



**GOVERNO DE SERGIPE**  
**DEPARTAMENTO ESTADUAL DE INFRAESTRUTURA**  
**RODOVIÁRIA DE SERGIPE**

Página:1 de 9

**TERMO**

**PROCESSO Nº: 1248/2024 - COMPRAS.GOV-DER/SE**

**TERMO DE REFERÊNCIA**

**AQUISIÇÃO DE LICENÇA DE SOFTWARE DE ANTIVÍRUS**

### 1. OBJETO

Contratação de empresa (Revenda) para fornecimento de licenças de software de antivírus e suporte pelo período de 2 anos.

### 2. JUSTIFICATIVA DA CONTRATAÇÃO

A aquisição das licenças de antivírus tem o objetivo prevenir a contaminação por vírus, malwares e suas variantes bem como ameaças cibernéticas distintas nos computadores do Departamento Estadual de Infra-Estrutura Rodoviária de Sergipe (DER/SE) que podem colocar em risco o sigilo, a integridade e disponibilidade das informações.

Com o grande volume de utilização e com o crescimento da utilização de e-mails e acesso às páginas de internet a aquisição de um software de antivírus é necessária para fornecer um mínimo de segurança à infraestrutura de rede de computadores do DER/SE.

As aquisições propõem uma maior proteção aos computadores e servidores, resguardando problemas que podem prejudicar os serviços do DER/SE.

Assim, a aquisição das licenças de antivírus é considerada imprescindível para garantir a disponibilidade, integridade e confiabilidade dos dados e continuidade das atividades do DER/SE.

### 3. ESPECIFICAÇÃO DOS BENS OU SERVIÇOS

| Item | Descrição do Item                                | QTD | Valor Unitário | TOTAL |
|------|--------------------------------------------------|-----|----------------|-------|
| 01   | Aquisição de Licenças e Atualização do Antivírus | 160 |                |       |

### TERMO DE REFERÊNCIA

**Contratação de empresa (Revenda) para fornecimento de licenças de software de antivírus e suporte pelo período de 2 anos.**

#### **1. Prover segurança para estações de trabalho, sejam físicas ou em ambiente virtualizado.**

**1.1.** Possuir console central única de gerenciamento. As configurações do Antivírus, AntiSpyware, Firewall, Detecção de intrusão controle de Dispositivos e Controle de Aplicações deverão ser realizadas através da mesma console;

**1.2.** O Produto deverá ter a capacidade de remoção do software de antivírus já instalado e ser instalado de forma remota pela console de gerenciamento;

**1.3.** O produto deverá possuir no mínimo os seguintes módulos:

**1.4.** Console de Gerenciamento fornecendo funcionalidades de gestão;

**1.5.** Módulos para estações físicas, laptops e servidores;

**1.6.** Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;

**1.7.** Utilizar o conceito de heurística;

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

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



**GOVERNO DE SERGIPE**  
**DEPARTAMENTO ESTADUAL DE INFRAESTRUTURA**  
**RODOVIÁRIA DE SERGIPE**

Página:3 de 9

- 1.10.** Oferecer inventário de softwares;
- 1.11.** Oferecer tecnologia onde a solução teste arquivos potencialmente perigosos em ambiente isolado antes da execução do mesmo no ambiente de produção;
- 1.12.** Oferecer proteção por base de assinaturas;

## **2. Console De Gerenciamento**

- 2.1.** Instalação e configuração
- 2.2.** Deve ser fornecido como um appliance virtual ou executável para instalação em servidores Windows ou Console com Gerenciamento na nuvem ( Cloud).
- 2.3.** Deverá suportar no mínimos os seguintes Hypervisors: VMWarevSphere, Citrix XenServer; XenDesktop, VDI-ina- Box;
- 2.4.** Microsoft Hyper-V, Red hat Enterprise Virtualization, Kernel-based Virtual Machine ou KVM, Oracle VM;
- 2.5.** Deverá ser fornecido com base de dados embutido na Console em Nuvem, sem a necessidade de baixar para máquina do administrador da Console;
- 2.6.** Permitir instalação remota via console WEB de gerenciamento para ambientes virtual VMWare ou Citrix;
- 2.7.** O mecanismo de varredura deverá estar disponível para download separadamente;
- 2.8.** A solução deverá 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);
- 2.9.** Deve ser totalmente em português.

## **3. Características Gerais**

- 3.1.** Arquitetura simples de atualização, com botão único para acesso a todas as funções e serviços serem atualizados;
- 3.2.** Permitir que o administrador escolha qual o pacote será atualizado;
- 3.3.** As notificações devem ser destacadas como item não lida, enviar e-mail para o administrador;
- 3.4.** No mínimo enviar notificações: Problemas com licenças, Alertas de Surto de vírus, Máquinas desatualizadas, Eventos de antimalware,
- 3.5.** Painel para Monitoramento baseado em "portlets" configuráveis com no mínimo as seguintes especificações: Nome; Tipo de relatório; Alvo do relatório;
- 3.6.** Deverá disponibilizar "portlets" para qualquer serviço de segurança, máquinas físicas, virtuais, dispositivos móveis;
- 3.7.** Inventário da Rede
- 3.8.** Possuir no mínimo as integrações abaixo: Múltiplos domínios do Active Directory, Múltiplos VMWarevCenters, Múltiplos Citrix XenServers;
- 3.9.** Possuir a possibilidade de definição de sincronização com o Active Directory em horas;
- 3.10.** Deverá ser compatível com Microsoft Hyper-V, RedHat VM, Oracle VM, KVM;
- 3.11.** Descoberta de rede para máquinas em grupo de trabalho;
- 3.12.** Possuir busca em tempo real pelo menos com os seguintes filtros: Nome, Sistema Operacional e Endereço IP;
- 3.13.** Possibilitar a instalação remota e desinstalação remota do antivírus;
- 3.14.** Possibilitar a configuração de pacotes de instalação do produto de antivírus;
- 3.15.** Possuir tarefas remotas e configuráveis de Scan;
- 3.16.** Possuir tarefa de reinicialização remota de estação ou servidor;
- 3.17.** Assinar políticas para no mínimo os níveis: Computador, Máquina Virtual ou Possuir a propriedade detalhada de objetos gerenciados para: Nome, IP, Sistema Operacional, Grupo, Política Assinada, ultimo status de malware;

## **4. Políticas**

- 4.1.** Modelo único para todos os equipamentos, seja físico ou virtual;



**GOVERNO DE SERGIPE**  
**DEPARTAMENTO ESTADUAL DE INFRAESTRUTURA**  
**RODOVIÁRIA DE SERGIPE**

Página:4 de 9

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

**4.3.**Deverá configurar as funcionalidades como escaneamento do Antivírus, firewall de duas vias de detecção de intrusão, controle de acesso à rede, controle de aplicação, controle de acesso web, autenticação e ações para serem aplicadas em caso de vírus e dispositivos em não conformidade;

### **5. Relatórios**

**5.1.**Relatório para cada serviço de segurança;

**5.2.**Facilidade de usar e visualização simplificada;

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

**5.4.**Filtros de agendamento de relatórios;

**5.5.**Arquivo com todas as instâncias de relatório agendados;

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

**5.7.**Oferecer possibilidade de criar relatórios de maneira dinâmica no painel administrativo da solução.

### **6. Quarentena**

**6.1.**Restauração remota, com configuração de localidade e deleção;

**6.2.**Criação e exclusão para arquivos restaurados;

### **7. Usuários**

**7.1.**Administração baseada em regras;

**7.2.**Disponibilizar tipos de usuários pré-definidos como no mínimo: Administrador - Gerente dos componentes da solução, Administrador de rede - Gerente dos serviços de segurança;

**7.3.**Relatório - Monitora e cria relatórios;

**7.4.**Deverá ser possível customizar um tipo de usuário;

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

**7.6.**Logs de utilização;

**7.7.**Registrar as ações do usuário na console de gerenciamento;

**7.8.**Detalhar cada ação do usuário;

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

### **8. Certificado de Segurança**

**8.1.**Deverá prover o acesso via HTTPS;

**8.2.**Deverá permitir a importação de certificados digitais;

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

### **9. Proteção Para Estações De Trabalho E Servidores Físicos**

**9.1.**Deverá permitir a configuração do scan do antivírus do cliente como: Scan local, Scan Híbrido, Scan Central;

**9.2.**Deverá permitir a instalação customizada do antivírus com no mínimo: Instalar o antivírus sem o controle de acesso à internet; Instalar o antivírus sem o módulo de firewall;

**9.3.**Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho: Windows 10 32 e 64Bits, Windows 7 32 e 64Bits.

**9.4.**Deverá suportar no mínimo os seguintes sistemas operacionais para servidores: Windows Server 2022, Windows Server 2019 Core, Windows Server 2019, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2.



**GOVERNO DE SERGIPE**  
**DEPARTAMENTO ESTADUAL DE INFRAESTRUTURA**  
**RODOVIÁRIA DE SERGIPE**

Página:5 de 9

**9.5.**Deverá suportar no mínimo os seguintes sistemas operacionais para distribuição Linux: Ubuntu 14.04 LTS ou superior, Red Hat Enterprise Linux / CentOS 6.0 ou superior, SUSE Linux Enterprise Server 11 SP4 ou superior, OpenSUSE Leap 42.x, Fedora 25 ou superior, Debian 8.0 ou superior, Oracle Linux 6.3 ou superior, Amazon Linux AMI 2016.09 ou superior;

**10. Gerenciamento e Instalação Remota**

**10.1.**Deverá permitir ao administrador customizar a instalação;

**10.2.**A instalação deverá ser possível executar com no mínimo das seguintes maneiras: Executar o pacote de antivírus diretamente na estação de trabalho, instalar remotamente, distribuído via console de gerência web;

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

**10.4.**A console de gerenciamento deve incluir informações detalhadas sobre as estações e servidores com no mínimo as seguintes informações: Nome, IP, Sistema Operacional, Política Aplicada;

**10.5.**Através da console, o administrador poderá enviar uma política única para configurar o antivírus;

**10.6.**A console de gerenciamento deverá incluir sessão de log com as seguintes informações: Login, Edição, Criação, Log-out, ter a capacidade de criar um único pacote independente ser for para 32 bits ou 64 bits, deverá permitir ao administrador criar grupos e subgrupos para mover as estações de trabalho;

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

**11. Proteção Para Estações E Servidores Virtuais**

**11.1.**Proteção de antivírus dedicado para ambientes virtuais;

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

**11.3.**A console de gerenciamento central da solução deverá ter a possibilidade de integrar com múltiplos vCenters daVMWare;

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

**11.5.**O produto deverá oferecer agente para virtualização dos seguintes produtos: Citrix Xen Server, Microsoft Hyper-V, Red Hat Virtualization, Oracle KVM, KVM;

**12. Funções Gerais**

**12.1.**Deverá ter métodos de detecção de vírus, Spyware, rootkits e outros mecanismos de segurança;

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

**13. Requisitos Mínimos suportados pelo Sistema.**

**13.1.**Plataformas de Virtualização: VMware vSphereandvCenter Server:

versão 6.5;

version 6.7, incluindo update 1, update 2a e update 3;

version 7.0, incluindo update 1, update 2, update 2b, update 2c e update 2d;

version 8.0, incluindo update 1, update 2.

VMware Horizon/View 7.8, 7.7, 7.6, 7.5, 7.1, 6.x, 5.x

VMware Workstation 11.x, 10.x, 9.x, 8.0.6



VMware Player 7.x, 6.x, 5.x

Citrix XenHypervisor: 7.1 (withthe XS71ECU2060 hotfix), 8.2.

Citrix Virtual Apps e Desktops 7 1808, 7 1811, 7 1903, 7 1906

Citrix XenApp e XenDesktop 7.18, 7.17, 7.16, 7.15 LTSR, 7.6 LTSR

Citrix VDI-in-a-Box 5.x

Microsoft Hyper-V Server 2008 R2, 2012, 2012 R2, 2016, 2019 or Windows Server 2008 R2, 2012, 2012 R2, 2016, 2019 (incluindo Hyper-V Hypervisor)

RedHat Enterprise Virtualization 3.0 (incluindo KVM Hypervisor)

Oracle VM 3.0

Oracle VM VirtualBox 5.2, 5.1

NutanixPrism com AOS 5.6, 5.5, 5.20 LTS, 5.18 STS, 5.15 LTS, 5.11, 5.10 (Enterprise Edition)

NutanixPrismwith AHV 20170830.115, 20170830.301, 20170830.395 e 20190916.294 (Community Edition)

**13.2.**Sistemas Operacionais desktops (32 e 64 Bits): Windows 7, Windows 10

**13.3.**Sistemas Operacionais Servidores: Windows Server 2022 Windows Server 2019 Core Windows Server 2019, Windows Server 2019 Core, Windows Server 2016, Windows Server 2016 Core, Windows Server 2012 R2, Windows Server 2012, Windows Small Business Server (SBS) 2011, Windows Server 2008 R2, Ubuntu 14.04 LTS ou superior, Red Hat Enterprise Linux / CentOS 6.0 ou superior, SUSE Linux Enterprise Server 11 SP4 ou superior, OpenSUSE Leap 42.x, Fedora 25 ou superior, Debian 8.0 ou superior, Oracle Linux 6.3 ou superior, Amazon Linux AMI 2016.09 ou superior;

#### **14. Componentes e Funcionalidade do Antivírus Geral**

**14.1.**Deverá fazer scan em tempo real automático;

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

**14.3.**Escaneamento de comportamento heurístico;

**14.4.**Deverá escanear em tempo real qualquer informação localizadas em mídias de armazenamento como:

CD/DVD, Discos Externos, Pen-Drivers, Deverá permitir a escolha e configuração de pastas a serem escaneada;

**14.5.**Para melhor proteção, o antivírus deverá ter no mínimo 3 tipos de detecção: Baseada em Assinaturas, Baseada em Heurística, Baseada em monitoramento contínuo de processos;

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

**14.7.**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;

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

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

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



**GOVERNO DE SERGIPE**  
**DEPARTAMENTO ESTADUAL DE INFRAESTRUTURA**  
**RODOVIÁRIA DE SERGIPE**

Página:7 de 9

- 14.11.**Deverá fazer a remoção automática de arquivos antigos, pré-definidos pelo administrador;
- 14.12.**Deverá permitir a movimentação do arquivo da quarentena para seu local original ou outro destino que o administrador definir;
- 14.13.**Deverá de forma automática criar exclusão para arquivos restaurados da quarentena;
- 14.14.**Deverá permitir escanear a quarentena após a atualização das atualizações de assinaturas;

**15. Controle de Usuário**

- 15.1.**Deverá ter módulo de controle de usuário integrando com as seguintes características: Bloqueio de acesso à internet, Bloqueio de acesso a aplicações definidas pelo administrador;

**16. Controle do Dispositivo**

- 16.1.**Deverá ser possível a instalação do módulo de controle de dispositivos através da console de gerenciamento;
- 16.2.**Através do módulo de controle de dispositivo deverá ser possível controlar: Bluetooth, CDRom/DVDROM, IEEE 1284.4, IEEE 1394, Windows Portable, Adaptadores de Rede, Adaptadores de rede Wireless, Discos Externos;
- 16.3.**Deverá permitir regras de definição de bloqueio/desbloqueio;
- 16.4.**Deverá permitir regras de exclusão;

**17. Atualização**

- 17.1.**Após a atualização o administrador deverá ter a capacidade de adiar uma reinicialização;
- 17.2.**Possibilidade de utilizar um servidor local para efetuar as atualizações das estações de trabalho;
- 17.3.**Permitir atualizações de assinatura de hora em hora;
- 17.4.**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.

**18. Proteção para caixa de e-mail:**

- 18.1.**Fornecer proteção para ambiente Exchange
- 18.2.**Oferecer tecnologia para proteção contra spam;
- 18.3.**Oferecer análise comportamental e proteção para zero-day;
- 18.4.**Oferecer proteção contra vírus e tentativas de phishing;

**19. Criptografia**

- 19.1.**Possibilidade de criptografia de disco através da console de gerenciamento seja em nuvem ou on-premise com módulo de Criptografia presente na mesma Console do Antivirus.
- 19.2.**Deverá utilizar quando necessários serviços de criptografia através agentes nativos da estação de trabalho baseada em Windows (BitLocker) ou Mac (FileVault);
- 19.3.**Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;
- 19.4.**Deverá ser compatível com:

macOS Sonoma (14.x)

macOS Ventura (13.x)

macOS Monterey (12.x)

macOS Big Sur (11.x)

**20. Proteção Avançada NGAV**



**GOVERNO DE SERGIPE**  
**DEPARTAMENTO ESTADUAL DE INFRAESTRUTURA**  
**RODOVIÁRIA DE SERGIPE**

Página:8 de 9

**20.1.** Detectar e bloquear todos os tipos de ameaças sofisticadas e malwares desconhecidos bem como eliminar malwares desconhecidos e ameaças avançadas que ignoram as soluções tradicionais de proteção de endpoints, incluindo o ransomware. Detectar e bloquear ataques avançados, como os ataques do PowerShell, baseados em scripts, ataques sem arquivos e malware sofisticado, devendo ser detectados e bloqueados antes de serem executados.

**20.2.** Detectar e parar, bloquear e interromper malwares sem arquivos.

**20.3.** Parar os ataques com base em macros e scripts. Analisar scripts, como Powershell, WMI, intérpretes de Javascript, etc, bem como adicionar técnicas de analisador de linha de comando para interceptar e proteger scripts, enquanto alerta os administradores e bloqueia a execução de scripts no caso de executar comandos maliciosos.

**20.4.** Reparo e resposta automatizada a ameaças

**20.5.** Quando uma ameaça é detectada, a ferramenta deve neutralizá-la imediatamente por meio de ações que incluem a conclusão do processo, a quarentena, a exclusão e a reversão de alterações mal intencionadas. Compartilhar as informações sobre ameaças em tempo real com a GPN, o serviço de inteligência contra ameaças baseadas na nuvem do fabricante, para impedir ataques semelhantes.

**20.6.** Obter visibilidade e contexto sobre ameaças devendo identificar e reportar atividades suspeitas alertando antecipadamente para comportamentos maliciosos, como ações suspeitas do sistema operacional.

**20.7.** Operar com um único agente e console integrados bem como personalizar automaticamente o pacote de instalação e minimizar o carregamento do agente.

**20.8.** Deverá ter um nível de proteção na fase de pré-execução com modelos locais de aprendizado de máquina e heurística avançada e treinada para detectar ferramentas de hackers, explorações e técnicas de ocultação de malware, a fim de bloquear ameaças sofisticadas antes que elas sejam executadas. Também deverá detectar técnicas de propagação e sites que hospedam kits de exploração, além de bloquear tráfego suspeito na web. Deverá permitir que os administradores de segurança ajustem a proteção para combater os riscos.

## **21. Machine Learning**

**21.1.** As técnicas de Machine Learning devem utilizar modelos e algoritmos extensamente treinados para prever e bloquear os ataques avançados.

**21.2.** A ferramenta de Machine Learning deve se basear em características estáticas e dinâmicas, e se treinar continuamente com bilhões de amostras de arquivos legítimos e maliciosos devendo melhorar significativamente a efetividade da detecção de malware e minimizar os falsos positivos. ações evasivas e conexões a centros de comando e controle.

## **22. Sandbox**

**22.1.** Sandbox integrado nos terminais que deverá analisar arquivos suspeitos em profundidade, acionar ações destrutivas em um ambiente virtual isolado, hospedado pelo fabricante, analisando seu comportamento e informando sobre intenções maliciosas. O Sandbox deve ser integrado com o agente e encaminhar automaticamente os arquivos suspeitos para análise. Ao retornar uma análise com resultado "malicioso", o Sandbox deverá bloquear automaticamente o arquivo malicioso em sistemas em toda rede imediatamente. O recurso de envio automático deve permitir que os administradores de segurança da empresa escolham o modo de monitoramento ou bloqueio, o que impede o acesso a um arquivo até que um resultado seja emitido. Os administradores também podem enviar arquivos manualmente para análise. As informações forenses devem fornecer um contexto claro das ameaças e ajudar a entender o comportamento delas.

## **23. Antiexploit Avançado**

**23.1.** Deverá conter antiexploit avançado para prevenção de exploração e proteção a memória e aplicativos vulneráveis, como navegadores, leitores de documentos, arquivos multimídia e tempo de execução (ou seja: Flash



ou Java). Os mecanismos avançados devem observar a rotina de acesso na memória para detectar e bloquear técnicas de exploração, como verificação de chamadas de API, pivotamento de pilha, ROP (return-oriented programming), etc.

#### **24. Inspetor de processo**

**24.1.** O Inspetor de Processos deverá operar em um modo de confiança zero, monitorando continuamente todos os processos em execução no sistema operacional. Deverá procurar atividades suspeitas ou comportamentos anormais de processos, como tentativas de ocultar o tipo de processo, executar código no espaço de outro processo (sequestro de memória do processo para escalonamento de privilégios), replicar, descartar arquivos, ocultar para processar aplicativos de listagem etc. Tomar as medidas de reparação adequadas, incluindo o encerramento do processo e a reversão das alterações efetuadas. Deverá detectar de malwares desconhecidos, avançados e ataques sem arquivos, incluindo ransomware.

#### **21. Detecção e Resposta - EDR**

**21.1.** Deverá realizar a correlação entre terminais, conhecida como EDR, levando a detecção de ameaças bem como aplicar funcionalidades de XEDR para detectar ataques avançados em vários terminais em infraestruturas híbridas (estações de trabalho ou servidores executando vários sistemas operativos)

**21.2.** Deverá analisar continuamente os riscos usando centenas de fatores para descobrir e priorizar os riscos de configuração para todos os seus terminais, permitindo ações automáticas de fortalecimento. Identificar ações e comportamentos dos usuários que representam um risco de segurança para a organização, como o uso de páginas web não criptografadas para fazer login em sites, gerenciamento de senhas inadequado, uso de USBs comprometidos, infecções recorrentes, etc.



**ASSINADO ELETRONICAMENTE**  
Verificar autenticidade conforme mensagem  
apresentada no rodapé do documento

ANTONIO SANTANA RABELO  
Gerente



**ASSINADO ELETRONICAMENTE**  
Verificar autenticidade conforme mensagem  
apresentada no rodapé do documento

Anderson das Neves Nascimento  
Diretor(a) Presidente

## Protocolo de Assinatura(s)

O documento acima foi proposto para assinatura digital. Para verificar as assinaturas acesse o endereço <http://edocsergipe.se.gov.br/consultacodigo> e utilize o código abaixo para verificar se este documento é válido.

Código de verificação: JJMM-RX8L-6BMI-RCAR



O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 30/10/2024 é(são) :

Legenda: ● Aprovada ● Indeterminada ● Pendente

- Anderson das Neves Nascimento - 18/10/2024 10:36:26 (Docflow)
- ANTONIO SANTANA RABELO - 18/10/2024 10:21:11 (Docflow)