# ESTUDO TÉCNICO PRELIMINAR

**Município de Taquari - RS**
**Secretaria Municipal de Administração**
**Necessidade da Administração: Aquisição - SOFTWARE ANTIVÍRUS COM SOLUÇÃO EDR**

1. **DESCRIÇÃO DA NECESSIDADE**
O presente estudo visa a contratação de empresa especializada para o fornecimento de 150 licenças de software antivírus com solução EDR (Endpoint Detection and Response), visando à proteção cibernética dos sistemas da Prefeitura Municipal de Taquari/RS. A contratação é essencial para reforçar a segurança contra ameaças cibernéticas, como vírus, malwares, ransomware e outros tipos de ataques virtuais, protegendo dados sensíveis e garantindo a integridade e disponibilidade dos sistemas e informações municipais.

2. **QUANTO À ESCOLHA DA SOLUÇÃO**
A escolha da solução de software antivírus com funcionalidade EDR não se trata de uma preferência de marca ou fabricante, mas sim de uma solução que atenda às necessidades específicas de segurança cibernética da Prefeitura Municipal de Taquari-RS, alinhada com a infraestrutura tecnológica já existente e a continuidade das operações de proteção contra ameaças cibernéticas. A proteção dos dados sensíveis da administração pública é uma prioridade estratégica, principalmente diante das crescentes ameaças digitais, como vírus, malwares e ransomware, que podem comprometer a continuidade dos serviços públicos e a segurança da informação.

A solução escolhida deverá ser capaz de detectar e mitigar ameaças com alta eficiência, oferecendo uma plataforma robusta e eficiente para a gestão centralizada de segurança em múltiplos dispositivos. A ferramenta deverá ser comprovadamente eficaz e confiável na proteção dos sistemas da Prefeitura de Taquari, permitindo que o Departamento de Informática, responsável pela administração da infraestrutura de TI, continue a proteger a integridade dos dados e a segurança da rede municipal de maneira eficiente e contínua.

A solução será uma ferramenta amplamente reconhecida no mercado, distribuída por revendedores autorizados, garantindo a competitividade do processo licitatório sem comprometer a qualidade e a confiabilidade da solução fornecida. A continuidade da utilização de soluções eficazes e comprovadas está diretamente alinhada ao Plano de Contratações Anual da Prefeitura e ao Planejamento Estratégico de Tecnologia da Informação municipal, que preveem a manutenção de soluções robustas no combate a ciberameaças.

Portanto, a escolha da solução de software antivírus com EDR reflete a necessidade de dar continuidade à proteção digital da Prefeitura Municipal de Taquari, garantindo a segurança dos dados sensíveis e a continuidade das operações governamentais.

3. **ALINHAMENTO ENTRE A CONTRATAÇÃO E O PLANEJAMENTO**
A contratação está prevista no Plano de Contratações Anual do Município de Taquari-RS, conforme demonstrando alinhamento com o planejamento desta Administração.

4. **DESCRIÇÃO DOS REQUISITOS DA CONTRATAÇÃO**
Considerando a imprescindível necessidade de contratação de solução de software antivírus com funcionalidade EDR, destaca-se que a aquisição de 150 licenças deste produto será realizada por meio de processo licitatório, em conformidade com a Lei nº 14.133/2021. Este processo licitatório busca garantir a obtenção da melhor proposta em termos de preço e qualidade, bem como assegurar que a contratação atenda a todos os requisitos de segurança cibernética da Administração Municipal.

5. **ESTIMATIVA DAS QUANTIDADES**
A estimativa é de 150 licenças do software antivírus com funcionalidade EDR, com validade de 36 meses (3 anos).

6. **ALTERNATIVAS DISPONÍVEIS NO MERCADO**
Durante o processo de pesquisa de mercado, foram utilizadas diversas fontes de informação, como a ferramenta **LicitaCon Cidadão**, disponibilizada pelo Tribunal de Contas do Estado do Rio Grande do Sul (TCE-RS), para obter informações sobre aquisições similares. A seguir, os processos encontrados:

- **Qualitek Tecnologia LTDA** (CNPJ: 10.224.281/0001-10):
Valor unitário: **R$ 275,08**

  Prazo de entrega: **10 dias**
- **Automassul Informática LTDA** (CNPJ: 03.683.195/0001-00):
Valor unitário: **R$ 235,00**

  (Informações obtidas por meio do **LicitaCon Cidadão**, Prefeitura Municipal de Toque Gonzales-RS)
- **Compumaq Soluções em Informática** (CNPJ: 91.663.815/0001-06):
Valor unitário: **R$ 195,00**

  (Informações obtidas por meio do **LicitaCon Cidadão**, Município de São Pedro da Serra-RS)

- **Vila Sanches da Rocha Morciani Informática** (CNPJ: 79.550.265/0001-13):
Valor unitário: **R$ 260,00**

  (Informações obtidas por meio do **LicitaCon Cidadão**, Câmara Municipal de Torres-RS)

| Empresa | Valor Unitário (R$) | Valor Total para 150 Licenças (R$) |
|---|---|---|
| Qualitek Tecnologia LTDA | R$ 275,08 | R$ 41.262,00 |
| Automassul Informática LTDA | R$ 235,00 | R$ 35.250,00 |
| Compumaq Soluções em Informática | R$ 195,00 | R$ 29.250,00 |

| | | |
|---|---|---|
| Vila Sanches da Rocha Morciani Informática | R$ 260,00 | R$ 39.000,00 |
| Valor Médio Unitário | | R$ 241,27 |

## 7. ESTIMATIVA DO VALOR DA CONTRATAÇÃO

Estima-se o valor total de **R$ 36.190,50**, considerando o **valor médio unitário** de **R$ 241,27**.

## 8. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

**SOFTWARE ANTIVÍRUS COM SOLUÇÃO EDR FOUNDATIONS COM AS SEGUINTES ESPECIFICAÇÕES**

1. **Do módulo de proteção de endpoint**
   - 1.1. A solução proposta deverá proteger os sistemas operacionais abaixo:
     - 1.1.1. Windows 7
     - 1.1.2. Windows 8
     - 1.1.3. Windows 8.1
     - 1.1.4. Windows 10
     - 1.1.5. Windows 11
   - 1.2. Servidores
     - 1.2.1. Windows Small Business Server 2011
     - 1.2.2. Windows MultiPoint Server 2011
     - 1.2.3. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022
   - 1.3. Servidores de terminal Microsoft
     - 1.3.1. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022
   - 1.4. Sistemas operacionais Linux de 32 bits:
     - 1.4.1. CentOS 6.7 e posterior
     - 1.4.2. Debian GNU/Linux 11.0 e posterior
     - 1.4.3. Debian GNU/Linux 12.0 e posterior
     - 1.4.4. Red Hat Enterprise Linux 6.7 e posterior
   - 1.5. Sistemas operacionais Linux de 64 bits:
     - 1.5.1. Amazon Linux 2.
     - 1.5.2. CentOS 6.7 e mais tarde
     - 1.5.3. CentOS 7.2 e posterior.
     - 1.5.4. CentOS Stream 8.
     - 1.5.5. CentOS Stream 9.
     - 1.5.6. Debian GNU/Linux 11.0 e posterior.
     - 1.5.7. Debian GNU/Linux 12.0 e posterior.
     - 1.5.8. Linux Mint 20.3 e superior.
     - 1.5.9. Linux Mint 21.1 e posterior.
     - 1.5.10. openSUSE Leap 15.0 e posterior.
     - 1.5.11. Oracle Linux 7.3 e posterior.
     - 1.5.12. Oracle Linux 8.0 e posterior.
     - 1.5.13. Oracle Linux 9.0 e posterior.
     - 1.5.14. Red Hat Enterprise Linux 6.7 e posterior
     - 1.5.15. Red Hat Enterprise Linux 7.2 e posterior.
     - 1.5.16. Red Hat Enterprise Linux 8.0 e posterior.
     - 1.5.17. Red Hat Enterprise Linux 9.0 e posterior.
     - 1.5.18. Rocky Linux 8.5 e posterior.
     - 1.5.19. Rocky Linux 9.1.

1.5.20. SUSE Linux Enterprise Server 12.5 ou posterior.
1.5.21. SUSE Linux Enterprise Server 15 ou posterior.
1.5.22. Ubuntu 20.04 LTS.
1.5.23. Ubuntu 22.04 LTS.
1.5.24. Sistemas operacionais Arm de 64 bits:
1.5.25. CentOS Stream 9.
1.5.26. SUSE Linux Enterprise Server 15.
1.5.27. Ubuntu 22.04 LTS.

1.6. Sistemas operacionais MAC OS:
1.6.1. macOS 12 – 14

1.7. Ferramentas de virtualização MAC OS:
1.7.1. Parallels Desktop 16 para Mac Business Edition
1.7.2. VMware Fusion 11.5 Profissional
1.7.3. VMware Fusion 12 Profissional

1.8. A solução proposta deverá suportar as seguintes plataformas virtuais:
1.8.1. VMware Workstation 17.0.2 Pro
1.8.2. VMware ESXi 8.0 Update 2
1.8.3. Microsoft Hyper-V Server 2019
1.8.4. Citrix Virtual Apps e Desktop 7 2308
1.8.5. Citrix Provisioning 2308
1.8.6. Citrix Hypervisor 8.2 Update 1

**2. Do módulo de gerenciamento avançado**

2.1. A solução proposta deve suportar arquitetura cloud-native e on-premisse;

2.2. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:
2.2.1. Amazon Web Services
2.2.2. Microsoft Azure

2.3. A solução proposta deve incluir as seguintes opções de integração SIEM:
2.3.1. HP (Microfoco) ArcSight
2.3.2. IBM QRadar
2.3.3. Splunk
2.3.4. KUMA

2.4. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

2.5. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

2.6. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

2.7. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

2.8. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

2.9. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

2.10. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

2.11. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

2.12. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.

2.13. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

2.14. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:
2.14.1. Status do dispositivo

2.14.2. Tag
2.14.3. Diretório ativo
2.14.4. Proprietários de dispositivos
2.14.5. Hardware

2.15. A solução proposta deve suportar os seguintes canais de entrega de notificação:
2.15.1. E-mail
2.15.2. Registro de sistema
2.15.3. SMS

2.16. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:
2.16.1. Atributos de rede
2.16.2. Nome
2.16.3. Domínio e/ou Sufixo de Domínio
2.16.4. Endereço de IP
2.16.5. Endereço IP para servidor de gerenciamento
2.16.6. Localização no Active Directory
2.16.7. Unidade organizacional
2.16.8. Grupo
2.16.9. Sistema operacional
2.16.10. Número do pacote de serviço
2.16.11. Arquitetura Virtual
2.16.12. Registro de aplicativos
2.16.13. Nome da Aplicação
2.16.14. Versão do aplicativo
2.16.15. Fabricante
2.16.16. Tipo e versão
2.16.17. Arquitetura

2.17. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

2.18. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

2.19. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:
2.19.1. Dispositivos Desktop/Servidores
2.19.2. Dispositivos móveis
2.19.3. Dispositivos de rede
2.19.4. Dispositivos virtuais
2.19.5. Componentes OEM
2.19.6. Periféricos de computador
2.19.7. Dispositivos IoT conectados
2.19.8. Telefones VoIP
2.19.9. Repositórios de rede

2.20. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:
2.20.1. Nome da Aplicação
2.20.2. Caminho do aplicativo
2.20.3. Metadados do aplicativo
2.20.4. Aplicativo Certificado digital
2.20.5. Categorias de aplicativos predefinidas pelo fornecedor
2.20.6. SHA256 e MD5

2.21. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:
2.21.1. Bluetooth
2.21.2. Dispositivos móveis
2.21.3. Modems externos
2.21.4. CD/DVD
2.21.5. Câmeras e scanners
2.21.6. MTPs
2.21.7. E a transferência de dados para dispositivos móveis

2.22. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

2.23. A solução sugerida deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

2.24. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

2.24.1. Estruturas de domínios e grupos de trabalho do Windows

2.24.2. Estruturas de grupos do Active Directory

2.24.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador

2.25. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

2.26. A solução proposta deve permitir realizar as seguintes ações para endpoints:

2.26.1. Verificação manual;

2.26.2. Verificação no acesso;

2.26.3. Verificação por demanda;

2.26.4. Verificação de arquivos compactados

2.26.5. Verificação de arquivos individuais, pastas e unidades;

2.26.6. Bloqueio e verificação de scripts

2.26.7. Proteção contra alteração de registros;

2.26.8. Proteção contra estouro de buffer;

2.26.9. Verificação em segundo plano/inativa

2.27. Verificação de unidade removível na conexão com o sistema;

2.28. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.

2.29. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.

2.30. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.

2.31. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.

2.32. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.

2.33. A solução proposta deve suportar Windows Failover Cluster.

2.34. A solução proposta deve ter um recurso de clustering integrado.

2.35. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.

2.36. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.

2.37. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.

2.38. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.

2.39. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.

2.40. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.

2.41. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.

2.42. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.

2.43. A solução proposta deverá possuir controles para download de DLL e drivers.

2.44. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão.

2.45. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.
2.46. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).
2.47. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.
2.48. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.
2.49. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.
2.50. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.
2.51. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.
2.52. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança antimalware através do servidor de administração.
2.53. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.
2.54. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações antimalware instalados, e para distribuir notificações sobre eventos por e-mail.
2.55. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.
2.56. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.
2.57. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. .
2.58. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.
2.59. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.
2.60. A solução proposta deve permitir ao administrador personalizar relatórios.
2.61. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.
2.62. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.
2.63. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.
2.64. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.
2.65. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.
2.66. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.

2.67. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;
2.68. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.
2.69. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:
2.70. Windows
2.71. Linux

3. A solução proposta deverá suportar os seguintes servidores de banco de dados:
   3.1. Windows:
      3.1.1. Microsoft SQL Server
      3.1.2. Microsoft Banco de dados SQL do Azure
      3.1.3. MySQL Standard e Enterprise
      3.1.4. MariaDB
      3.1.5. PostgreSQL
   3.2. Linux:
      3.2.1. MySQL
      3.2.2. MariaDB
      3.2.3. PostgreSQL
4. A solução proposta deverá suportar as seguintes plataformas virtuais:
   4.1. Windows:
      4.1.1. VMware vSphere 6.7 e 7.0
      4.1.2. Estação de trabalho VMware 16 Pro
      4.1.3. Servidor Microsoft Hyper-V 2012 de 64 bits
      4.1.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
      4.1.5. Microsoft Servidor Hyper -V 2016 de 64 bits
      4.1.6. Servidor Microsoft Hyper-V 2019 de 64 bits
      4.1.7. Servidor Microsoft Hyper-V 2022 de 64 bits
      4.1.8. Citrix XenServer 7.1 LTSR
      4.1.9. Citrix XenServer 8.x
      4.1.10. Oracle VM VirtualBox 6.x
   4.2. Linux:
      4.2.1. VMware vSphere 6.7, 7.0 e 8.0
      4.2.2. VMware Desktop 16 Pro e 17 Pro
      4.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits
      4.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits
      4.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits
      4.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits
      4.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits
      4.2.8. Citrix XenServer 7.1 e 8.x
      4.2.9. Oracle VM VirtualBox 6.x e7.x

**5. Do módulo de gerenciamento simplificado**
   5.1. A solução proposta deve suportar arquitetura cloud;
   5.2. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.
   5.3. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.
   5.4. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.
   5.5. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.
   5.6. A solução proposta deve atender as condições apontadas no item e subintes 6.
   5.7. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.
   5.8. A solução proposta deve incluir informações do endpoint:
      5.8.1. IP público de internet;
      5.8.2. IP interno do dispositivo;

5.8.3. Versão do agente de proteção;
5.8.4. Ultima comunicação com a console, contendo data e hora;
5.8.5. Informações do sistemas operacional;

**6. Requisitos gerais**

6.1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
6.1.1. Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.
6.2. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
6.3. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).
6.4. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.
6.5. A solução proposta deve suportar o subsistema Linux no Windows.
6.6. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
6.6.1. Proteção contra ameaças sem arquivos (Fileless);
6.6.2. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;
6.7. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;
6.8. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.
6.9. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.
6.10. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.
6.11. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.
6.12. A solução proposta deve fornecer análise comportamental baseada em machine learning.
6.13. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.
6.14. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
6.14.1. Controles de aplicativos,
6.14.2. Controle web e dispositivos
6.14.3. HIPS e Firewall
6.14.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;
6.15. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.
6.16. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.
6.17. A solução proposta deve ter bancos de dados de reputação locais e globais.
6.18. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.
6.19. A solução proposta deve incluir um módulo capaz, no mínimo, de:
6.19.1. Bloqueio de aplicativos com base em sua categorização.
6.19.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.
6.19.3. A adição de sub-redes e a modificação de permissões de atividade.
6.20. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.
6.21. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.

6.22. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.
6.23. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.
6.24. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.
6.25. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.
6.26. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.
6.27. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.
6.28. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.
6.29. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.
6.30. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;
6.31. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;
6.32. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.
6.33. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.
6.34. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.
6.35. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.
6.36. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.
6.37. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.
6.38. A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.
6.39. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.
6.40. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.
6.41. A solução proposta deve ter categoria de detecção para bloquear banners de sites.
6.42. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;
6.43. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.
6.44. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.
6.45. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.
6.46. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

6.47. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.
6.48. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.
6.49. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.
6.50. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.
6.51. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.
6.52. A solução proposta deve suportar o controle de scripts executados em PowerShell.
6.53. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.
6.54. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.
6.55. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.
6.56. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.
6.57. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.
6.58. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.
6.59. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
6.59.1. Filtro de anexos.
6.59.2. Verificação de mensagens de email ao receber, ler e enviar.
6.60. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.
6.61. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;
6.62. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);
6.63. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.
6.64. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.
6.65. A solução proposta deve incluir suporte ao protocolo IPv6.
6.66. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.
6.67. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
6.68. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.
6.69. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.
6.70. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.
6.71. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.
6.72. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.
6.73. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.

6.74. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.
6.75. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.
6.76. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.
6.77. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.
6.78. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.
6.79. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.
6.80. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.
6.81. A solução proposta deve suportar endereços IPv6.
6.82. A solução proposta deve suportar verificação em duas etapas (autenticação).
6.83. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.
6.84. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.
6.85. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.
6.86. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.
6.87. A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.
6.88. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.
6.89. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.
6.90. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.
6.91. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.
6.92. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.
6.93. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.
6.94. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.
6.95. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.
6.96. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.
6.97. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.
6.98. A solução proposta deve ter a capacidade de excluir atualizações baixadas.

## 9. JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA CONTRATAÇÃO

Não se aplica o princípio do parcelamento devido à inviabilidade técnica e à perda de economia de escala, considerando que o software exige uma licença única para sua implementação.

10. **RESULTADOS PRETENDIDOS**
A contratação do SOFTWARE ANTIVÍRUS COM SOLUÇÃO EDR visa garantir a segurança dos dados municipais, reforçando as defesas contra ameaças cibernéticas e protegendo as informações sensíveis da administração pública. O principal objetivo é garantir a continuidade das operações governamentais sem interrupções causadas por incidentes de segurança.

11. **PROVIDÊNCIAS PRÉVIAS AO CONTRATO**
Não há necessidade de providências prévias adicionais além das indicadas no texto.

12. **CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES**
Não são identificadas contratações acessórias para a execução do objeto, uma vez que todos os meios necessários podem ser supridos pela contratação proposta.

13. **POSSÍVEIS IMPACTOS AMBIENTAIS**
A contratação do SOFTWARE ANTIVÍRUS COM SOLUÇÃO EDR não causará impactos ambientais diretos, pois se trata de um produto digital. Não há necessidade de produção de materiais físicos, e as atualizações do software são realizadas virtualmente, o que minimiza a geração de resíduos eletrônicos.

14. **DECLARAÇÃO DE VIABILIDADE**
Com base na justificativa e nas especificações técnicas, declaramos que a contratação é viável, atendendo aos padrões e preços de mercado.

15. **LICENCIAMENTO E GARANTIA**

- Todos os itens e serviços devem estar licenciados e válidos, no mínimo, pelo período de 36 meses contados a partir da data da entrega das licenças.
- A solução deve possuir garantia do fabricante da solução pelo mesmo prazo de licenciamento dos produtos.
- Caberá ao fabricante, durante a vigência da garantia, disponibilizar atualizações para as bases de assinaturas de malwares e componentes da solução.