TERMO DE REFERÊNCIA

Processo n.º 3968/2025 – COMP.CON.DIRETA-SEAD

1.0. OBJETO.

1. Contratação de 600 (seiscentas) licenças de uma solução de software de antivírus corporativo com capacidade de correlacionar eventos de segurança cibernética em toda a infraestrutura administrativa.

1.1. Os bens objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar.

1.3. Especificações

ITEM	DESCRIÇÃO	COD	UNID	QUANT	VL. UNT. SANEADO	VL. TOTAL SANEADO
1	SOFTWARE - TIPO ANTI VIRUS PARA SERVIDORES E ESTAÇÕES, COM VERSÃO ATUALIZADA,COM INSTALAÇÃO, SUPORTE E GARANTIA, DEMAIS INFORMAÇÕES CONFORME TERMO DEREFERÊNCIA.	457225-4	UND	600	R$ 104,05	R$ 62.700,00
					VALOR TOTAL SANEADO	R$ 62.700,00
A “média saneada” consiste em realizar uma avaliação crítica dos preços obtidos na pesquisa, a fim de descartar valores *(se houver*) que apresentem grandes variações em relação aos demais.						
Regra: A composição dos valores de mercado, evita-se a ocorrência de discrepâncias significativas nos valores das amostras obtidas, retirando do conjunto dos dados os valores extremos de desvios, a fim de reduzir o coeficiente de variação, conferindo confiabilidade e representatividade na aferição dos preços correntes de mercado.						
Usando o CV (Coeficiente de Variação) como parâmetro de homogeneidade do conjunto de dados, pode-se expurgar os extremos inferiores e superiores, de tal forma a obter CV menor que 25%. Para delimitar esses extremos, calcula-se a média mais (+) o desvio padrão (limite superior) e a média menos (-) o desvio padrão (limite inferior). O que estiver fora dessa faixa é eliminado.						
CV= (DP/M)/3						
Limite Superior: Média (M) + Desvio Padrão (DP)						
Limite Inferior: Média (M) – Desvio Padrão (DP)						

2.0. DOTAÇÃO ORÇAMENTÁRIA

2.1- A Despesa será realizada com os recursos orçamentários previstos para o exercício de 2025,

conforme abaixo:

15104 – Unidade Orçamentária	Secretaria de Estado da Administração
04 - Função	Administração
126 – Sub-função	Tecnologia da Informação
0036 – Programa de Governo	Coordenação e Manutenção do Poder executivo
0721 – Ação/Projeto/Atividade	Gestão da Tecnologia da Informação
339040 Natureza da Despesa	Outras despesas correntes
Fonte de Recursos	1500

3.0. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. Considerando a necessidade de contratação de empresa especializada não apenas no fornecimento, mas também na instalação e implantação. Sendo o suporte técnico da solução, incluindo atualizações contínuas pelo fabricante durante 36 (trinta e seis) meses, o que assegura a perenidade e a efetividade do sistema. A implementação de antivírus corporativo robusto, além de constituir medida corretiva, representa ação preventiva imprescindível para manter o controle e a visibilidade da infraestrutura tecnológica da Administração, permitindo neutralizar ameaças antes que ocasionem prejuízos irreparáveis à continuidade dos serviços públicos; Evidencia-se, adicionalmente, que, no âmbito do dever legal de licitar, foram realizadas consultas às Atas de Registro de Preços vigentes no Portal do ComprasNet.SE (https://www.comprasnet.se.gov.br/), em licitações em curso inseridas no Sistema, bem como Pregões Eletrônicos do Sistema de Registro de Preços (SRP), para que fosse objeto de "carona", não obtendo êxito, uma vez que as especificações e/ou quantidades não atenderam à demanda do setor requisitante.

3.2. A proposta inclui a contratação de uma empresa especializada para a instalação e implantação do software, sendo o suporte técnico e atualizações contínuas pelo fabricante por um período de 36 meses.

3.3. Assim sendo, por se tratar de *software* fundamental para o desenvolvimento das atividades atribuídas aos profissionais da Diretoria de Tecnologia da Informação/SEAD, justifica-se a aquisição do software acima mencionado.

3.3 A Contratação dos serviços poderá ocorrer de forma direta em conformidade com o Art. 75, inciso II, da Lei 14.133/2021, devido ao baixo valor estimado para contratação.

4.0. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERANDO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

4.1. Para a necessidade da SEAD não se vislumbra outra maneira a não ser na modalidade subscrição /assinatura, ou seja, licenciamento pago como serviço. A subscrição/assinatura dá direito à utilização da

licença apenas durante o período contratado e inclui acesso imediato às atualizações, melhorias e suporte, durante o período contratado.

5.0. REQUISITOS DA CONTRATAÇÃO

5.1.A contratação será por "Valor Unitário por item" com fornecimento de acordo com a necessidade da Contratante sendo o prazo de entrega de até 10 dias a contar do recebimento da Nota de Empenho/Ordem de Fornecimento/Contrato.

5.2 Validade da Proposta: Validade de 60 (Sessenta) dias corridos.

5.3 A Contratada deverá possuir atividade econômica compatível com o objeto proposto pela administração pública.

5.4. Atender as exigências legais cabíveis ao processo realizado.

5.5. Os produtos deverão possuir garantia de até 36 (trinta e seis) meses.

5.6. Deverão ser fornecidos todas as licenças de uso em nome do órgão adquirente e conter as seguintes características;

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

 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;

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

 O produto deverá possuir no mínimo os seguintes módulos:

 Console de Gerenciamento fornecendo funcionalidades de gestão;
 Módulos para estações físicas, laptops e servidores;
 Módulo para ambientes virtualizados, sendo criado especialmente para ambientes virtuais;

 Utilizar o conceito de heurística;

 Oferecer tecnologia onde a solução explore vulnerabilidades de softwares instalados no intuito de reduzir o risco de infecções (anti-exploit);
 Oferecer tecnologia nativa no intuito de eliminar ameaças do tipo Ransomware;

 Oferecer inventário de softwares;

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

 Oferecer proteção por base de assinaturas;

2. Console De Gerenciamento

 Instalação e configuração

 Deve ser fornecido como um appliance virtual ou executável para instalação em servidores Windows ou Console com Gerenciamento na nuvem (Cloud).

 Deverá suportar no mínimos os seguintes Hypervisors: VMWare vSphere, Citrix XenServer; XenDesktop, VDI-ina-Box e Proxmox, Microsoft Hyper-V, Red hat Enterprise Virtualization, Kernelbased Virtual Machine ou KVM, Oracle VM;

 Deverá ser fornecido com base de dados embutido na Console em Nuvem, sem a necessidade de baixar para máquina do administrador da Console;

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

 O mecanismo de varredura deverá estar disponível para download separadamente;

 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);

 Deve ser totalmente em português.

3. Características Gerais

 Arquitetura simples de atualização, com botão único para acesso a todas as funções e serviços serem atualizados;

 Permitir que o administrador escolha qual o pacote será atualizado;

 As notificações devem ser destacadas como item não lida, enviar e-mail para o administrador;

 No mínimo enviar notificações: Problemas com licenças, Alertas de Surto de vírus, Máquinas desatualizadas, Eventos de antimalware;

 Painel para Monitoramento baseado em "portlets" configuráveis com no mínimo as seguintes especificações: Nome; Tipo de relatório; Alvo do relatório;

 Deverá disponibilizar "portlets" para qualquer serviço de segurança, máquinas físicas, virtuais, dispositivos móveis;

 Inventário da Rede

 Possuir no mínimo as integrações abaixo: Múltiplos domínios do Active Directory, Múltiplos VMWare vCenters, Múltiplos Citrix Xen Servers;

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

 Deverá ser compatível com Microsoft Hyper-V, Red Hat VM, Oracle VM, KVM;

 Descoberta de rede para máquinas em grupo de trabalho;

 Possuir busca em tempo real pelo menos com os seguintes filtros: Nome, Sistema Operacional e Endereço IP;

 Possibilitar a instalação remota e desinstalação remota do antivírus;

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

 Possuir tarefas remotas e configuráveis de Scan;

 Possuir tarefa de reinicialização remota de estação ou servidor;

 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

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

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

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

5. Relatórios

 Relatório para cada serviço de segurança;

 Facilidade de usar e visualização simplificada;

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

 Filtros de agendamento de relatórios;

 Arquivo com todas as instâncias de relatório agendados;

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

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

6. Quarentena

 Restauração remota, com configuração de localidade e deleção;

 Criação e exclusão para arquivos restaurados;

7. Usuários

 Administração baseada em regras;

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

 Relatório - Monitora e cria relatórios;

 Deverá ser possível customizar um tipo de usuário;

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

 Logs de utilização;

 Registrar as ações do usuário na console de gerenciamento;

 Detalhar cada ação do usuário;

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

8. Certificado de Segurança

 Deverá prover o acesso via HTTPS;

 Deverá permitir a importação de certificados digitais;

 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

 Deverá permitir a configuração do scan do antivírus do cliente como: Scan local, Scan Hibrido, Scan Central;

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

 Deverá suportar no mínimo os seguintes sistemas operacionais para estação de trabalho: Windows 11 32 e 64Bits, Windows 10 32 e 64Bits, Windows 7 32 e 64Bits.

 Deverá suportar no mínimo os seguintes sistemas operacionais para 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.

 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

 Deverá permitir ao administrador customizar a instalação;

 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 gerencia web;

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

 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;

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

 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;

 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 Proteção de antivírus dedicado para ambientes

virtuais;

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

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

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

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

12. Funções Gerais

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

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

13. Requisitos Mínimos suportados pelo Sistema.

 Plataformas de Virtualização: VMware vSphere and vCenter 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 Xen Hypervisor: 7.1 (with the 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), Red Hat Enterprise Virtualization 3.0 (incluindo KVM Hypervisor)

 Oracle VM 3.0

 Oracle VM VirtualBox 5.2, 5.1

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

 Nutanix Prism with AHV 20170830.115, 20170830.301, 20170830.395 e 20190916.294 (Community Edition)

 Sistemas Operacionais desktops (32 e 64 Bits): Windows 7, Windows 10, Windows 11;

 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

 Deverá fazer scan em tempo real automático;

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

 Escaneamento de comportamento heurístico;

 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;

 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;

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

 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;

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

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

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

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

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

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

 Deverá permitir escanear a quarentena após a atualização das atualizações de assinaturas;

15. Controle de Usuário

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

16. Controle do Dispositivo

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

 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;

 Deverá permitir regras de definição de bloqueio/desbloqueio;

 Deverá permitir regras de exclusão;

17. Atualização

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

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

 Permitir atualizações de assinatura de hora em hora;

 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.

18. Proteção para caixa de e-mail:

 Fornecer proteção para ambiente Exchange

 Oferecer tecnologia para proteção contra spam;

 Oferecer análise comportamental e proteção para zero-day;

 Oferecer proteção contra vírus e tentativas de phishing;

19. Criptografia

 Possibilidade de criptografia de disco através da console de gerenciamento seja em nuvem ou onpremise com módulo de Criptografia presente na mesma Console do Antivirus.

 Deverá utilizar quando necessários serviços de criptografia através agentes nativos da estação de trabalho baseada em Windows (BitLocker) ou Mac (FileVault);

 Deverá solicitar autenticação quando iniciado o sistema operacional do equipamento;

 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**

 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.

 Detectar e parar, bloquear e interromper malwares sem arquivos.

 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.

 Reparo e resposta automatizada a ameaças
 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.

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

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

 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 permite que os administradores de segurança ajustem a proteção para combater os riscos.

21. Machine Learning

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

 A ferramenta de Machine Learning deve se basear em características estáticas e dinâmicas, e se treinarem continuamente com bilhões de amostras de arquivos legítimos e maliciosas 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

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 fornecem um contexto claro das ameaças e ajudar a entender o comportamento delas.

23. Antiexploit Avançado

 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(returnoriented programming), etc.

24. Inspetor de processo

 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 (seqüestro 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.

25. Detecção e Resposta (XDR)

 A solução deve ir além do endpoint, oferecendo capacidades de detecção e resposta estendidas (XDR) para correlacionar eventos de segurança entre múltiplos endpoints e diferentes sistemas.

 Detecção e Resposta de Endpoint (EDR/XDR) com Capacidade de correlacionar eventos de segurança em toda a infraestrutura, fornecendo uma visão completa dos ataques em andamento.

 Análise de Causa Raiz com Ferramentas que permitem investigar e visualizar a cadeia de um ataque, desde o ponto inicial até o impacto final, com suporte para histórico.

 A solução deve ser capaz de mapear técnicas de ataque e táticas de defesa de acordo com o framework MITRE ATT&CK, facilitando a compreensão e a resposta a ameaças.

 Capacidade de implementar respostas automatizadas, como isolamento de hosts comprometidos, e permitir ações remotas, como execução de comandos e quarentena de arquivos.

26. Tipo de suporte

 Suporte remoto tipo 8x5: pelo período de 36 meses em horário comercial das 08:00 às 12:00 / 14:00 as18:00. Através do Fabricante que deverá disponibilizar;

 Uma central de Atendimento através de ligações telefônicas, web e e-mail, em língua portuguesa, para abertura de chamados técnicos. Este serviço deverá obrigatoriamente estar disponível 8x5;

27. Qualificação técnica

 Apresentação de, no mínimo, 01 (um) Atestados de Qualificação Técnica fornecido por pessoa jurídica de direito público ou privado, que comprove que a licitante forneceu ou está fornecendo, de maneira satisfatória e a contento, produtos ao objeto da presente licitação;

 Deverão constar obrigatoriamente no(s) referido(s) atestado(s) as seguintes informações:
razão social, CNPJ, endereço, contato, nome e cargo de quem o emitiu.

28. Declaração de Autorização do Fabricante ou Distribuidor Oficial.

 Declaração formal do fabricante ou de distribuidor autorizado, atestando que a empresa licitante está habilitada a comercializar e prestar os serviços de instalação e implantação.

5.7. Deverão ser fornecidas todas as chaves de ativação que se fizerem necessárias às instalações.

5.8. Todos os manuais e documentos técnicos necessários para as suas instalações e para o seu uso e operação, em idioma português brasileiro.

5.9. Possibilidade de renovação de todas as licenças contratadas.

5.10. O fabricante deverá fornecer suporte técnico via correio eletônico e/ou telefone, durante o horário comercial, em dia útil, com atendimento em idioma português brasileiro.

5.11. Serviços de manutenção, atualização de versões e suporte técnico (incluindo manutenções corretivas) deverão ser prestados pelo Fabricante.

5.12. Permitir a transferência da licença entre computadores, caso necessário.

5.13. Deverá ser fornecido o cartão de registro e/ou licença de uso, contendo todas as chaves, senhas, números de identificação, série e demais informações necessárias para a identificação, instalação, reinstalação e operação do produto.

5.14. Caso seja constatado fornecimento incompleto ou vício do produto, o fornecedor será convocado para substituir ou complementar o material no prazo máximo de 05(cinco) dias a contar da convocação pelo representante da instituição.

5.15. O licenciamento deve garantir o direito a atualizações de segurança e correções durante o ciclo de vida do produto.

5.16. A entrega do objeto do presente processo de Dispensa de Valor será de acordo com a necessidade da Contratante na Rua Duque de Caxias, 346, Bairro: São José, CEP:49015-320, Aracaju/SE Tel: (079)3226-2200 - Fax: (079)3214-0306.

5.17. O recebimento dos serviços/produtos será de acordo com o art. 140 da Lei 14.133/21 conforme abaixo;

a) provisoriamente, de forma sumária, pelo responsável por seu acompanhamento e fiscalização, com verificação posterior da conformidade dos produtos com as exigências do instrumento contratual;

b) definitivamente, por servidor ou comissão designada pela autoridade competente, mediante termo detalhado que comprove o atendimento das exigências contratuais.

c) O objeto do contrato poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

d) O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança da obra ou serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato, nos limites estabelecidos pela lei ou pelo contrato.

§ 3º Os prazos e os métodos para a realização dos recebimentos provisório e definitivo serão definidos em regulamento ou no contrato.

§ 4º Salvo disposição em contrário constante do edital ou de ato normativo, os ensaios, os testes e as demais provas para aferição da boa execução do objeto do contrato exigidos por normas técnicas oficiais correrão por conta do contratado.

5.18. A contratada sujeitar-se-á à fiscalização dos órgãos competentes, em todos os aspectos inerentes à execução do objeto contratado, não se eximindo da responsabilidade inclusive sobre a comprovação do atendimento às normas técnicas e às exigências da legislação que rege a matéria.

5.19. A CONTRATANTE reserva-se o direito de devolver, no todo ou em parte, as licenças fornecidas fora da especificação constante no Termo de Referência.

6.0- MODELO DE EXECUÇÃO DO OBJETO

6.1.A Contratante enviará Solicitação/Ordem de Fornecimento para pedido do objeto contratado de forma eletrônica (e-mail) à Contratada com prazo de 48 horas para confirmação de recebimento.

6.2.O *software* devem estar de acordo com os critérios estabelecidos neste Termo de Referência.

6.3. Para o *software* especificado, deverão ser fornecidas:

- Todas as licenças de uso em nome do Órgão adquirente;

- Todas as chaves de ativação que se fizerem necessárias às instalações;

- As mídias, se aplicável, contendo os respectivos códigos executáveis para a instalação; .

- Todos os *drivers* e/ou outros componentes de *software* necessários para as suas instalações;

- Todos os manuais e documentos técnicos necessários para as suas instalações e para o seu uso e operação;

6.4.Os serviços deverão ser disponibilizados pela CONTRATADA em dias úteis e em horário compreendido das 08:00 às 18:00 hs.

6.5.O endereço eletrônico utilizado para envio da Solicitação/Ordem de Fornecimento deverá constar na Proposta fornecida pela contratada.

Materiais a serem disponibilizados

6.3. Para a perfeita execução dos serviços, a Contratada deverá disponibilizar o software nas quantidades estimadas e qualidades estabelecidas no item 1.3, promovendo sua substituição quando necessário.

Especificação da garantia do serviço (art. 40, §1º, inciso III, da Lei nº 14.133, de 2021)

6.4. O prazo de garantia contratual mínima dos produtos é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor).

7.0- DO RECEBIMENTO E DO PAGAMENTO

Do recebimento

7.1. O recebimento do software contratado, deverá ser de acordo com as instruções contidas no item 6.0,

será efetuado pelo fiscal do Empenho/Ordem de Fornecimento/Contrato.

7.2. O Contratado fica obrigado 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 o fornecimento do produto, até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.5. A fiscalização não efetuará o ateste do fornecimento do produto até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório.

7.5.1. Os produtos poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

7.6. Os produtos serão recebidos definitivamente pelo fiscal designado pela Secretaria da Administração o senhor Leandro Félix Santos Guimarães, após a verificação da qualidade e quantidade do serviço e consequente aceitação.

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

7.8.Enviar a documentação pertinente ao setor competente para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

7.9.No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

7.10.Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança.

7.11. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

8.0. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

Formas e Critérios de Seleção do Fornecedor

8.1. O fornecedor será selecionado por meio da realização de procedimento de contratação direta, com fundamento na hipótese do art. 75, inciso II, da Lei nº 14.133/2021, pelo critério de menor preço por item.

8.2. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, caso exigidos e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

8.3. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

8.4. Para fins de contratação deverá o fornecedor comprovar os seguintes requisitos de habilitação:

8.4.1 HABILITAÇÃO PESSOA JURÍDICA:

8.4.1.1. No caso de Empresário Individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

8.4.1.2. No caso de Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual – CCMEI;

8.4.1.3. No caso de Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

8.4.1.4. No caso de Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

8.4.1.5. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

8.4.1.6. RG e CPF do empresário, ou sócios, conforme cada caso;

8.4.2 HABILITAÇÕES FISCAL, SOCIAL E TRABALHISTA

8.4.2.1. Pessoa Jurídica

8.4.2.1.1. Prova de inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ), se Pessoa Jurídica;

8.4.2.1.2. Certidão Conjunta Negativa de Tributos Federais e Dívida Ativa da União, abrangendo inclusive as contribuições sociais previstas nas alíneas “a” a “d” do § único do art. 11, da Lei Federal nº 8.212, de 24, de junho d3 1991, emitida pela Procuradoria Geral da Fazenda Nacional e a Secretaria da Receita Federal do Brasil;

8.4.2.1.3. Certificado de Regularidade de Situação – CRS, relativo ao FGTS;

8.4.2.1.4. Certidão Negativa de Débito do Estado ou Distrital do domicílio ou sede do fornecedor;

8.4.2.1.5. Certidão Negativa dos Tributos Municipais, do domicílio ou sede do fornecedor;

8.4.2.1.6. Certidão Negativa de Débitos Trabalhistas, fornecida pela Justiça do Trabalho;

8.4.4 QUALIFICAÇÃO ECONÔMICO-FINANCEIRA:

8.4.4.1. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei n.º 14.133,

de 2021, art. 69, caput, inciso I).

8.4.4.2. Declaração de que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

8.4.4.3. Declaração de que não existem fatos supervenientes impeditivos de sua participação e contratação com a Administração Pública.

9. CONDIÇÕES, FORMA E PRAZO DE PAGAMENTO

9.1. O Órgão CONTRATANTE, após o exato cumprimento das obrigações assumidas, efetuará o pagamento a CONTRATADA em prazo não superior a 30(trinta) dias consecutivos, contado a partir do recebimento e aceita da Nota Fiscal;

9.2. Os pagamentos serão realizados mediante apresentação de Nota Fiscal, contendo:

a. data da emissão;

b. estar endereçada ao Secretaria de Estado da Administração SEAD/SECLOG, situada a Rua Duque de Caxias, nº 346, Setor Almoxarifado, Aracaju – SE, sob CNPJ nº 34.849.652/0001-17;

c. valor unitário;

d. valor total:

e. a especificação do(s) material(ais);

f. apresentar a Nota Fiscal eletrônica em original.

9.3. A(s) Nota(s) fiscal(ais) que apresente(m) incorreções serão devolvidas à CONTRATADA para as devidas correções. Nesse caso, o prazo de que trata o item anterior começará a fluir a partir da data de apresentação da Nota Fiscal, sem incorreções;

9.4. O pagamento será creditado em conta corrente da CONTRATADA, por meio de ordem bancária a favor de qualquer instituição bancária indicada na Nota Fiscal, devendo, para isso, ficar explícito o nome do banco, agência, localidade e número da conta corrente em que deverá ser efetivado o crédito;

9.5. O pagamento será feito com recursos Tesouro - Recursos Ordinários;

9.6. O Fiscal do contrato somente atestará o recebimento do objeto e liberará a Nota(s) Fiscal(is) para pagamento quando cumpridas pela CONTRATADA, todas as condições pactuadas;

9.7. Cada pagamento somente será efetuado após a comprovação pelo CONTRATADO de que se encontra em dia com suas obrigações para com o sistema social, mediante apresentação das Certidões Negativas de Débito com o INSS, com FGTS e a Certidão Municipal.

10. DAS OBRIGAÇÕES DA CONTRATADA

10.1**.** Fornecer os produtos com estrita obediência à descrição constante no termo de referência e proposta apresentada e garantia legal e demais normas do Código de Defesa do Consumidor.

10.2. Não será admitida fornecer produtos em desacordo ao que consta neste termo de referência.

10.3. Iniciar o fornecimento com a emissão de Empenho/Ordem de Fornecimento/Contrato da Secretaria da Administração;

10.4. Não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada, exceto nas condições se previamente autorizadas pela Administração.

10.5. Substituir o (s) produto (s) que for entregue em desacordo com o homologado no processo.

10.6. Responsabilizar-se por danos materiais ou físicos causados por empregados ou prepostos diretamente à contratante ou a terceiros, decorrentes de sua culpa ou dolo.

10.7. Responsabilizar-se por vícios e danos no material a ser entregue, sendo obrigatória a substituição dos mesmos que estiverem em desacordo com a legislação vigente, inclusive sobre garantias e qualidade dos materiais entregues.

10.8. Indicação de preposto à CONTRATANTE para a execução do objeto contratado junto à Contratante.

10.9.A Contratada deverá fornecer durante instalação/implantação, e o período de vigência do Empeho/Ordem de Fornecimento/contrato, todas as manutenções do *software* licenciado, revisões dos manuais e da documentação, além de prestar suporte técnico em consonância com as orientações do fabricante da solução. Caso sejam detectados *bugs* ou falhas no *software*, a empresa deverá fornecer atualizações necessárias à correção do problema.

11. DAS OBRIGAÇÕES DA CONTRATANTE

11.1. Receber o objeto no prazo e condições estabelecidas.

11.2. Verificar minuciosamente, no prazo fixado, a conformidade do fornecimento provisoriamente com as especificações e da proposta, para fins de aceitação e recebimento definitivo.

11.3. Comunicar à Contratada, por escrito, sobre imperfeições, falhas ou irregularidades verificadas no objeto fornecido, para que seja substituído, reparado ou corrigido.

11.4. Acompanhar e fiscalizar o cumprimento das obrigações da Contratada, através de comissão/servidor especialmente designado.

11.5. Efetuar o pagamento à Contratada no valor correspondente ao fornecimento do objeto, no prazo e forma estabelecidos.

11.6. A SEAD não responderá por quaisquer compromissos assumidos pela Contratada com terceiros,

ainda que vinculados à execução do presente Termo de Contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da Contratada, de seus empregados, prepostos ou subordinados.

12. DAS SANÇÕES ADMINISTRATIVAS

12.1. Comete infração administrativa nos termos da Lei nº 14.133, de 2021 e da Lei nº 10.520, de 2002, a Contratada que:

12.1.1. Inexecutar total ou parcialmente qualquer das obrigações assumidas em decorrência da contratação;

12.1.2. Ensejar o retardamento da execução do objeto;

12.1.3. Fraudar na execução do contrato;

12.1.4. Comportar-se de modo inidôneo;

12.1.5. Cometer fraude fiscal; e

12.1.6. Não mantiver a proposta.

12.2. A Contratada que cometer qualquer das infrações discriminadas no subitem acima ficará sujeita, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

12.2.1. Advertência por faltas leves, assim entendidas aquelas que não acarretem prejuízos significativos para a Contratante;

12.2.2. Multa moratória de 0,30% (zero, trinta por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

12.2.3. Multa compensatória de 10% (dez por cento) sobre o valor total do contrato, no caso de inexecução total do objeto;

12.2.4. Em caso de inexecução parcial, a multa compensatória, no mesmo percentual do subitem acima, será aplicada de forma proporcional à obrigação inadimplida;

12.2.5. Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos;

12.2.6. Impedimento de licitar e contratar com o Estado;

12.2.7. Declaração de inidoneidade para licitar ou contratar com a Administração Pública, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida a reabilitação perante a própria autoridade que aplicou a penalidade, que será concedida sempre que a Contratada ressarcir a Contratante pelos prejuízos causados.

12.3. Também ficam sujeitas às penalidades do art. 160, da Lei nº 14.133, de 2021, as empresas ou profissionais que:

12.3.1.Tenham sofrido condenação definitiva por praticar, por meio dolosos, fraude fiscal no

recolhimento de quaisquer tributos;

12.3.2. Tenham praticado atos ilícitos visando a frustrar os objetivos da licitação; e

12.3.3. Demonstrem não possuir idoneidade para contratar com a Administração em virtude de atos ilícitos praticados.

12.3.4. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa à Contratada, observando-se o procedimento previsto na Lei nº 14.133, de 2021.

12.3.5. A autoridade competente, na aplicação das sanções, levará em consideração a gravidade da conduta do infrator, o caráter educativo da pena, bem como o dano causado à Administração, observado o princípio da proporcionalidade.

13. DA RESCISÃO

13.1. A inexecução total ou parcial do ajuste enseja a sua rescisão, sem prejuízo das penalidades previstas neste Termo de Referência.

13.2. O ajuste será rescindido pelo CONTRATANTE, se verificada a ocorrência de quaisquer das hipóteses elencadas no artigo 137 da Lei nº 14.133/21.

13.3. A rescisão será formalmente motivada nos autos do processo, assegurados o contraditório e a ampla defesa.

13.4. O ajuste será rescindido caso o CONTRATANTE verifique que a qualidade dos objetos entregues pela CONTRATADA estejam fora das especificações necessárias.

14. DO FORO

14.1 Fica eleito o Foro de Aracaju/SE, para dirimir questões oriundas desta contratação.

Aracaju, 30 de outubro de 2025

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: X8RM-N4VN-G2DU-XLQA

O(s) nome(s) indicado(s) para assinatura, bem como seu(s) status em 26/11/2025 é(são) :

Legenda: Aprovada Indeterminada Pendente

- Bruno Vasconcellos de Lucena ***76727*** GERÊNCIA DE COMPRAS E CONTRATAÇÕES - SEAD Secretaria de Estado da Administração 30/10/2025 07:23:18 (Docflow)
- JOSE ANTONIO GONCALVES PASSOS ***03979*** GERÊNCIA DE COMPRAS E CONTRATAÇÕES - SEAD Secretaria de Estado da Administração 30/10/2025 08:35:26 (Docflow)
- LEANDRO FELIX SANTOS GUIMARAES ***23883*** DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO - SEAD Secretaria de Estado da Administração 29/10/2025 11:34:01 (Docflow)
- OSMAN DOS SANTOS ***07717*** ASSESSORIA TÉCNICA DO DEPARTAMENTO DE ADMINISTRAÇÃO E FINANÇAS - SEAD Secretaria de Estado da Administração 30/10/2025 08:33:26 (Docflow)