;

4.6.2.3.2.4. Windows Server 2008;

4.6.2.3.2.5. Windows Server 2003 R2 Instalação apenas do módulo de antivírus;

4.6.2.3.2.6. Windows Server 2003 com SP1 Instalação apenas do módulo de antivírus;

4.6.2.3.2.7. Linux Red Hat Enterprise;

4.6.2.3.2.8. CentOS 5.6 ou superior;

4.6.2.3.2.9. Ubuntu 10.04 LTS ou superior;

4.6.2.3.2.10. SUSE Linux Enterprise Server 11 ou superior;

4.6.2.3.2.11. OpenSUSE 11 ou superior;

4.6.2.3.2.12. Fedora 15 ou superior;

4.6.2.3.2.13. Debian 5.0 ou superior.

4.7. COMPONENTES E FUNCIONALIDADE DO ANTIVÍRUS GERAL

4.7.1. Funcionalidades Gerais

4.7.1.1. Deverá fazer scan em tempo real automático;

4.7.1.2. Deverá ser configurável para não escanear arquivos conforme necessidade do administrador, ou seja, por tamanho ou por tipo de extensão;

4.7.1.3. Escaneamento de comportamento heurístico;

4.7.1.4. Deverá escanear em tempo real qualquer informação localizada em mídias de armazenamento como:

4.7.1.4.1. CD/DVD;

4.7.1.4.2. Discos Externos;

4.7.1.4.3. Pen-Drivers.

4.7.1.5. Deverá permitir a escolha e configuração de pastas a ser escaneada;

4.7.1.6. Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção:

4.7.1.6.1. Baseada em Assinaturas;

4.7.1.6.2. Baseada em Heurística;

4.7.1.6.3. Baseada em monitoramento contínuo de processos.

4.7.1.7. Deverá ter a capacidade de escaneamento nos protocolos HTTP e SSL na Estações de trabalho;

4.7.1.8. O cliente do antivírus deverá ter o módulo de Antiphishing que deverá ter a opção de verificar links pesquisados com os sites de pesquisas Search Advisor na Estações de trabalho.

4.7.2. Quarentena

4.7.2.1. Deverá permitir o envio automático de arquivos da quarentena para o laboratório de vírus;

4.7.2.2. Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador;

4.7.2.3. Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir;

4.7.2.4. Deverá de forma automática criar exclusão para arquivos restaurados da quarentena;

4.7.2.5. Deverá permitir escanear a quarentena após a atualização das atualizações de assinaturas.

4.7.3. Controle de Usuário

4.7.3.1. Deverá ter módulo de controle de usuário integrando com as seguintes características:

4.7.3.1.1. Bloqueio de acesso a internet;

4.7.3.1.2. Bloqueio de acesso a aplicações definidas pelo administrador.

4.7.4. Controle de Dispositivo

4.7.4.1. Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;

4.7.4.2. Através do módulo de controle de dispositivo deverá ser possível controlar:

4.7.4.2.1. Bluetooth;

4.7.4.2.2. CDROM/DVDROM;

4.7.4.2.3. IEEE 1284.4;

4.7.4.2.4. IEEE 1394;

4.7.4.2.5. Windows Portable;

4.7.4.2.6. Adaptadores de Rede;

4.7.4.2.7. Adaptadores de rede Wireless;

4.7.4.2.8. Discos Externos;

4.7.4.3. Deverá permitir regras de definição de bloqueio/desbloqueio;

4.7.4.4. Deverá permitir regras de exclusão.

4.7.5. Atualização

4.7.5.1. Após a atualização o administrador deverá ter a capacidade de adiar uma reinicialização;

4.7.5.2. Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;

4.7.5.3. Permitir atualizações de assinatura de hora em hora;

4.7.5.4. Permitir motor de varredura local, no servidor de rede ou em nuvem afim de aumentar o desempenho da estação de trabalho quando a mesma estiver sendo escaneada.

4.8. SEGURANÇA PARA DISPOSITIVOS MÓVEIS

4.8.1. Requisitos mínimos do Sistema Operacional para Smartphone:

4.8.1.1. Android 2.2 ou superior.

4.8.2. Recursos:

4.8.2.1. Permitir atribuir dispositivo com usuário do Active Directory;

4.8.2.2. A ativação do dispositivo da console de gerenciamento deverá ser através de um QR code;

4.8.2.3. Deverá permitir no mínimo as seguintes ações:

4.8.2.3.1. Impor bloqueio de tela e autenticação;

4.8.2.3.2. Desbloquear o dispositivo;

4.8.2.3.3. Restaurar as configurações de fábrica;

4.8.2.3.4. Localizar o Dispositivo;

4.8.2.3.5. Análise de dispositivos para o Sistema Operacional Android.

4.8.3. Configurações de Segurança:

4.8.3.1. Caso o dispositivo não esteja em conformidade com as políticas estabelecidas deverá ser possível as ações abaixo:

4.8.3.1.1. Ignorar;

4.8.3.1.2. Bloquear acesso;

4.8.3.1.3. Bloquear o dispositivo;

4.8.3.1.4. Restaurar as configurações de fábrica;

4.8.3.1.5. Remover o dispositivo do console de gerenciamento;

4.8.3.2. Deverá permitir o uso de senha. A senha pode ser configurada conforme necessidade do administrador com no mínimo os seguintes recursos:

4.8.3.2.1. Senha simples ou complexa;

4.8.3.2.2. Números e caracteres;

4.8.3.2.3. Comprimento mínimo;

4.8.3.2.4. Caracteres especiais mínimos;

4.8.3.2.5. Período de expiração da senha;

4.8.3.2.6. Definir restrição de reutilização de senha;

4.8.3.2.7. Definir o número de tentativas de entradas de senha incorretas;

4.8.3.2.8. Período de bloqueio do dispositivo.

4.9. CRIPTOGRAFIA

4.9.1. Deverá oferecer:

4.9.1.1. Possibilidade de criptografia de disco através da mesma console de gerenciamento do antivírus, seja em nuvem ou on-premise;

4.9.1.2. Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento.

5. QUALIFICAÇÃO TÉCNICA E SERVIÇOS ESPECIALIZADOS

5.1. Qualificação Técnica:

5.1.1. A empresa deverá apresentar Atestado de Capacidade Técnica fornecido por pessoa jurídica de direito público ou privado, declarando ter fornecido bens compatíveis com o objeto deste Termo de Referência;

5.1.2. Todos os atestados ou declarações exigidas deverão ser apresentados em original ou cópia autenticada por cartório competente, assinadas por pessoa responsável com indicação de nome e cargo exercido na empresa;

5.1.3. No caso de comprovação por mais de um atestado, os atestados somados ou não, deverão cobrir o quantitativo mínimo de 20% (vinte por cento) do objeto do Termo de Referência ou similar;

5.1.4. Para os itens nos quais o percentual requerido apresente fração, considerar-se-á o número inteiro imediatamente superior;

5.1.5. Não será aceito pela SSPGO atestado ou declaração emitido pela própria licitante, sob pena de infringência ao princípio da moralidade, pois a licitante não possui a impessoalidade necessária para atestar sua própria capacitação técnica.

5.2. Instalação:

5.2.1. Entende-se como fase em que se dará a instalação e configuração dos produtos, ou seja, efetiva implementação do projeto especificado;

5.2.2. A instalação e testes dos produtos devem estar inclusos no custo do produto;

5.2.3. A implementação deverá ser realizada de tal forma que as interrupções no ambiente de produção sejam as mínimas possíveis e estritamente necessárias, e, ainda, não causem transtornos aos usuários finais do órgão;

5.2.4. A CONTRATADA deverá executar testes funcionais básicos para verificar o perfeito funcionamento do ambiente. Estes testes deverão ser realizados nos componentes de hardware e software envolvidos no projeto;

5.2.5. Durante a execução dos serviços, pelo menos um representante da SSPGO participará e fará composição na equipe designada para as atividades.

5.3. Garantia e Suporte Técnico:

5.3.1. O prazo de garantia das licenças da solução ofertada deverá ser de, no mínimo, 30(trinta) meses, contados a partir da data do aceite definitivo;

5.3.2. A CONTRATADA deverá fornecer Central de Serviços para abertura de chamados técnicos em horário comercial, de 08:00 às 18:00 de segunda a sexta-feira com SLA para início

de atendimento em até 12 horas após abertura do chamado;

5.3.2.3. A Central de Serviços deverá ser acionada por meio de ligação telefônica, por e-mail ou por sistema de Service Desk disponível pela Internet, para abertura dos chamados;

5.3.2.4. Os chamados deverão ser atendidos via acesso remoto utilizando-se de softwares ou atendimento via telefone. Caso seja necessário e definido pela CONTRATANTE, o atendimento deverá ser fornecido presencialmente na modalidade on-site;

5.3.2.5. Para a prestação dos serviços de suporte remoto, deverão ser utilizados os protocolos HTTP e HTTPS da Internet, SSH ou VPN;

5.3.2.6. A CONTRATADA, sendo fabricante ou não da solução ofertada, deverá disponibilizar um telefone de suporte técnico no Brasil e em Língua Portuguesa para que a SSPGO obtenha suporte telefônico diretamente do fabricante se necessário, tantas e quantas vezes desejar durante a vigência das licenças.

5.4. Treinamento e Capacitação:

5.4.1. A capacitação deverá ser fornecida a no mínimo 04 (quatro) colaboradores da área de TI da SSPGO;

5.4.2. A capacitação deverá consistir em treinamento oficial em acordo com as políticas do fabricante da solução fornecida;

5.4.3. Deverá ser ministrado por instrutor certificado na solução e deverá fornecer, para todos os participantes, material didático oficial impresso ou eletrônico e em português;

5.4.4. O treinamento deverá ser realizado presencialmente, em infraestrutura disponibilizada pela SSPGO e deverá possuir carga horária mínima de 8 (oito) horas;

5.4.5. Após a realização da capacitação, a empresa deverá fornecer certificado de conclusão para cada participante;

5.4.6. O treinamento deverá ser realizado no prazo máximo até 30 (trinta) dias corridos, após a assinatura do contrato.

6. VIGÊNCIA, PRAZO E LOCAL DE ENTREGA/EXECUÇÃO DO OBJETO

6.1. O Contrato terá duração de 30(trinta) meses, podendo ser prorrogado até o prazo de 48(quarenta e oito) meses após o início da vigência do contrato conforme Lei 8.666/93.

6.2. O início da execução contratual deverá ocorrer em até 60 (sessenta) dias contados da publicação da outorga do contrato no Diário Oficial do Estado de Goiás.

6.3. Os serviços e/ou equipamentos deverão ser entregues na Gerência de Telecomunicação da Secretaria da Segurança Pública do Estado de Goiás.

6.4. Endereço: Avenida Anhanguera nº 7.364 – Setor Aeroviário – CEP: 74.435-300 – Goiânia - Goiás.

6.5. A entrega e instalação dos equipamentos e/ou serviços deverá ser em horário comercial (8:00h às 18:00h), de segunda-feira a sexta-feira ou em datas e horários definidos em comum acordo entre as partes.

7. VALIDADE DA ATA DE REGISTRO DE PREÇOS

7.1. Homologado o resultado da licitação, a adjudicatária será formalmente convocada para retirar, assinar e devolver a Ata de Registro de Preços que firmará o compromisso para futura contratação, a qual corresponderá à Minuta da Ata de Registro de Preços anexa ao edital adaptada à proposta vencedora, observadas as disposições da Lei nº 8.666/93 e alterações subsequentes.

7.2. **A vigência da Ata de Registro de Preços será de 12 (doze) meses**, a contar da data da publicação do seu extrato no Diário Oficial do Estado.

8. PAGAMENTO

8.1. O pagamento será realizado em até 30(trinta) dias, a contar da data de recebimento definitivo do produto e aprovado os termos das Notas Fiscais, e será efetivado por meio de crédito em conta corrente aberta exclusivamente na “Caixa Econômica Federal”, em atenção ao disposto no art. 4º da Lei nº 18.364, de 10 de janeiro de 2014.

8.2. O pagamento da(s) nota(s) fiscal(is) fica condicionado ao cumprimento dos critérios de recebimento previstos no edital.

9. RESPONSÁVEL PELA ELABORAÇÃO DO TERMO DE REFERÊNCIA

9.1. Este termo foi elaborado por Jánison Calixto dos Santos.

9.2. Dúvidas deverão ser tratadas pelo e-mail janison.calixto@ssp.go.gov.br

Documento assinado eletronicamente por **JANISON CALIXTO DOS SANTOS**, **Gerente**, em 05/12/2019, às 09:01, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

A autenticidade do documento pode ser conferida no site **http://sei.go.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=1** informando o código verificador **000010479320** e o código CRC **B898544F**.