ESTADO DE GOIÁS
DEFENSORIA PÚBLICA DO ESTADO DE GOIÁS
DEPARTAMENTO DE COMPRAS – DPE-GO

TERMO DE REFERÊNCIA

1. OBJETO

1.1. Contratação de empresa para fornecimento de licenças de uso de software "Antivírus", incluindo instalação e configuração, garantia de atualização contínua, suporte técnico e treinamento, com a finalidade de prover segurança e proteção para os equipamentos como: estações de trabalho (desktop), smartphones e notebooks da Defensoria Pública do Estado de Goiás conforme quantidades, condições e especificações técnicas descritas neste Termo de Referência:

1.2. Quantitativos e valores estimados:

LOTE	ITEM	DESCRIÇÃO DO OBJETO	QTD	VALOR MÉDIO UNITÁRIO	VALOR MÉDIO TOTAL
1	1.1.	**Aquisição de licenças complementares** de uso do software de segurança de endpoint ("Antivírus"), contemplando AntiSpyware, Controle de Dispositivos de forma centralizada por console de gerenciamento local e/ou em nuvem, com garantia de atualização e serviço de suporte técnico por **12 (doze) meses**, da marca **Bitdefender GravityZone Advanced Business Security.**	**565**	R$ 58,07	R$ 32.809,55
VALOR TOTAL ESTIMADO DO LOTE 1:					**R$ 32.809,55**
2	2.1.	**Aquisição de novas licenças** de uso do software de segurança de endpoint ("Antivírus"), contemplando AntiSpyware, Controle de Dispositivos de forma centralizada por console de gerenciamento local e/ou em nuvem, com garantia de atualização e serviço de suporte técnico por **36 (doze) meses. Bitdefender, Kaspersky, McAfee, VIPRE ou equivalente técnico.**	**1.720**	R$ 137,50	R$ 236.500,00
	2.2.	Contratação de serviço de instalação e configuração de software, referente às licenças de uso de software do item 2.1.	**1**	R$ 11.566,67	R$ 11.566,67
	2.3.	Contratação de serviço de capacitação de 16 horas (turma de até 8 alunos), referente à licenças de uso de software do item 2.1.	**1**	R$ 14.666,67	R$ 14.666,67
VALOR TOTAL ESTIMADO DO LOTE 2:					**R$ 262.733,34**

1.2.1. O preço médio estimativo apurado do Lote 01 é de **R$ 32.809,55 (trinta e dois mil oitocentos e nove reais e cinquenta e cinco centavos)** e o preço médio estimativo apurado do Lote 02 é de **R$ 262.733,34 (duzentos e sessenta e dois mil setecentos e trinta e três reais e trinta e quatro centavos).**

1.3. O objeto da licitação tem a natureza de serviço comum de Tecnologia da Informação.

1.4. Todos os itens serão fornecidos sob demanda.

1.5. O prazo de vigência das licenças que tratam o item 1.1 é de 12 (doze) meses contados a partir da data de efetivo fornecimento;

1.6. O prazo de vigência das licenças que tratam o item 2.1 é de 36 (trinta e seis) meses contados a partir da data de efetivo fornecimento;

2. JUSTIFICATIVAS

2.1. Todos os computadores (estações de trabalho e servidores), notebooks, smarthphones, bem como os serviços suportados estão vulneráveis, tanto a ataques internos, quanto externos.

2.2. Considerando a crescente evolução das ameaças digitais – vírus, malwares e suas variantes – e as descobertas diárias de vulnerabilidades nos sistemas computacionais, as quais são amplamente exploradas por softwares maliciosos, faz-se necessária a aquisição de software específico e que abranja as mais recentes funcionalidades no que se refere a proteção contra esse tipo de ameaça. Tais ameaças podem comprometer em caráter definitivo e de forma irrecuperável o ambiente computacional da DPE-GO, contaminando arquivos e sistemas, capturando dados, causando indisponibilidade e comprometendo a confiabilidade de sistemas, bem como a integridade dos dados armazenados nos computadores e servidores de rede da instituição.

2.3. No que se refere ao item 2.3 - Capacitação, há necessidade de treinamento para que os técnicos da Diretoria de Tecnologia da Informação sejam capazes de manter e otimizar o uso da solução de segurança, isto por meio da ativação e configuração das inúmeras funcionalidades contidas nesta.

2.4. Portanto, é essencial a aquisição das licenças para corroborar com o processo de garantia da disponibilidade, integridade e confiabilidade dos dados da DPE-GO, bem como com a mitigação de possíveis incidentes que comprometam a continuidade dos serviços de TI da instituição.

3. AGRUPAMENTO DE ITENS EM LOTES

3.1. Os itens 2.1 a 2.3, do Objeto deste TR, devem ser fornecidos por uma única empresa, haja vista que são partes integrantes da solução.

3.2. Em atenção aos artigos 3º, § 1º, I, 15, IV e 23, §§ 1º e 2º, todos da Lei 8.666/1993, os itens que compõem a solução são do mesmo fabricante e, por conseguinte, a adjudicação do objeto por lote tem a finalidade de evitar celebração de contrato com várias empresas para atendimento de itens interdependentes do objeto do certame

4. ESPECIFICAÇÕES TÉCNICAS

4.1. **LOTE 1 - Item 1.1 - Fornecimento de de Licenças Complementares de Solução de Segurança de Endpoint ("Antivírus").**

4.1.1. Vigência: **12 (doze) meses;**

4.1.2. Identificação do Produto: Bitdefender Gravityzone Advanced Business Security

4.1.3. Requisitos Gerais:

4.1.3.1. Prover segurança para estações de trabalho.

4.1.3.2. Possuir console central de gerenciamento, podendo ser na nuvem da Contratada ou da Contratante e/ou local da Contratante, que se comuniquem.

4.1.3.3. As configurações do Antivírus, AntiSpyware, Firewall, Detecção de intrusão controle de Dispositivos e Controle de Aplicações deverão ser realizadas através da mesma console.

4.1.3.4. O Produto deve ter a capacidade de remoção do software de antivírus já instalado e ser instalado de forma remota pela console de gerenciamento.

4.1.3.5. Utilizar o conceito de heurística;

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

4.1.3.7. Oferecer tecnologia nativa no intuito de eliminar ameaças do tipo Ransomware;

4.1.3.8. Oferecer inventário de softwares;

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

4.1.3.10. Oferecer proteção por base de assinaturas;

4.1.4. O produto deve possuir no mínimo os seguintes módulos:

4.1.4.1. Console de Gerenciamento fornecendo funcionalidades de gestão;

4.1.4.2. Módulos para estações físicas, laptops e servidores;

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

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

4.1.4. Console de Gerenciamento

4.1.4.1. Deve ser fornecido como um *appliance* virtual. Deve suportar no mínimo os seguintes Hypervisors:

4.1.4.1.1. VMWare vSphere;

4.1.4.1.2. Microsoft Hyper-V;

4.1.4.1.3. Kernel-based Virtual Machine ou KVM;

4.1.4.1.4. Xen Server;

4.1.4.2. Deve ser fornecido com base de dados embutido;

4.1.4.3. Permitir instalação remota via console WEB de gerenciamento para ambientes virtuais;

4.1.4.4. Permitir gerenciamento da console em nuvem com banco de dados também em nuvem;

4.1.4.5. O mecanismo de varredura deve estar disponível para download separadamente;

4.1.4.6. A solução deve permitir a inclusão de um modulo de balanceamento para casos em vários servidores tenham a mesma função (para alta disponibilidade, recuperação de desastres, performance entre outras);

4.1.4.7. Deve ser totalmente em português.

4.1.4.8. Arquitetura simples de atualização, com um simples clicar de botão todas as funções e serviços devem ser atualizadas;

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

4.1.4.10. As notificações devem ser destacadas como item não lido. Deve ter opção de enviar e-mail para o administrador com as notificações;

4.1.4.1.11. No mínimo enviar notificações:

4.1.4.1.11.1. Problemas com licenças;

4.1.4.1.11.2. Alertas de Surto de vírus;

4.1.4.1.11.3. Máquinas desatualizadas;

4.1.4.1.11.4. Eventos de antimalware;

4.1.5. Painel para Monitoramento

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

4.1.5.1.1. Nome;

4.1.5.1.2.Tipo de relatório;

4.1.5.1.3.Alvo do relatório;

4.1.5.1.4. Deve disponibilizar “portlets” para qualquer serviço de segurança, máquinas físicas, virtuais, dispositivos móveis;

4.1.6. Inventário da Rede

4.1.6.1. Possuir no mínimo as integrações abaixo:

4.1.6.1.1. Múltiplos domínios do Active Directory;

4.1.6.1.2. Múltiplos VMWare vCenters;

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

4.1.6.1.4. Deve ser compatível com Microsoft Hyper-V, Xen Server e KVM;

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

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

4.1.6.2.1. Nome;

4.1.6.2.2. Sistema Operacional;

4.1.6.2.3. Endereço IP;

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

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

4.1.6.5. Possuir tarefas remotas e configuráveis de Scan;

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

4.1.6.7. Assinar políticas para no mínimo os níveis:

4.1.6.7.1. Computador;

4.1.6.7.2. Máquina Virtual;

4.1.6.7.3. OU (Unidade Organizacional);

4.1.6.8. Possuir a propriedade detalhada de objetos gerenciados para:

4.1.6.8.1. Nome;

4.1.6.8.2. IP;

4.1.6.8.3. Sistema Operacional;

4.1.6.8.4. Grupo;

4.1.6.8.5. Política Assinada;

4.1.6.8.6. Ultimo status de malware;

4.1.7. Políticas

4.1.7.1. Modelo único para todos os equipamentos, seja físico ou virtual;

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

4.1.7.3. Deve 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, criptografia (Android), localização de dispositivo (Mobile), autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade;

4.1.8. Relatórios

4.1.8.1. Deve apresentar as seguintes funcionalidades:

4.1.8.1.1. Relatório para cada serviço de segurança;

4.1.8.1.2. Facilidade de usar e visualização simplificada;

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

4.1.8.1.4. Filtros de agendamento de relatórios;

4.1.8.1.5. Arquivo com todas as instâncias de relatório agendados;

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

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

4.1.9. Quarentena

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

4.1.9.1.Criação e exclusão para arquivos restaurados;

4.1.10. Usuários

4.1.10.1. Deve apresentar no mínimo as seguintes funcionalidades:

4.1.10.1.1. Administração baseada em regras;

4.1.10.1.2. Disponibilizar tipos de usuários pré-definidos como no mínimo:

4.1.10.1.2.1. Administrador – Gerente dos componentes da solução;

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

4.1.10.1.2.3. Relatório – Monitora e cria relatórios;

4.1.10.1.3. Deve ser possível customizar um tipo de usuário;

4.1.10.1.4. Deve permitir a integração do usuário com o Active Directory para autenticação da console de gerenciamento;

4.1.10. Logs

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

4.1.10.2. Detalhar cada ação do usuário;

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

4.1.11. Certificado de Segurança

4.1.11.1. Deve prover o acesso via HTTPS;

4.1.11.2. Deve permitir a importação de certificados digitais;

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

4.1.12. Proteção para Estações de Trabalho e Servidores Físicos

4.1.12.1. Deve permitir a configuração do scan do antivírus do cliente como:

4.1.12.1.1. Scan local;

4.1.12.1.2. Scan Hibrido;

4.1.12.1.3. Scan Central;

4.1.12.2. Deve permitir a instalação customizada do antivírus com no mínimo:

4.1.12.2.1. Instalar o antivírus sem o controle de acesso a internet; (Windows Workstation)

4.1.12.2.2. Instalar o antivírus sem o módulo de firewall; (Windows Workstation)

4.1.12.3. Deve suportar no mínimo os seguintes sistemas operacionais para estação de trabalho:

4.1.12.3.1. Windows 10 64Bits ou Superior;

4.1.12.4. Deve suportar no mínimo os seguintes sistemas operacionais para servidores:

4.1.12.4.1. Windows Server 2012R2 ou Superior;

4.1.12.4.2. Linux 2.6.36 ou superior;

4.1.13. Gerenciamento e Instalação Remota

4.1.13.1. Deve permitir ao administrador customizar a instalação;

4.1.13.2. A instalação deve ser possível executar com no mínimo das seguintes maneiras:

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

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

4.1.13.3. Deve ser possível ter um relatório com as estações instaladas e as faltantes da instalação;

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

4.1.13.4.1. Nome;

4.1.13.4.2. IP;

4.1.13.4.3. Sistema Operacional;

4.1.13.4.4. Política Aplicada;

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

4.1.13.6. A console de gerenciamento deve incluir sessão de log com as seguintes informações:

4.1.13.6.1. Login;

4.1.13.6.2. Edição;

4.1.13.6.3. Criação;

4.1.13.6.4. Log-out;

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

4.1.13.8. Deve permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;

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

4.1.14. Proteção de antivírus dedicado para Ambientes Virtuais

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

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

4.1.14.3. Deve proteger em tempo real e agendado as máquinas virtuais Linux;

4.1.14.4. O produto deve oferecer agente para virtualização de ao menos as seguintes soluções:

4.1.14.4.1. VMware vSphere;

4.1.14.4.2. Xen Server;

4.1.14.4.3. Microsoft Hyper-V;

4.1.14.4.4. KVM;

4.1.14.5. Funções Gerais:

4.1.14.5.1. Deve ter métodos de detecção de vírus, Spyware, rootkits e outros mecanismos de segurança;

4.1.14.5.2. Deve reportar o estado atual das VMs no mínimo, protegida/desprotegida;

4.1.14.6. Requisitos Mínimos do Sistema:

4.1.14.6.1. Plataformas de Virtualização

4.1.14.6.2. VMware vSphere;

4.1.14.6.3. Microsoft Hyper-V;

4.1.14.6.4. Xen Server;

4.1.14.6.5. KVM;

4.1.15. Sistemas Operacionais desktops, ou versões superiores:

4.1.15.1. Microsoft Windows 10

4.1.16. Sistemas Operacionais Servidores, ou versões superiores:

4.1.16.1. Microsoft Windows Server 2012 R2

4.1.16.2. Linux 2.6.36 ou superior;

4.1.17. Componentes e Funcionalidades do Antivírus Geral

4.1.17.1. Deve fazer scan em tempo real automático;

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

4.1.17.3. Escaneamento de comportamento heurístico;

4.1.17.4. Deve escanear em tempo real qualquer informação localizada em mídias de armazenamento como:

4.1.17.4.1. CD/DVD;

4.1.17.4.1. Discos Externos;

4.1.17.4.1. Pen-Drivers;

4.1.17.5. Deve permitir a escolha e configuração de pastas a ser escaneada;

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

4.1.17.6.1. Baseada em Assinaturas;

4.1.17.6.2. Baseada em Heurística;

4.1.17.6.3. Baseada em monitoramento contínuo de processos;

4.1.17.7. Deve ter a capacidade de escaneamento nos protocolos HTTP e SSL na Estações de trabalho;

4.1.17.8. O cliente do antivírus deve ter o módulo de Antiphishing;

4.1.17.9. Deve possuir módulo de firewall que de acordo com o administrador poderá ou não ser instalado/desinstalado nas estações de trabalho;

4.1.17.10. O módulo de firewall deverá ser possível configurar o modo invisível tanto a nível de rede local ou Internet nas estações de trabalho;

4.1.18. Quarentena

4.1.18.1. Deve permitir o envio automático de arquivos da quarentena para o laboratório de vírus;

4.1.18.2. Deve fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador;

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

4.1.18.4. Deve de forma automática criar exclusão para arquivos restaurados da quarentena;

4.1.18.5. Deve permitir escanear a quarentena após a atualização das atualizações de assinaturas;

4.1.19. Controle de Usuário

4.1.19.1. Deve ter módulo de controle de usuário integrando com as seguintes características:

4.1.19.2. Bloqueio de acesso a internet;

4.1.19.3. Bloqueio de acesso a aplicações definidas pelo administrador;

4.1.20. Controle de Dispositivo

4.1.20.1. Deve ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;

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

4.1.20.2.1. Bluetooth;

4.1.20.2.2. CDROM/DVDROM;

4.1.20.2.3. IEEE 1284.4;

4.1.20.2.4. IEEE 1394;

4.1.20.2.5. Windows Portable;

4.1.20.2.6. Adaptadores de Rede;

4.1.20.2.7. Adaptadores de rede Wireless;

4.1.20.2.8. Discos Externos;

4.1.20.3. Deve permitir regras de definição de bloqueio/desbloqueio;

4.1.20.4. Deve permitir regras de exclusão;

4.1.21. Atualização

4.1.21.1. Após a atualização o administrador deve ter a capacidade de adiar uma reinicialização;

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

4.1.21.3. Permitir atualizações de assinatura de hora em hora;

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

4.1.22. Proteção para Smartphones

4.1.22.1. Requisitos mínimos do Sistema Operacional para Smartphone:

4.1.22.1.1. Android 5 ou superior;

4.1.22.1.2. iOS 8 ou superior.

4.1.22.2. Recursos:

4.1.22.2.1. Permitir atribuir dispositivo com usuário do Active Directory;

4.1.22.2.2. A ativação do dispositivo da console de gerenciamento deve ser através de um QR code;

4.1.22.2.3. Os pacotes de instalação devem estar disponíveis nas lojas dos Sistemas Operacionais;

4.1.22.2.4. Deve permitir no mínimo as seguintes ações:

4.1.22.2.4.1. Impor bloqueio de tela e autenticação;

4.1.22.2.4.1. Desbloquear o dispositivo;

4.1.22.2.4.1. Restaurar as configurações de fábrica;

4.1.22.2.4.1. Localiza o Dispositivo;

4.1.22.2.5. Análise de dispositivos para o Sistema Operacional Android;

4.1.22.2.6. Criptografia de memória do dispositivo para o Sistema Operacional Android;

4.1.22.3. Configurações de Segurança

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

4.1.22.3.1.1. Ignorar;

4.1.22.3.1.2. Bloquear acesso;

4.1.22.3.1.3. Bloquear o dispositivo;

4.1.22.3.1.4. Restaurar as configurações de fábrica;

4.1.22.3.1.5. Remover o dispositivo do console de gerenciamento;

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

4.1.22.3.2.1. Senha simples ou complexa;

4.1.22.3.2.2. Números e caracteres;

4.1.22.3.2.3. Comprimento mínimo;

4.1.22.3.2.4. Caracteres especiais mínimos;

4.1.22.3.2.5. Período de expiração da senha;

4.1.22.3.2.6. Definir restrição de reutilização de senha;

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

4.1.22.3.2.8. Período de bloqueio do dispositivo;

4.1.23. Proteção para caixa de e-mail:

4.1.23.1. Fornecer proteção para ambiente Exchange;

4.1.23.2. Oferecer tecnologia para proteção contra spam;

4.1.23.3. Oferecer análise comportamental e proteção para zero-day;

4.1.23.4. Oferecer proteção contra vírus e tentativas de phishing;

4.1.24. Criptografia

4.1.24.1. Deve oferecer:

4.1.24.1.1. Possibilidade de criptografia de disco através da console de gerenciamento seja em nuvem ou on-premise;

4.1.24.1.2. Deve utilizar quando necessários serviços de criptografia SEM agentes nativos da estação de trabalho seja baseada em Windows (BitLocker) ou Mac (FileVault);

4.1.24.1.3. Deve solicitar autenticação quando iniciado o sistema operacional do equipamento;

4.1.24.1.4. Deve ser compatível com Mac OS X Moutain, Mavericks, Yosemite, Sierra.

4.2. **LOTE 2 - Item 2.1 - Fornecimento de Licenças de Solução de Segurança de Endpoint ("Antivírus")**

4.2.1. Vigência: **36 (trinta e seis) meses;**

4.2.2. Bitdefender, Kaspersky, McAfee, VIPRE ou equivalente técnico.

4.2.3. Requisitos Gerais:

4.2.3.1. Possuir uma única console de gerenciamento e configurações com funcionalidades para antivírus, antispyware, firewall, detecção\prevenção de intrusão ou defesa de ataque de rede, controle de dispositivos, sandbox e proteção específica contra malwares do tipo ransomware.

4.2.3.2. Ter a capacidade de remoção da atual solução instalada 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;

4.2.3.3. Deverá possuir no mínimo as seguintes funcionalidades e módulos:

4.2.3.3.1. Console de gerenciamento única, centralizada e funcionalidades de gestão e configurações de políticas e endpoints gerenciados;

4.2.3.3.2. Módulo para estações físicas e servidores;

4.2.3.3.3. Módulo para ambientes virtualizados e datacenters;

4.2.3.3.4. Módulo para dispositivos móveis;

4.2.3.3.5. Agente único para todos os módulos e recursos da solução a ser instalada nos endpoints;

4.2.3.3.6. Oferecer proteção por lista de vacinas (assinaturas);

4.2.3.3.7. Módulo específico para proteção de ataques de malwares tipo ransomware;

4.2.3.3.8. Prover técnicas avançadas e complementares de detecção como análise comportamental, análise heurística, inteligência artificial, anti-exploits, monitoramento de processos, machine learning, sandbox e painel de incidentes para tratamento e ações contra possíveis malwares.

4.2.3.4. A console de gerenciamento deverá ser entregue por meio de uma central única, baseada em web (protocolo HTTPS) ou MMC (Microsoft Management Console) e deverá conter todas a ferramentas para a monitoração e controle da proteção dos endpoints;

4.2.3.5. Deverá permitir instalação de console local (on-premise) com banco de dados local ou instalação em nuvem (cloud) com banco de dados em nuvem;

4.2.3.5.1. Para a opção de console local (on-premises), poderá ser fornecida como um appliance virtual ou executável para instalação em servidores Windows ou Linux, suportando no mínimo as seguintes plataformas de virtualização:

4.2.3.5.1.1. Microsoft Hyper-V;

4.2.3.5.1.2. VMWare vSphere;

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

4.2.3.5.1.4. Oracle VM;

4.2.3.5.1.5. Red hat Enterprise Virtualization;

4.2.3.5.1.6. Kernel-based Virtual Machine ou KVM.

4.2.3.5.2. Deverá ser fornecida com base de dados em sistema de gerenciamento de banco de dados externo SQL ou Oracle, ou embarcada na solução sem custos de licenciamento adicionais para a ativação;

4.2.3.6. Deverá proteger em tempo real e agendado os endpoints físicos ou virtuais em qualquer plataforma de sistema operacional, seja Windows, Linux ou Mac, em console local (on-premises) ou em console em nuvem (cloud);

4.2.3.7. Deverá suportar no mínimo os seguintes sistemas operacionais Windows para instalação dos agentes nos endpoints (estações e servidores):

4.2.3.7.1. Microsoft Windows Server 2019;

4.2.3.7.2. Microsoft Windows Server 2016;

4.2.3.7.3. Microsoft Windows Server 2012 R2;

4.2.3.7.4. Microsoft Windows 11;

4.2.3.7.5. Microsoft Windows 10;

4.2.3.8. Deverá suportar no mínimo os seguintes sistemas operacionais Linux para instalação dos agentes nos endpoints (estações e servidores):

4.2.3.8.1. Red Hat Enterprise Linux;

4.2.3.8.2. CentOS 5.6 ou superior;

4.2.3.8.3. Ubuntu 12.04 LTS ou superior;

4.2.3.8.4. SUSE Linux Enterprise Server 11 ou superior;

4.2.3.8.5. OpenSUSE 13 ou superior;

4.2.3.8.6. Fedora 20 ou superior;

4.2.3.8.7. Debian 8.0 ou superior.

4.2.3.9. Deverá suportar no mínimo os seguintes sistemas operacionais macOS para instalação dos agentes nos endpoints:

4.2.3.9.1. macOS Sierra (10.12) ou superior.

4.2.3.10. Deverá suportar no mínimo os seguintes sistemas operacionais para dispositivos móveis, tipo Tablets e Smartphones:

4.2.3.10.1. IOS 8.0 ou superior;

4.2.3.10.2. Android 4.03 ou superior.

4.2.3.11. Os pacotes de instalação para o agente dos dispositivos móveis devem estar disponíveis nas lojas dos respectivos sistemas operacionais;

4.2.3.12. Para proteção de dispositivos móveis deverá permitir no mínimo as seguintes ações:

4.2.3.12.1. Bloqueio de tela e autenticação;

4.2.3.12.2. Desbloqueio do dispositivo;

4.2.3.12.3. Restaurar as configurações de fábrica;

4.2.3.12.4. Localizar o dispositivo;

4.2.3.12.5. Criptografia de memória do dispositivo para o sistema operacional Android.

4.2.3.13. A solução deverá oferecer agente de proteção para os endpoints virtualizados, no mínimo para as seguintes plataformas de virtualização:

4.2.3.13.1. Microsoft Hyper-V;

4.2.3.13.2. VMware ESXi;

4.2.3.13.3. Citrix Xen Server;

4.2.3.13.4. Nutanix;

4.2.3.13.5. Red Hat Virtualization;

4.2.3.13.6. Oracle KVM;

4.2.3.13.7. KVM.

4.2.3.14. Para plataforma de virtualização VMWare, deverá:

4.2.3.14.1. Ser integrado e oferecer o escaneamento sem instalar o agente nos endpoints virtuais;

4.2.3.14.2. Possibilitar a integração com o VShield e com múltiplos vCenters.

4.2.3.15. Prover proteção de segurança para datacenters com suporte para Windows e Linux que atenda ambientes SDDC (Software Defined Data Center), hyperconvergência e nuvem híbrida, considerando ambientes híbridos e Multi-Cloud com console de gerenciamento e instalação centralizada e unificada, que atenda os servidores de virtualização e suas máquinas virtuais conectadas aos mesmos;

4.2.3.16. A console deverá apresentar dashboard com o resumo dos status de proteção dos endpoints, bem como indicar os alertas de eventos de criticidades alta, média e informacional;

4.2.3.17. Deverá permitir a importação de certificados digitais para comunicação segura entre console de gerenciamento e clientes gerenciados;

4.2.3.18. Deve possuir mecanismo de comunicação via API, para integração com outras soluções de segurança, como por exemplo SIEM;

4.2.3.19. Deve permitir sincronização com o Active Directory (AD) para gestão de usuários e grupos integrados às políticas de proteção;

4.2.3.20. Deve possuir a possibilidade de aplicar regras diferenciadas baseado em grupos ou usuários;

4.2.3.21. Deve a console ser capaz de criar e editar diferentes políticas para a aplicação das proteções exigidas e aplicadas a nível de usuários, não importando em que equipamentos eles estejam acessando;

4.2.3.22. 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);

4.2.3.23. Deve ser totalmente em português;

4.2.3.24. A console de gerenciamento deve incluir informações detalhadas sobre os endpoints com no mínimo as seguintes informações:

4.2.3.24.1. Nome (Netbios);

4.2.3.24.2. Sistema operacional;

4.2.3.24.3. Política e regras aplicada;

4.2.3.24.4. Endereço IP;

4.2.3.25. A console de gerenciamento deverá prover registro de logs com no mínimo as seguintes informações:

4.2.3.25.1. Login (usuário);

4.2.3.25.2. Alterações\Edições;

4.2.3.25.3. Criação;

4.2.3.25.4. Logout (usuário);

4.2.3.26. Deve permitir a escolha de quais pacotes e políticas serão atualizados;

4.2.3.27. Prover mecanismo de envio de notificações por e-mail no mínimo para osseguintes eventos:

4.2.3.27.1. Licenciamento da solução;

4.2.3.27.2. Surto e incidentes de malwares;

4.2.3.27.3. Endpoints desatualizados.

4.2.3.28. O gerenciamento deve ser baseado em “portlets” configuráveis para gerência e monitoramento de qualquer tipo de endpoint sejam máquinas físicas, virtuais e dispositivos móveis, com no mínimo as seguintes especificações:

4.2.3.28.1. Nome;

4.2.3.28.2. Tipo de relatórios;

4.2.3.28.3. Objetivo dos relatórios;

4.2.3.29. Permitir a descoberta de rede (Discovery) para endpoints em grupo de trabalho;

4.2.3.30. Para descoberta de rede (Discovery) e registro de inventário de objetos na console de gerenciamento, deve permitir no mínimo as seguintes integrações com plataformas de virtualização:

4.2.3.30.1. Múltiplos domínios do Active Directory;

4.2.3.30.2. Múltiplos VMWare vCenters;

4.2.3.30.3. Múltiplos Citrix Xen Servers.

4.2.3.31. Permitir a possibilidade de definição de sincronização de tempo com o Active Directory;

4.2.3.32. Possuir mecanismo de busca (Search) de endpoints no mínimo para os seguintes filtros:

4.2.3.32.1. Nome;

4.2.3.32.2. Sistema operacional;

4.2.3.33. Possibilitar a instalação e desinstalação remota do agente de antivírus nos endpoints;

4.2.3.34. Permitir a configuração de pacotes de instalação da solução de antivírus nos endpoints;

4.2.3.35. Permitir a instalação do agente nos endpoints no mínimo das seguintes formas:

4.2.3.35.1. Executar o pacote de antivírus diretamente nos endpoints;

4.2.3.35.2. Instalar remotamente, distribuído pela console de gerenciamento.

4.2.3.36. Ter a capacidade de criar um único pacote de instalação independente se o sistema operacional for para 32 Bits ou 64 Bits;

4.2.3.37. Deve possuir mecanismo contra a desinstalação do agente do endpoint pelo usuário e cada endpoint deverá ter uma senha única, não sendo autorizadas soluções com senha única válida para todos os endpoints;

4.2.3.38. Deverá permitir a criação de grupos e subgrupos para mover os endpoints;

4.2.3.39. O agente utilizado deve ser único para todas as funcionalidades e módulos de proteção da solução, sem a necessidade de instalação de novos softwares e agentes complementares no endpoint.

4.2.3.40. Permitir configurar tarefas remotas de varredura (scan) nos endpoints;

4.2.3.41. Permitir a reinicialização remota dos endpoints;

4.2.3.42. Deve ser possível atribuir políticas para no mínimo os seguintes níveis:

4.2.3.42.1. Endpoint físico;

4.2.3.42.2. Endpoint virtual;

4.2.3.42.3. Usuários do Active Directory;

4.2.3.42.4. Grupos do Active Directory;

4.2.3.42.5. Grupo de endpoints.

4.2.3.43. Permitir a visualização no mínimo das seguintes propriedades de objetos (endpoints) gerenciados:

4.2.3.43.1. Nome (Netbios);

4.2.3.43.2. Sistema operacional;

4.2.3.43.3. Endereço IP;

4.2.3.43.4. Grupo;

4.2.3.43.5. Política atribuída;

4.2.3.43.6. Status de infecção de malwares.

4.2.3.44. Deve possuir um modelo\forma único(a)de políticas a ser aplicado(a) para todos os endpoints gerenciados, sejam físicos ou virtuais;

4.2.3.45. Deve ser possível o envio de uma política única os agentes de antivírus instalados nos endpoints, com as configurações, funcionalidades e módulos pré-definidos;

4.2.3.46. Permitir a configuração de funcionalidades como proteção de malware, escaneamento (scan), controle de acesso a rede, controle de dispositivos, proteção contra ransomwares, proteção de rede, proteção contra exploração de vulnerabilidades, controle de acesso web, autenticação e ações para serem aplicadas em caso de endpoints em não conformidade;

4.2.3.47. Para emissão de relatórios, deverá prover no mínimo as seguintes funcionalidades:

4.2.3.47.1. Os recursos devem ser nativos da própria console de gerenciamento;

4.2.3.47.2. Facilidade de operação e visualização simplificada;

4.2.3.47.3. Relatório para cada tipo de proteção disponível na solução;

4.2.3.47.4. Envio agendado por e-mail para qualquer destinatário;

4.2.3.47.5. Configurar filtros de agendamento para envio dos relatórios;

4.2.3.47.6. Registro com todas as instâncias de relatório gerados;

4.2.3.47.7. Exportar o relatório nos formatos .PDF e/ou .CSV;

4.2.3.47.8. Possibilidade de criar relatórios dinâmicos;

4.2.3.47.9. Emissão de relatório com os endpoints instalados e não instalados;

4.2.3.48. Para os usuários de administração da console de gerenciamento, deverá prover no mínimo as seguintes funcionalidades:

4.2.3.48.1. Administração baseada em regras;

4.2.3.48.2. Disponibilizar tipos de usuários pré-definidos como no mínimo:

4.2.3.48.2.1. Administrador – Gerência completa da solução;

4.2.3.48.2.2. Operador–Gerência dos serviços\módulos da solução.

4.2.3.48.2.3. Monitor – Monitora e cria relatórios;

4.2.3.49. Deverá ser possível customizar um tipo de usuário para administração;

4.2.3.50. Deverá permitir a integração de usuários com o Active Directory para autenticação;

4.2.3.51. Registrar (log) de forma detalhada as ações dos usuários;

4.2.3.52. Permitir pesquisas (Search) das ações executadas pelos usuários com opção de filtro por intervalo de tempo;

4.2.3.53. Deverá ter métodos de detecção de vírus, spyware, rootkits e outros mecanismos de segurança para os diversos tipos de malware;

4.2.3.54. Permitir atualizações de assinaturas de hora em hora;

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

4.2.3.55.1. Scan local;

4.2.3.55.2. Scan local/remoto;

4.2.3.55.3. Scan remoto.

4.2.3.56. Deverá reportar o estado atual dos endpoints virtuais no mínimo, protegido/desprotegido;

4.2.3.57. Deverá fazer escaneamento em tempo real e automático;

4.2.3.58. Deverá ser possível configurar filtros para não escanear arquivos por tamanho ou por tipo de extensão;

4.2.3.59. Deverá possuir escaneamento baseado em análise heurística;

4.2.3.60. Deverá permitir a escolha e configuração de pastas a serem escaneadas;

4.2.3.61. Deverá prover no mínimo os seguintes tipos de detecção:

4.2.3.61.1. Baseada em assinaturas;

4.2.3.61.2. Baseada em análise comportamental;

4.2.3.61.3. Baseada em heurística;

4.2.3.61.4. Baseada em monitoramento contínuo de processos;

4.2.3.62. Deverá permitir a execução de escaneamento remoto nos endpoints (disponível para sistemas Windows e Linux) de forma simples e não requerer reinicialização dos endpoints virtuais;

4.2.3.63. Deve ser possível incorporar o escaneamento remoto em modelos e imagens VDI (Virtual Desktop) para minimizar a sobrecarga de gerenciamento;

4.2.3.64. Deverá estabelecer conexão com um servidor de segurança autorizado, permitindo acesso local ao sistema de arquivos, registro, memória e processos, realizando dessa forma o escaneamento de ameaças de forma remota, analisando somente os metadados dos endpoints;

4.2.3.65. Deverá prover alternativa de conexão para outros servidores de segurança disponíveis em caso de tempo de resposta lento ou indisponibilidade súbita, permitindo um balanceamento de carga para otimizar performance e prover alta disponibilidade;

4.2.3.66. Deve permitir utilizar o motor de varredura local, no servidor de segurança ou em nuvem afim de aumentar o desempenho do endpoint quando o mesmo estiver com o processo de escaneamento em execução.

4.2.3.67. Permitir gerenciar localmente no endpoint, a desinfecção, a quarentena e o bloqueio de processos;

4.2.3.68. Deverá manter no endpoint gerenciado, cache local de itens analisados para ganhos de desempenho.

4.2.3.69. Para a funcionalidade de quarentena, deverá:

4.2.3.69.1. Permitir restauração remota, com configuração de localidade e deleção;

4.2.3.69.2. Ser possível a criação e exclusão de arquivos restaurados;

4.2.3.69.3. Permitir o envio automático de arquivos para o laboratório de vírus do fabricante;

4.2.3.69.4. Fazer a remoção automática de arquivos antigos e pré-definidos nas configurações;

4.2.3.69.5. Permitir mover o arquivo para seu local de origem ou outro destino desejável;

4.2.3.69.6. Criar de forma automática a exclusão para arquivos restaurados da quarentena;

4.2.3.69.7. Permitir escanear a quarentena após a atualização de assinaturas.

4.2.3.70. Deve possuir um módulo de controle de dispositivos com as seguintes funcionalidades:

4.2.3.70.1. Ser possível a ativação do módulo de controle de dispositivos no agente instalados nos endpoints pela console de gerenciamento;

4.2.3.70.2. Ser possível controlar no mínimo os seguintes dispositivos:

4.2.3.70.2.1. CDROM/DVDROM;

4.2.3.70.2.2. Padrão IEEE 1284.4;

4.2.3.70.2.3. Padrão IEEE 1394;

4.2.3.70.2.4. Windows Portable;

4.2.3.70.2.5. Bluetooth;

4.2.3.70.2.6. Discos Externos;

4.2.3.70.2.7. Adaptadores de Rede;

4.2.3.70.2.8. Adaptadores de rede Wireless.

4.2.3.70.3. Possibilidade de escanear qualquer informação localizada em mídias de armazenamento como:

4.2.3.70.3.1. CD/DVD;

4.2.3.70.3.2. Discos Externos;

4.2.3.70.3.3. Pen-Drivers.

4.2.3.70.4. Permitir regras de definição de bloqueio/desbloqueio e exclusão.

4.2.3.71. Deve possuir módulos de proteção de rede (tipo HIPS) e contra exploração de vulnerabilidades com as seguintes funcionalidades:

4.2.3.71.1. Proteção contra exploração do tipo buffer overflow ou mitigação deste tipo de ataque;

4.2.3.71.2. Atualização periódica de novas assinaturas;

4.2.3.71.3. Possuir no mínimo as seguintes técnicas de proteção e prevenção:

4.2.3.71.3.1. Algoritmo de correspondências com padrões - onde os dados de entrada são comparados com um conjunto de sequências conhecidas de código já identificado como um vírus;

4.2.3.71.3.2. Emulação - uma técnica para a detecção de vírus polimórficos, ou seja, vírus que se escondem criptografando-se de maneira diferente cada vez que se espalham;

4.2.3.71.3.3. Redução de ameaças - detecção de prováveis ameaças por uma variedade de critérios, como extensões duplas (por exemplo. jpg.txt) ou a extensão não coincida com o tipo de arquivo verdadeiro (por exemplo, um arquivo executável ou arquivo .exe com a extensão .txt);

4.2.3.71.3.4. Prevenção contra carregamento de bibliotecas de memória em um processo de host. (Reflective DLL Injection);

4.2.3.71.3.5. Proteção contra cargas na memória utilizando técnicas tais como Meterpreter e Mimikatz e ferramentas como Metasploit;

4.2.3.71.3.6. Verificação de ameaças web avançadas bloqueando e verificando o conteúdo em tempo real e remontando com emulação de Java Script e análise comportamental para identificar e parar o código malicioso de malwares avançados.

4.2.3.71.4. A solução deverá ter tecnologia específica para proteção contra ataques avançados que explorem vulnerabilidades conhecidas e desconhecidas (ataques dia zero – zero day) nos endpoints e contemplar no mínimo as seguintes especificações:

4.2.3.71.4.1. Possuir técnica de machine learning para auxiliar na detecção de tentativas de exploração das vulnerabilidades, principalmente vulnerabilidades desconhecidas (zero-day), entregando as seguintes características complementares:

4.2.3.71.4.1.1. Deve ser local (instalada no agente) e ajustável, onde deverá ser possível definir o nível de sensibilidade do mesmo para determinados tipos de ameaças emergentes, tais como Ataques Dirigidos, Ransomware, Exploits, etc.;

4.2.3.71.4.1.2. Deve ser nativa da própria solução, não sendo necessário a instalação de softwares de terceiros para sua utilização;

4.2.3.71.4.1.3. Deve ter capacidade de detectar ameaças no estágio de pré-execução do processo nos endpoints.

4.2.3.71.4.2. Proteger contra explorações invasivas, sequestro de processos e monitorar os processos de sistemas operacionais;

4.2.3.71.4.3. Possuir mecanismo para proteção de ataques sem arquivo (file-less);

4.2.3.71.4.4. Proteger aplicativos comumente utilizados, tais como aplicativos da suíte Microsoft Office, leitores de PDF como Adobe Reader, Flash Player e navegadores (browsers) de internet;

4.2.3.71.4.5. Caso o aplicativo desejado não esteja listado na solução para proteção contra exploração de vulnerabilidades, deverá ser possível adicionar aplicações diversas incluindo os seus processos para bloqueio de tentativas de exploração de vulnerabilidades conhecidas e desconhecidas;

4.2.3.71.4.6. Ser possível definir ações contra tentativas de exploração, no mínimo reportar e matar/bloquear o processo explorado;

4.2.3.71.4.7. Prover proteção contra qualquer nova ameaça emergente ou exploits desconhecidos;

4.2.3.71.4.8. Possuir mecanismo de detecção contra as seguintes técnicas de exploits:

4.2.3.71.4.8.1. Tentativas de criação de shell reverso, utilizando Meterpreter;

4.2.3.71.4.8.2. Explorações do VBScript;

4.2.3.71.4.8.3. Injeção de código malicioso em threads recém-criadas;

4.2.3.71.4.8.4. Escalação de privilégio em sistemas operacionais baseados em Windows;

4.2.3.71.4.8.5. Vazamento de hashes de senha e configurações de segurança de sistemas operacionais (processo LSASS).

4.2.3.72. Deve possuir um módulo de proteção contra malwares do tipo ransomware com as seguintes funcionalidades:

4.2.3.72.1. Deve dispor de tecnologia para proteção contra malware do tipo ransomware não baseada exclusivamente na detecção por assinaturas;

4.2.3.72.2. Deve bloquear a criptografia de arquivos em recursos compartilhados a partir de um processo malicioso, inclusive, que esteja sendo executado remotamente a partir de outro endpoint;

4.2.3.72.3. Deve monitorar pastas compartilhadas, rastreando o estado dos arquivos armazenados e os protegendo;

4.2.3.72.4. Na detecção de atividade maliciosa de criptografia por malware do tipo ransomware, a solução deve interromper o processo de criptografia e restaurar os arquivos ao seu estado original, impedindo a perda de dados corporativos.

4.2.3.73. Deve possuir o módulo ou recurso de painel de incidentes ou similar com as seguintes funcionalidades mínimas:

4.2.3.73.1. Prover visibilidade sobre as detecções dos módulos de prevenção da solução, tal como árvores de processos e time-line dos eventos (processos, registros de sistema, conexões de rede, arquivos, etc.) que geraram a detecção. Não serão aceitas soluções que exibem apenas informações básicas de uma detecção de malware;

4.2.3.73.2. Cada detecção de ameaça deverá ser registrada como um incidente a ser analisado pelo administrador da solução, podendo alterar o status deste incidente entre as seguintes opções: aberto/pendente, investigando/sob análise, falso positivo, fechado/resolvido ou status similares e que entreguem o mesmo fluxo de controle no tratamento do incidente;

4.2.3.73.3. Deverá exibir o "caminho crítico" que gerou a detecção da ameaça, facilitando dessa forma a visão do administrador da solução quanto a investigação do incidente gerado pelos módulos de NGAV;

4.2.3.73.4. Deve exibir um mapa, árvore de processos, diagrama ou qualquer método intuitivo através de imagens que facilite a compreensão da detecção, tal como os artefatos (processos, registros, domínios, etc) que desencadearam a detecção da ameaça pelos módulos de NGAV;

4.2.3.73.5. Deverá exibir o processo de remediação que foi realizado durante a detecção, tal como bloqueio de processo, quarentena, bloqueio de IP, etc.;

4.2.3.73.6. Deverá exibir detalhes de processos detectados como maliciosos, com no mínimo as informações de PID do processo, hash (SHA256 ou MD5), número de certificado do processo, caminho do processo no endpoint, tamanho do arquivo, usuário que executou, time stamp da execução;

4.2.3.73.7. Deverá ser possível a adição de processos detectados em blacklist e whitelist;

4.2.3.73.8. Deve prover recursos para resposta às detecções geradas no ambiente, tal como acesso remoto aos endpoints (via shell/linha de comando) para execução de procedimentos de resposta, assim como o isolamento dos endpoints da rede, permitindo apenas sua comunicação com a console de gerenciamento da solução, seja local ou em nuvem.

4.2.3.74. Deve possuir o módulo ou recurso de sandbox seguintes funcionalidades mínimas:

4.2.3.74.1. Prover análise adicional em artefatos como scripts, executáveis e documentos. Deve ser possível ajustar o nível de sensibilidade para análise e pré-filtragem de cada tipo de arquivo, além de permitir a criação de lista de exclusões para extensões que não devem ser analisadas pelo Sandbox;

4.2.3.74.2. Deve ser nativo da própria ferramenta, não sendo necessário a instalação de softwares de terceiros para sua utilização;

4.2.3.74.3. Deve ter capacidade de detectar ameaças no estágio de pré-execução do processo nos endpoints;

4.2.3.74.4. O ambiente de detonação (sandbox) deverá estar localizado na nuvem do fabricante, permitindo o envio manual e automático de artefatos de qualquer local, via internet, independentemente da localização física dos endpoints;

4.2.3.74.5. Deve permitir a configuração de proxy, caso o endpoint necessite para envio das amostras ao sandbox;

4.2.3.74.6. Deve ser possível definir as ações a serem tomadas pelo sandbox no caso de detecção de um artefato malicioso, sendo: desinfectar o objeto; deletar o objeto; mover para quarentena; somente reportar;

4.2.3.74.7. Deve ser possível definir os tipos de arquivos que poderão ser submetidos ao sandbox, tais como aplicativos, documentos, scripts, e-mails, dentre outros;

4.2.3.74.8. Após a análise e detonação do artefato no sandbox, um relatório forense deverá ser exibido na console, com todos os detalhes sobre a execução dos arquivos no ambiente de detonação, além de especificar se o mesmo é ou não um artefato malicioso;

4.2.3.74.9. Todas as submissões ao ambiente do sandbox devem ser registradas na console de administração da solução, independente do arquivo ter sido submetido manual ou automaticamente, informando o status da análise do artefato, tal como seu resultado (limpo ou infectado/malicioso).

4.3. **LOTE 2 - Item 2.2 - Serviço de Instalação e Configuração de Software**

4.3.1. A instalação e configuração dos produtos deverá ser realizada em dias úteis de segunda-feira a sexta-feira de 09h00 às 17h00.

4.3.2. 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 da CONTRATANTE.

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

4.3.4. A CONTRATADA, a suas custas, deverá realizar a remoção da solução de antivírus instalada no *endpoint* no momento da instalação da solução ofertada.

4.3.4.1. Havendo necessidade técnica de realizar a remoção de forma presencial, A CONTRATADA deverá arcar com todos os custos de deslocamento de seus técnicos, não cabendo nenhum custo adicional à CONTRATANTE.

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

4.4. **LOTE 2 - Item 2.3 - Serviço de Capacitação**

4.4.1. A capacitação deverá ser fornecida para uma turma de no mínimo 08 (oito) servidores da área de tecnologia da CONTRATANTE;

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

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

4.4.4. Deverá ser realizada presencialmente, em infraestrutura disponibilizada pela CONTRATADA e deverá possuir carga horária mínima de 16 (dezesseis) horas;

4.4.5. Deverá ser realizado no prazo máximo até 30 (trinta) dias corridos, após a emissão da ordem de fornecimento;

4.4.6. Após a realização da capacitação, a CONTRATADA deverá fornecer certificado de conclusão para cada participante.

5. GARANTIA, ASSISTÊNCIA TÉCNICA E SUPORTE

5.1. Todas as licenças deverão ser emitidas pelo Fabricante, com respectivos pacotes de atualização e garantia por 12 (doze) meses para a Aquisição do LOTE 1 e 36 (trinta e seis) meses para a Aquisição do LOTE 2;

5.2. A Central de Atendimento da CONTRATADA deverá ser acionada por meio de ligação telefônica, por e-mail ou preferencialmente por sistema de service desk disponível na Internet, para abertura de chamados;

5.3. Os serviços de abertura de chamados deverão estar disponíveis em regime 24x7;

5.4. A CONTRATADA deverá fornecer atualizações automáticas das versões de software, e manter a homogeneidade da última versão em toda a solução fornecida;

5.5. Toda intervenção na solução adquirida deverá ser comunicada e negociada previamente, para que sejam definidas a data e hora da sua realização;

5.6. A CONTRATANTE permitirá o acesso dos técnicos credenciados pela CONTRATADA às instalações onde se encontrarem os equipamentos para a prestação dos serviços de manutenção. Entretanto, tais técnicos ficarão sujeitos às normas internas de segurança da CONTRATANTE, notadamente àquelas atinentes à identificação, trânsito e permanência nas suas dependências;

5.7. Caso seja necessária a permanência do técnico da CONTRATADA nas instalações da CONTRATANTE além do tempo previsto para resolução do problema, tal fato não deverá representar qualquer ônus adicional à última.

5.8. A CONTRATADA deverá disponibilizar à CONTRATANTE um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução adquirida, inclusive de firmware, sem ônus para a CONTRATANTE.

5.9. **Níveis de Serviço Esperados (LOTES 1 e 2)**

5.9.1. Atendimento telefônico por número 0800, ou equivalente ao custo de ligação local, como serviço de uso ilimitado;

5.9.2. No local (on-site) – serviço de uso ilimitado, prestado em caso de emergência ou que ocasionem interrupção na execução do serviço prestado pela Contratada, e também compreendendo os seguintes tipos de atendimento local: suporte para upgrade de versões e releases do software; solução de problemas detectados (troubleshoot); análise e correção de eventos relacionados à segurança e à performance do software e do ambiente; atualização simultânea nos ambientes dos órgãos e entidades da CONTRATANTE.

5.9.3. Para efeito dos atendimentos técnicos, a CONTRATADA deverá observar os níveis de severidade e respectivos prazos máximos fixados abaixo:

Nível	DESCRIÇÃO
1	Serviços totalmente indisponíveis
2	Serviços parcialmente indisponíveis ou com degradação de tempo de resposta
3	Serviços disponíveis com ocorrência de alarmes de aviso, consultas sobre problemas, dúvidas gerais sobre o equipamento fornecido

PRAZOS DE ATENDIMENTO				
Modalidade	Prazos	Níveis de Severidade		
		1	2	3
Telefone, e-mail, web e remoto	Início atendimento	1 hora	2 horas	24 horas

	Término atendimento	8 horas	16 horas	72 horas
On-site	Início atendimento	-	-	24 horas
	Término atendimento	-	-	72 horas

5.9.4. Para casos de severidade de nível 1, caso o atendimento não seja finalizado até as 20h00min, o técnico não poderá interrompê-lo, devendo continuá-lo até sua finalização, exceto quando explicitamente autorizado pela CONTRATANTE, que determinará o momento posterior para continuação do atendimento;

5.9.5. Todo o chamado somente será caracterizado como "encerrado" mediante concordância da CONTRATANTE;

5.9.6. Para as situações em que a solução definitiva de problemas no ambiente demande reimplantação, reestruturação ou reinstalação do produto, esta deverá ser programada e planejada com a antecedência necessária, de modo a não prejudicar a operação dos demais sistemas da CONTRATANTE;

5.9.7. Em caso de inexecução total ou parcial, ou qualquer outra inadimplência, sem motivo de força maior, a empresa contratada estará sujeita, sem prejuízo da responsabilidade civil e criminal, no que couber, garantida a prévia defesa, às penalidades previstas na legislação aplicável, para as seguintes hipóteses:

a) por atraso injustificado;

b) por inexecução total e parcial dos Serviços.

6. CONDIÇÕES DE FORNECIMENTO E RECEBIMENTO

6.1. Os softwares que tratam os itens 1.1 e 2.1 do objeto devem ser fornecidos em até 10 (dez) dias úteis após o recebimento da ordem de fornecimento pela CONTRATADA.

6.2. O serviço de instalação que trata o item 2.2. do objeto deve iniciar-se em até 10 (dez) dias úteis após o recebimento da ordem de fornecimento pela CONTRATADA, devendo ser concluído em até 15 (quinze) dias úteis após o início da execução.

6.2.1. A licitante deverá entregar declaração de capacidade técnica profissional junto com a Proposta de Preços, datada e assinada por seu representante legal de que, no momento da assinatura do Contrato, disporá de profissional(is) com comprovação de experiência para os serviços de suporte técnico e configuração nas soluções ofertadas.

6.3. O serviço de capacitação que trata o item 2.3. do objeto deve ser realizado no prazo máximo até 30 (trinta) dias corridos após a emissão da ordem de fornecimento;

6.4. Os softwares serão recebidos provisoriamente pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes neste Termo de Referência e na proposta, devendo ser elaborado relatório circunstanciado, contendo o registro, a análise e a conclusão acerca das ocorrências na execução do contrato e demais documentos que julgarem necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

6.5. A emissão da Nota Fiscal/Fatura deve ser precedida do recebimento definitivo dos serviços, nos termos abaixo.

6.6. No prazo de até 5 dias corridos do adimplemento da parcela, a CONTRATADA deverá entregar toda a documentação comprobatória do cumprimento da obrigação contratual;

6.7. O recebimento provisório será realizado pelo gestor do contrato, ou pela equipe de fiscalização após a entrega da documentação acima, da seguinte forma:

6.7.1. A CONTRATANTE realizará inspeção minuciosa de todos os serviços executados ou produtos fornecidos, por meio de profissionais técnicos competentes, acompanhados dos profissionais encarregados pelo serviço, com a finalidade de verificar a conformidade dos bens e/ou serviços, bem como, constatar e relacionar eventuais arremates, retoques e revisões finais que se fizerem necessários.

6.7.1.1. Para efeito de recebimento provisório, ao final de cada período de faturamento, o fiscal técnico do contrato irá apurar o resultado das avaliações da execução do objeto e, se for o caso, a análise do desempenho e qualidade da prestação dos serviços realizados em consonância com os indicadores previstos, que poderá resultar no redimensionamento de valores a serem pagos à contratada, registrando em relatório a ser encaminhado ao gestor do contrato.

6.7.1.2. A CONTRATADA fica obrigada a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou

materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

6.7.1.3. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis.

6.7.2. No prazo de até 10 dias corridos a partir do recebimento dos documentos da CONTRATADA, cada fiscal ou equipe de fiscalização deverá elaborar Relatório Circunstanciado em consonância com suas atribuições, que será conjuntamente validado pelo gestor do Contrato.

6.7.2.1. Quando a fiscalização for exercida por um único servidor, o relatório circunstanciado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo.

6.7.2.2. Será considerado como ocorrido o recebimento provisório com a entrega do relatório circunstanciado ou, em havendo mais de um a ser feito, com a entrega do último.

6.7.2.3. Na hipótese de a verificação a que se refere o parágrafo anterior não ser procedida tempestivamente, reputar-se-á como realizada, consumando-se o recebimento provisório no dia do esgotamento do prazo.

6.8. No prazo de até 10 (dez) dias corridos a partir do recebimento provisório dos serviços, o Gestor do Contrato deverá providenciar o recebimento definitivo, ato que concretiza o ateste da execução dos serviços, obedecendo as seguintes diretrizes:

6.8.1. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à CONTRATADA, por escrito, as respectivas correções;

6.8.2. Emitir Termo Circunstanciado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas; e

6.8.3. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização.

6.9. O recebimento provisório ou definitivo do objeto não exclui a responsabilidade da Contratada pelos prejuízos resultantes da incorreta execução do contrato, ou, em qualquer época, das garantias concedidas e das responsabilidades assumidas em contrato e por força das disposições legais em vigor (Lei n° 10.406, de 2002).

6.10. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, devendo ser corrigidos/refeitos/substituídos no prazo fixado pelo fiscal do contrato, às custas da Contratada, sem prejuízo da aplicação de penalidades.

6.11. Não será admitida a subcontratação do objeto.

7. PAGAMENTO

7.1. O pagamento será realizado após ao completo fornecimento do item solicitado.

7.2. A CONTRATADA deverá apresentar a Nota Fiscal correspondente ao fornecimento realizado na unidade administrativa responsável pelo acompanhamento e gestão do contrato para ateste;

7.3. O pagamento será efetuado em até 30 dias, após o recebimento definitivo dos serviços realizado pelo gestor do contrato.

7.4. Na ocorrência de rejeição da(s) Nota(s) Fiscal(is), motivada por erro ou incorreções, o prazo para pagamento estipulado acima passará a ser contado a partir da data da sua reapresentação.

8. OBRIGAÇÕES DA CONTRATADA:

8.1. Responsabilizar-se integralmente pelo fiel cumprimento do contrato.

8.2. Prestar todos os esclarecimentos solicitados pela CONTRATANTE a cujas reclamações e pedidos se obriga a atender.

8.3. Fornecer os softwares e executar os serviços de acordo com as especificações presentes neste Termo de Referência.

8.4. Executar os serviços por intermédio de profissionais devidamente especializados e qualificados.

8.5. Atender aos chamados da CONTRATANTE quando solicitada e solucionar as pendências, às suas expensas.

8.6. Comunicar à CONTRATANTE qualquer anormalidade de caráter urgente e prestar os esclarecimentos que julgar necessário.

8.7. Manter-se, durante toda a execução dos serviços, em compatibilidade com as obrigações a serem assumidas, todas as condições de habilitação e qualificação exigidas neste termo de referência e no edital.

8.8. Arcar com todas as despesas, diretas ou indiretas, decorrentes do cumprimento das obrigações assumidas, sem nenhum ônus para a CONTRATANTE;

8.9. Designar um representante responsável pelo gerenciamento dos serviços e com poderes para tratar de assuntos junto ao CONTRATANTE;

8.10. Responder por quaisquer danos que venham a ser causados por seus empregados ou prepostos, a terceiros ou ao próprio CONTRATANTE, ou pela omissão deles no desempenho de suas tarefas, desde que fique realmente comprovada a responsabilidade.

8.11. Arcar com todas as despesas de locomoção dos profissionais envolvidos na prestação dos trabalhos, inclusive quanto às despesas de diárias, passagens, hospedagem, estada, alimentação e qualquer outro tipo de custo, para a realização de reuniões e/ou para os serviços cuja prestação deva ser realizada nas dependências da CONTRATANTE.

9. OBRIGAÇÕES DA CONTRATANTE:

9.1. Proporcionar todas as facilidades à boa execução dos serviços objeto deste termo de referência.

9.2. Comunicar à CONTRATADA as possíveis irregularidades detectadas na execução dos serviços.

9.3. Designar servidor para acompanhar e fiscalizar os fornecimentos de equipamentos e as prestações de serviços, bem como para dirimir quaisquer dúvidas advindas da entrega e qualidade do serviço prestado.

9.4. Prestar as informações e os esclarecimentos necessários ao bom desempenho das atividades.

9.5. Atestar o recebimento do objeto contratado e a execução dos serviços, após verificação das especificações, rejeitando o que não estiver de acordo por meio de notificação à CONTRATADA.

9.6. Efetuar o pagamento à CONTRATADA na forma e nos prazos previstos neste termo de referência, após o cumprimento das formalidades legais.

9.7. Exigir, a qualquer tempo, comprovação das condições da CONTRATADA que ensejaram a contratação.

10. CONFIDENCIALIDADE E SIGILO DAS INFORMAÇÕES

10.1. Na execução dos serviços descritos neste Termo de Referência, a CONTRATADA poderá ter acesso a informações restritas da DPE-GO. Assim, caberá a CONTRATADA:

10.1.1. Zelar pelo sigilo inerente à execução do objeto e pela confidencialidade quanto aos dados e informações da DPE-GO que eventualmente tenha acesso, empregando todos os meios necessários para tanto;

10.1.2. Responsabilizar-se pela divulgação não autorizada ou pelo uso indevido de qualquer informação pertinente a DPE-GO;

10.2. Em caso de não cumprimento das condições de confidencialidade e sigilo estabelecidas, a CONTRATADA responderá de forma incondicional, civil, criminal e administrativamente pelo fato, sem prejuízo do direito da DPE-GO de promover a rescisão contratual, com a aplicação das penalidades cabíveis.

11. HABILITAÇÃO TÉCNICA

11.1. COMPROVAÇÃO DE CAPACIDADE PARA O FORNECIMENTO

11.1.1. A licitante confirmará a habilitação técnica, nos termos do Art. 30, § 1º, da Lei 8.666/93, pela entrega de atestado(s) ou declaração(ções) de desempenho anterior em serviços da mesma natureza do objeto a ser contratado, em nome da licitante, a ser(em) fornecido(s) por pessoa jurídica de direito público ou privado, que comprovem a execução e o bom desempenho na prestação de serviços.

11.1.2. Para fins de entendimento da natureza do objeto, deve-se considerar atestado(s) contemplando o fornecimento e implantação satisfatórios de:

11.1.2.1. Ao menos 282 (duzentas e oitenta e duas) licenças de uso do software de segurança de endpoint ("Antivírus"), contemplando AntiSpyware, controle de dispositivos de forma centralizada por console de

gerenciamento local e/ou em nuvem, com garantia de atualização e serviço de suporte técnico, sendo esta métrica equivalente a 50% da quantidade de licenças previstas no item 1.1 do objeto.

11.2. COMPROVAÇÃO DE CAPACIDADE TÉCNICA DO(S) PROFISSIONAL(IS) DA(S) CONTRATADA(S)

11.2.1. A licitante deverá entregar declaração de capacidade técnica profissional junto com a Proposta de Preços, datada e assinada por seu representante legal, declarando que no momento da assinatura do Contrato disporá de profissional(is) com comprovação de experiência na instalação e configuração das soluções ofertadas.

11.2.1.1. Tal comprovação se faz necessária para garantir a segurança técnica e operacional na instalação das soluções ofertadas.

11.3. REQUISITOS DOS ATESTADOS DE DESEMPENHO ANTERIOR EM SERVIÇOS DA MESMA NATUREZA DO OBJETO A SER CONTRATADO

11.3.1. Para fins de comprovação os Atestados de Capacidade Técnica deverão ser emitidos em papel timbrado e conter obrigatoriamente:

11.3.1.1. Razão Social, CNPJ e endereço completo da empresa/órgão emitente;

11.3.1.2. Razão Social da contratada;

11.3.1.3. Número e vigência do contrato;

11.3.1.4. Objeto do contrato;

11.3.1.5. Descrição dos serviços realizados;

11.3.1.6. Declaração de que foram atendidas as expectativas do cliente quanto ao cumprimento dos cronogramas pactuados;

11.3.1.7. Local e data de emissão;

11.3.1.8. Identificação do responsável pela emissão do atestado, com nome, cargo e dados para contato (telefone e correio eletrônico);

11.3.1.9. Assinatura do responsável pela emissão do atestado.

11.3.2. No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial do licitante, isto é, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente do atestado e da empresa proponente.

11.3.3. Conforme previsto na Lei 8.666, no art. 43 § 3° e em consonância com as orientações e determinações do Tribunal de Contas da União, os Atestados de Capacidade Técnica apresentados poderão ser objeto de diligência para verificação de autenticidade de seu conteúdo, momento em que serão solicitados ao emitente dos atestados documentos e evidências que descrevam e comprovem a execução dos serviços ali declarados:

11.3.4. No processo de diligência serão colhidas evidências que comprovem a capacidade técnica, tais como: relatórios, registros de reunião, impressão das telas das soluções de Banco de Dados, documentação de projetos (planejamento de projeto, planos de gestão, documentos de requisitos, diagramas, especificações técnicas, padrões, dentre outros) para a devida comprovação dos serviços atestados.

11.3.5. Encontrada divergência entre o especificado nos atestados e o apurado em eventual diligência, inclusive validação do Contrato de prestação de serviços entre o emissor do atestado e a licitante, além da desclassificação no processo licitatório, fica sujeita a licitante às penalidades cabíveis.

12. CONTROLE DA EXECUÇÃO

12.1. 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.

13. DAS SANÇÕES

13.1. – Sem prejuízo das demais sanções legais cabíveis, pelo não cumprimento dos compromissos acordados, poderão ser aplicadas, a critério da Contratante, as seguintes penalidades à Contratada:

a) Aquele que, convocado dentro do prazo de validade de sua proposta, não celebrar o contrato, deixar de entregar ou apresentar documentação falsa exigida para o certame, ensejar o retardamento da execução do seu objeto, não mantiver a proposta, falhar ou fraudar na execução do contrato, comportar-se de modo inidôneo, fizer declaração falsa ou cometer fraude fiscal, garantindo o direito à ampla defesa, ficará impedido de licitar e de contratar com a Administração e será descredenciado do CADFOR, pelo prazo de até 05 (cinco) anos, sem prejuízo das multas previstas em Edital e no contrato e das demais cominações legais.

b) A inexecução contratual, inclusive por atraso injustificado na execução do contrato, sujeitará o contratado, as penalidades referidas nos arts. 86 e 87 da Lei nº 8.666/93, a advertência e multa de mora, graduada de acordo com a gravidade da infração, obedecidos os seguintes limites máximos:

I – 10% (dez por cento) sobre o valor do contrato, em caso de descumprimento total da obrigação, inclusive no de recusa do adjudicatário em firmar o contrato.

II – 0,3% (três décimos por cento) ao dia, até o trigésimo dia de atraso, sobre o valor da parte do fornecimento ou serviço não realizado.

III – 0,7% (sete décimos por cento) sobre o valor da parte do fornecimento não realizado por cada dia subsequente ao trigésimo.

c) Advertência.

d) Suspensão temporária de participação em licitação e impedimento de contratar com a Administração nos termos do art. 81 da Lei Estadual nº 17.928/2012.

e) Declaração de inidoneidade para licitar e contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação, na forma da lei, perante a Contratante.

f) As sanções previstas nas alíneas a), c), d) e e) poderão ser aplicadas junto a da alínea b).

13.2. Antes da aplicação de qualquer penalidade será garantido à Contratada o contraditório e a ampla defesa.

13.3. A multa será descontada dos pagamentos eventualmente devidos pela Contratante ou ainda, quando for o caso, cobrada judicialmente.

14. RESPONSÁVEL PELA ELABORAÇÃO DO TERMO DE REFERÊNCIA:

Goiânia, 05 de setembro de 2022.

Murilo Mendes Teixeira

Chefe do Departamento de Infraestrutura em tecnologia da Informação

Vinícius Alexandre da Silva Machado

Chefe do Departamento de Compras

Lorena Fernandes Vilarinho Mouzinho

Assessora do Departamento de Compras

Documento assinado eletronicamente por **VINICIUS ALEXANDRE DA SILVA MACHADO**, **Chefe de Departamento ou Seção**, em 05/09/2022, às 15:48, conforme art. 2º, § 2º, III, "b", da Lei 17.039/2010 e art. 3ºB, I, do Decreto nº 8.808/2016.

Documento assinado eletronicamente por **MURILO MENDES TEIXEIRA**, **Chefe de Unidade**, em 05/09/2022, às 20:41, 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 **000033380548** e o código CRC **16991C25**.

DEPARTAMENTO DE COMPRAS
ALAMEDA CORONEL JOAQUIM DE BASTOS 282, 4º ANDAR - Bairro SETOR MARISTA -
GOIANIA - GO - CEP 74175-150 - (62)3201-3509.