CÂMARA MUNICIPAL DE GOIÂNIA | ESTADO DE GOIÁS PODER LEGISLATIVO

TERMO DE REFERÊNCIA

(art. 6º, XXIII, da Lei nº 14.1333/2021)

CONTRATAÇÃO DE SERVIÇOS - PREGÃO / CONCORRÊNCIA

Processo Administrativo 00000.004492.2024-98

1. DO OBJETO E DO PRAZO DE VIGÊNCIA (Art. 6º, XXIII, "a" da Lei nº 14.133/2021)

1.1. Contratação de serviços de solução de segurança de computadores contra ataques cibernéticos englobando implantação, suporte e garantia, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

LOTE				
ITEM	**ESPECIFICAÇÃO**	**CATSER**	**UNIDADE DE MEDIDA**	**QUANTIDADE**
1	Contratação de solução de segurança de estações de trabalho e servidores contra ataques cibernéticos (incluindo implantação, suporte e garantia)	27502	licença	450 licenças para computadores por 3 anos

1.2. O objeto desta contratação não se enquadra como sendo serviço especial, sendo caracterizado como comum, visto que possui padrões de desempenho e qualidade que podem ser objetivamente definidos, por meio de especificações usuais de mercado, compatível com a finalidade a que se destina, sem prejuízo da eficiência, qualidade e durabilidade, nos termos do art. 6º, XIII, da Lei nº 14.133/2021.

1.3. O parcelamento por lotes não se aplica ao presente objeto, sendo o critério de julgamento da contratação o de **menor preço por item,** mostrando-se tecnicamente e economicamente viável, tendo em vista o objetivo de propiciar a ampla participação de licitantes na disputa, aumentando a competitividade e a viabilização de melhores propostas

1.4. O prazo de vigência da contratação é de 3 (três) anos contados da assinatura do contrato, prorrogável por até 10 anos, na forma dos artigos 106 e 107 da Lei nº 14.133/2021, considerando tratar-se de serviço contínuo de bem, decorrente de necessidade permanente ou prolongada desta Administração, conforme art. 6º, inciso XV da Lei nº 14.133/2021.

1.5. O custo estimado total da contratação consta em documento anexo (Anexo I).

1.6. O contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO (Art. 6º, XXIII, “b” da Lei nº 14.133/2021)

2.1. A fundamentação da contratação e de seus quantitativos encontra-se pormenorizada no Estudo Técnico Preliminar.

2.2. O objeto da contratação está previsto no Plano de Contratações Anual 2025: DFD 12/2024 - DRTIN.

3. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO, CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO SERVIÇO (Art. 6º, XXIII, “c”, Lei nº 14.133/2021 e art. 3º, Lei nº 12.305/2010)

3.1 Solução de proteção avançada contra ataques cibernéticos para estações

de trabalho.

3.1.1 Características gerais:

3.1.1.1 Do módulo de proteção de endpoint;

3.1.1.2 A solução proposta deverá proteger os sistemas operacionais abaixo:

3.1.1.2.1 Windows 10

3.1.1.2.2 Windows 11

3.1.1.3 Servidores

3.1.1.3.1 Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022 e posteriores

3.1.1.3.2 Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022 e posteriores

3.1.1.4 Sistemas operacionais Linux:

3.1.1.4.1 Debian GNU/Linux 11.0 e posterior

3.1.1.4.2 Debian GNU/Linux 12.0 e posterior

3.1.1.4.3 Red Hat Enterprise Linux 7.2 e posterior

3.1.1.4.4 CentOS 7.2 e posterior.

3.1.1.4.5 CentOS Stream 8.

3.1.1.4.6 CentOS Stream 9.

3.1.1.4.7 Oracle Linux 9.0 e posterior.

3.1.1.4.8 SUSE Linux Enterprise Server 12.5 ou posterior.

3.1.1.4.9 SUSE Linux Enterprise Server 15 ou posterior.

3.1.1.4.10 Ubuntu 20.04 LTS e Posterior

3.1.1.5 A solução proposta deverá suportar as seguintes plataformas virtuais:

3.1.1.5.1 VMware Workstation 17.0.2 Pro

3.1.1.5.2 VMware ESXi 6.7 e posteriores

3.1.1.5.3 Microsoft Hyper-V Server 2019

3.1.1.5.4 Citrix Virtual Apps e Desktop 7 2308

3.1.1.5.5 Citrix Provisioning 2308

3.1.1.5.6 Citrix Hypervisor 8.2 Update 1

3.1.1.6 As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

3.1.2 Do módulo de gerenciamento avançado

3.1.2.1 A solução proposta deve suportar arquitetura cloud-native ou on-premisse;

3.1.2.2 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;

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

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

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

3.1.2.6 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.

3.1.2.7 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.

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

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

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

3.1.2.11 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:

3.1.2.11.1 Status do dispositivo

3.1.2.11.2 Tag

3.1.2.11.3 Diretório ativo

3.1.2.12 A solução proposta deve suportar os seguintes canais de entrega de notificação:

3.1.2.12.1 E-mail

3.1.2.12.2 Registro de sistema

3.1.2.12.3 SMS

3.1.2.13 A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:

3.1.2.13.1 Atributos de rede

3.1.2.13.2 Nome

3.1.2.13.3 Domínio e/ou Sufixo de Domínio

3.1.2.13.4 Endereço de IP

3.1.2.13.5 Endereço IP para servidor de gerenciamento

3.1.2.13.6 Localização no Active Directory

3.1.2.13.7 Unidade organizacional

3.1.2.13.8 Grupo

3.1.2.13.9 Sistema operacional

3.1.2.14 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.

3.1.2.15 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.

3.1.2.16 As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

3.1.2.16.1 Dispositivos Desktop/Servidores

3.1.2.16.2 Dispositivos móveis

3.1.2.16.3 Dispositivos de rede

3.1.2.17 A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

3.1.2.17.1 Nome da Aplicação

3.1.2.17.2 Caminho do aplicativo

3.1.2.17.3 Metadados do aplicativo

3.1.2.17.4 Aplicativo Certificado digital

3.1.2.17.5 Categorias de aplicativos predefinidas pelo fornecedor

3.1.2.17.6 SHA256 e MD5

3.1.2.18 A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

3.1.2.18.1 Bluetooth

3.1.2.18.2 Dispositivos móveis

3.1.2.18.3 Modems externos

3.1.2.18.4 CD/DVD

3.1.2.18.5 Câmeras e scanners

3.1.2.18.6 MTPs

3.1.2.18.7 E a transferência de dados para dispositivos móveis

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

3.1.2.20 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:

3.1.2.20.1 Estruturas de domínios e grupos de trabalho do Windows

3.1.2.20.2 Estruturas de grupos do Active Directory

3.1.2.21 Verificação de unidade removível na conexão com o sistema;

3.1.2.22 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.

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

3.1.2.24 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.

3.1.2.25 A solução proposta deve suportar Windows Failover Cluster.

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

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

3.1.2.28 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.

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

3.1.2.30 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.

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

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

3.1.2.33 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.

3.1.2.34 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.

3.1.2.35 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).

3.1.2.36 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.

3.1.2.37 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.

3.1.2.38 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.

3.1.2.39 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.

3.1.2.40 A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.

3.1.2.41 A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.

3.1.2.42 A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.

3.1.2.43 A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.

3.1.2.44 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.

3.1.2.45 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. .

3.1.2.46 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.

3.1.2.47 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.

3.1.2.48 A solução proposta deve permitir ao administrador personalizar relatórios.

3.1.2.49 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.

3.1.2.50 A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.

3.1.2.51 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.

3.1.2.52 A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.

3.1.2.53 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;

3.1.2.54 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.

3.1.2.55 A solução proposta deve suportar integração com solução APT.

3.1.2.56 A solução proposta deve suportar a integração com o serviço Managed Detection and Response.

3.1.2.57 A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.

3.1.2.58 A solução proposta deve fornecer um local central para

armazenamento de chaves de criptografia e múltiplas opções de recuperação.

3.1.2.59 O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário.

3.1.2.60 A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.

3.1.2.61 A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.

3.1.2.62 A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:

3.1.2.62.1 Uso do Trusted Platform Module e configurações de senha.

3.1.2.62.2 Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.

3.1.2.63 Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).

3.1.2.64 A solução proposta deve suportar criptografia em Microsoft Surface Tablets.

3.1.2.65 A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:

3.1.2.65.1 Instalação remota de software de terceiros

3.1.2.65.2 Relatórios sobre software e hardware existentes

3.1.2.65.3 Monitoramento para instalação de software não autorizado

3.1.2.65.4 Remoção de software não autorizado

3.1.2.66 A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de

terceiros instalados.

3.1.2.67 A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.

3.1.2.68 A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.

3.1.2.69 A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.

3.1.2.70 A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.

3.1.2.71 O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.

3.1.2.72 A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança

3.1.2.73 A solução proposta deve permitir ao administrador aprovar atualizações.

3.1.2.74 A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.

3.1.2.75 A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.

3.1.2.76 A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.

3.1.2.77 A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.

3.1.2.78 A solução proposta deverá proporcionar a possibilidade de

corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.

3.1.2.79 A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).

3.1.2.80 A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.

3.1.2.81 A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.

3.1.2.82 A solução proposta deve incluir campos dedicados que contenham informações sobre 'Exploração encontrada para a vulnerabilidade'.

3.1.2.83 A solução proposta deve incluir campos dedicados que contenham informações sobre "Ameaça encontrada para a vulnerabilidade".

3.1.2.84 A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.

3.1.2.85 A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.

3.1.2.86 A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.

3.1.2.87 A solução proposta deve apoiar a implantação do sistema operacional.

3.1.2.88 A solução proposta deve suportar Wake-on LAN e UEFI.

3.1.2.89 A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.

3.1.2.90 A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as

atualizações.

3.1.2.91 A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.

3.1.2.92 A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.

3.1.2.93 A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.

3.1.2.94 A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.

3.1.2.95 A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.

3.1.2.96 A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.

3.1.2.97 A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.

3.1.2.98 A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:

> **3.1.2.98.1** Inicie a instalação ao reiniciar ou desligar o computador.
>
> **3.1.2.98.2** Instale o gerador necessário todos os pré-requisitos do sistema.
>
> **3.1.2.98.3** Permitir a instalação de novas versões de aplicativos durante as atualizações.
>
> **3.1.2.98.4** Baixe atualizações para o dispositivo sem instalá-las.

3.1.2.99 A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.

3.1.2.10 A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.

3.1.2.101 O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:

3.1.2.101.1 CEF;

3.1.2.101.2 LEEF;

3.1.2.102 A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.

3.1.2.103 O relatório da solução proposta deve conter informações CVE.

3.1.2.104 A solução proposta deve suportar instalação de aplicações e software de terceiros;

3.1.3 Do módulo de gerenciamento simplificado

3.1.3.1 A solução proposta deve suportar arquitetura cloud;

3.1.3.2 A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

3.1.3.3 O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

3.1.3.4 A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.

3.1.3.5 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.

3.1.3.6 A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.

3.1.3.7 A solução proposta deve incluir informações do endpoint:

3.1.3.7.1 IP público de internet;

3.1.3.7.2 IP interno do dispositivo;

3.1.3.7.3 Versão do agente de proteção;

3.1.3.7.4 Ultima comunicação com a console, contendo data e hora;

3.1.3.7.5 Informações do sistema operacional;

3.1.3.8 A solução proposta deve incluir treinamento em segurança cibernética.

3.1.4 Requisitos gerais

3.1.4.1 A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:

3.1.4.1.1 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.

3.1.4.2 A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.

3.1.4.3 A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).

3.1.4.4 A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.

3.1.4.5 A solução proposta deve suportar o subsistema Linux no Windows.

3.1.4.6 A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

3.1.4.6.1 Proteção contra ameaças sem arquivos (Fileless);

3.1.4.6.2 Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

3.1.4.7 A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;

3.1.4.8 A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.

3.1.4.9 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.

3.1.4.10 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.

3.1.4.11 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.

3.1.4.12 A solução proposta deve fornecer análise comportamental baseada em machine learning.

3.1.4.13 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.

3.1.4.14 A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:

3.1.4.14.1 Controles de aplicativos,

3.1.4.14.2 Controle web e dispositivos

3.1.4.14.3 HIPS e Firewall

3.1.4.14.4 Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;

3.1.4.14.5 Gerenciamento de criptografia de arquivos e discos;

3.1.4.14.6 Controle adaptativo para detecção de anomalias;

3.1.4.15 A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.

3.1.4.16 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.

3.1.4.17 A solução proposta deve ter bancos de dados de reputação locais e globais.

3.1.4.18 A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.

3.1.4.19 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.

3.1.4.20 A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.

3.1.4.21 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.

3.1.4.22 A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:

3.1.4.22.1 Modo silencioso;

3.1.4.22.2 Discos rígidos e dispositivos removíveis;

3.1.4.22.3 De todos as contas de usuários do dispositivo.

3.1.4.23 A funcionalidade de limpeza remota de dados da solução

proposta deve suportar os seguintes modos:

3.1.4.23.1 Exclusão imediata de dados;

3.1.4.23.2 Exclusão de dados adiada.

3.1.4.24 A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:

3.1.4.24.1 Excluir usando os recursos do sistema operacional - os arquivos são excluídos;

3.1.4.24.2 Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.

3.1.4.25 A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.

3.1.4.26 A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.

3.1.4.27 A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.

3.1.4.28 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.

3.1.4.29 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.

3.1.4.30 A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.

3.1.4.31 A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.

3.1.4.32 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;

3.1.4.33 A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;

3.1.4.34 A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.

3.1.4.35 A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.

3.1.4.36 A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.

3.1.4.37 A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.

3.1.4.38 A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.

3.1.4.39 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.

3.1.4.40 A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.

3.1.4.41 A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.

3.1.4.42 A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.

3.1.4.43 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.

3.1.4.44 A solução proposta deve ter categoria de detecção para bloquear banners de sites.

3.1.4.45 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;

3.1.4.46 A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.

3.1.4.47 A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.

3.1.4.48 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.

3.1.4.49 A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

3.1.4.50 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.

3.1.4.51 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.

3.1.4.52 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.

3.1.4.53 O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.

3.1.4.54 O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.

3.1.4.55 A solução proposta deve suportar o controle de scripts

executados em PowerShell.

3.1.4.56 A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.

3.1.4.57 A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.

3.1.4.58 A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.

3.1.4.59 A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.

3.1.4.60 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.

3.1.4.61 A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.

3.1.4.62 A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:

3.1.4.62.1 Filtro de anexos.

3.1.4.62.2 Verificação de mensagens de email ao receber, ler e enviar.

3.1.4.63 A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.

3.1.4.64 A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;

3.1.4.65 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.);

3.1.4.66 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.

3.1.4.67 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.

3.1.4.68 A solução proposta deve incluir suporte ao protocolo IPv6.

3.1.4.69 A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.

3.1.4.70 A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

3.1.4.71 Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.

3.1.4.72 Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

3.1.4.73 A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.

3.1.4.74 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.

3.1.4.75 A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.

3.1.4.76 A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.

3.1.4.77 A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.

3.1.4.78 A solução proposta deve fornecer controles de aplicativos e

dispositivos para estações de trabalho Windows.

3.1.4.79 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.

3.1.4.80 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.

3.1.4.81 A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.

3.1.4.82 A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.

3.1.4.83 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.

3.1.4.84 A solução proposta deve suportar endereços IPv6.

3.1.4.85 A solução proposta deve suportar verificação em duas etapas (autenticação).

3.1.4.86 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.

3.1.4.87 A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.

3.1.4.88 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.

3.1.4.89 A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.

3.1.4.90 A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.

3.1.4.91 A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.

3.1.4.92 A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.

3.1.4.93 A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.

3.1.4.94 A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.

3.1.4.95 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.

3.1.4.96 A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.

3.1.4.97 A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.

3.1.4.98 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.

3.1.4.99 A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.

3.1.4.100 A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.

3.1.4.101 A solução proposta deve ter a capacidade de excluir atualizações baixadas.

3.1.4.102 A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.

3.1.4.103 A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.

3.1.4.104 A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.

3.1.4.105 A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.

3.1.4.106 Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.

3.1.4.107 A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.

3.1.4.108 A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.

3.1.4.109 A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.

3.1.4.110 A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:

3.1.4.110.1 Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.

3.1.4.110.2 Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

3.1.4.111 A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.

3.1.4.112 A solução proposta deve gerar relatoiros de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

3.1.5 Do módulo de EDR

3.1.5.1 Deve apresentar um gráfico de propagação de ameaças com

os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

3.1.5.2 Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.

3.1.5.3 A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;

3.1.5.4 Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;

3.1.5.5 Deve apresentar informações detalhadas contendo:

3.1.5.5.1 Usuário que executou a ação;

3.1.5.5.2 Informações acesso privilegiado;

3.1.5.6 A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.

3.1.5.7 A solução proposta deve suportar integração com serviço de reputação em nuvem.

3.1.5.8 A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)

3.1.5.9 O agente EDR deve ter integração com o aplicativo de proteção de endpoint(agente único).

3.1.5.10 Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;

3.1.5.11 A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.

3.1.5.12 A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema

sobre a detecção.

3.1.5.13 A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.

3.1.5.14 A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.

3.1.5.15 A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.

3.1.5.16 A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.

3.1.5.17 A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.

3.1.5.18 A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.

3.1.5.19 A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.

3.1.5.20 A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:

3.1.5.21 Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).

3.1.5.22 Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.

3.1.5.23 Informações gerais sobre a detecção, incluindo modo de detecção.

3.1.5.24 Alterações no registro associadas à detecção.

3.1.5.25 Histórico da presença de arquivos no dispositivo.

3.1.5.26 Ações de resposta executadas pela aplicação.

3.1.5.27 O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.

3.1.5.28 A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:

3.1.5.29 Processo

3.1.5.30 Conexões de rede

3.1.5.31 Alterações no registro

3.1.5.32 Detalhes do download de objeto

3.1.5.33 A solução proposta deve fornecer orientação de resposta (resposta guiada).

3.1.5.34 A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:

3.1.5.35 Impedir a execução de objetos

3.1.5.36 Isolamento de host

3.1.5.37 Excluir objeto do host ou grupo de hosts

3.1.5.38 Colocar um objeto em quarentena

3.1.5.39 Execute a verificação do sistema

3.1.5.40 Execução remota de programa/processo/comando

3.2. SERVIÇO DE SUPORTE

3.2.2. Todo o Serviço de Suporte deverá ser prestado por profissional certificado pelo Fabricante da Solução, em nível compatível com a prestação do serviço. Deverá ser apresentado comprovação da certificação dos profissionais responsáveis no ato da assinatura do contrato.

3.2.3. Deverá disponibilizar um serviço preventivo de verificação e atualização de versões ou correções (patches) que se fizerem necessários, específicos para a solução ofertada;

3.2.4. deverá prestar suporte a todos os componentes de software fornecidos que forem necessários para a implementação e utilização da solução.

3.2.5. A contratada deverá notificar a contratante sobre atualizações de segurança, patches e correções assim que estiverem disponíveis, caso autorizado aplicar as atualizações de segurança e evolutiva dos produtos;

3.2.6. A contratada deverá prover Serviço Especializado de Suportes corretivo para ajustes, correções e configurações da solução a ser fornecida. Neste serviço deverá estar incluso todo tipo de suporte para funcionamento da solução;

3.2.7. A contratada deverá:

3.2.7.1. Implementar um sistema de abertura de chamados, para registrar, rastrear e priorizar incidentes e requisições de suporte;

3.2.7.2. Atribuir números de caso exclusivos para facilitar a comunicação e o acompanhamento;

3.2.7.3. Garantir disponibilidade 24/7 para responder a incidentes críticos.

3.2.8. Suporte Técnico

3.2.8.1. Deverá ser oferecido suporte técnico da Contratada, com a possibilidade de abertura de chamados, das 7h00 às 20h00, em dias úteis, para a resolução de problemas. É importante destacar que os serviços de suporte técnico devem contemplar as manutenções corretivas e evolutivas para a solução contratada e não podem acarretar custos adicionais ao CONTRATANTE, além do que foi previamente acordado.

3.2.8.2. A empresa contratada deve encaminhar o chamado para o suporte do fabricante sempre que necessário, seja devido à criticidade, impacto ou urgência do problema, ou caso seja necessário o envolvimento direto do fabricante no processo de correção. É imprescindível que seja fornecido acesso ao site do fabricante para acompanhamento dos chamados, acesso à base de conhecimento e aos fóruns relacionados à solução.

3.2.8.3. Os serviços de suporte técnico abrangem:

3.2.8.3.1. Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução.

3.2.8.3.2. Elaboração de relatórios, estudos e diagnósticos sobre o ambiente.

3.2.8.3.3. Transferência de conhecimento aos técnicos da Contratante referente aos problemas vivenciados e às soluções aplicadas, na forma a ser determinada pelas partes.

3.2.8.3.4. Realização de instalação, atualização e configuração de novas versões dos produtos após a disponibilização das atualizações tecnológicas pelo fabricante.

3.2.8.4. O suporte técnico deve contemplar o atendimento para sanar dúvidas relacionadas com instalação, configuração e uso do software ou para correção de problemas, em especial na configuração de parâmetros, falhas, erros, defeitos ou vícios identificados no funcionamento da solução.

3.2.8.5. O suporte técnico deve contemplar, quando for o caso, atendimento a eventual problema de instalação ou configuração de softwares básicos e de infraestrutura de TIC (sistemas operacionais, servidores de banco de dados, servidores de aplicação, etc.) necessários ao funcionamento da solução.

3.2.8.6. Deve contemplar também a atualização de versões do software aplicativo, as quais incorporam correções de erros ou problemas registrados e melhorias implementadas pela fabricante, num empacotamento estável do sistema. O serviço de atualização de versão tem por finalidade assegurar a devida atualização da solução durante o período de vigência da garantia. Refere-se ao fornecimento de novas versões e releases da solução lançados no período. A cada nova liberação de versão e release, serão disponibilizados em formato digital manuais e demais documentos técnicos, bem como nota informativa das funcionalidades implementadas. Em caso de lançamento de patch de correção, a CONTRATADA deverá comunicar o fato ao CONTRATANTE e indicar a forma de obtenção e os defeitos que serão corrigidos pelo patch. Em ambos os casos, a comunicação deve ser feita no prazo de até 30 dias, a contar do lançamento de nova versão ou solução de correção.

3.2.8.7. A CONTRATADA será responsável pelos serviços de implantação das novas versões e releases dos produtos por ela fornecidos como partes do objeto, bem como pela aplicação dos patches de correção e pacotes de serviço (service packs) relativos a esses produtos. Para a implantação das novas versões/releases, bem como para a aplicação dos patches, deverá ser aberto chamado de suporte técnico com nível de severidade adequado e a prestação dos serviços deve ser agendada com os responsáveis pela solução na CONTRATANTE;

3.2.8.8. Deverá ser prestado suporte técnico remoto com atendimento mediante registro de chamados em página de website, em sistema fornecido pela CONTRATADA e/ou pelo fabricante; e também através de contato telefônico. Esse serviço destina-se a esclarecimento de dúvidas e resolução de problemas relacionados à configuração e uso dos componentes da solução CONTRATADA;

3.2.8.9. As peças substitutas deverão apresentar padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento e devem integrar a garantia da solução;

3.2.8.10. A CONTRATADA auxiliará o CONTRATANTE na reinstalação das ferramentas, caso seja necessário, ao longo do tempo de garantia da ferramenta;

3.2.8.11. A CONTRATADA deverá disponibilizar os seguintes canais de acesso ao suporte técnico:

3.2.8.11.1. Portal Web;

3.2.8.11.2. E-mail;

3.2.8.11.3. Central 0800; e/ou

3.2.8.11.4. Telefone fixo.

3.2.8.12. O atendimento deve ser contínuo, 24 horas por dia, 7 dias por semana, durante todo o ano, incluindo feriados, em língua portuguesa. O início do atendimento e o prazo de solução devem ser determinados de acordo com o nível de severidade exigido para o caso.

3.3. SERVIÇO DE IMPLANTAÇÃO

3.3.1. Nesta etapa, compreende-se a instalação e configuração da solução contratada, contados a partir da emissão da Ordem de Serviço (OS);

3.3.2. O serviço de implantação abrange integralmente as fases essenciais para a integração, instalação e configuração da solução contratada, alinhando-se precisamente com as especificações técnicas e requisitos predefinidos. Esta abordagem abarca desde o planejamento inicial até a conclusão efetiva, assegurando uma transição suave dos processos existentes para a nova solução;

3.3.3. O Plano de Implantação assume a forma de um documento fundamental que consolida a estratégia para instalação, configuração e entrega da solução contratada. Sua importância reside em orientar e alinhar as atividades, garantindo eficiência e uma implementação adequada da solução conforme os requisitos estabelecidos;

3.3.4. O documento deverá conter no mínimo os requisitos de ambiente tecnológicos necessários para a instalação das licenças, cronograma e detalhamento das atividades a serem realizadas, topologia do ambiente pós instalação da solução, matriz de responsabilidade, plano de comunicação;

3.3.5. Durante esta etapa, a equipe da Contratada deverá estar presente nos horários de instalação definidos pelo Contratante. As atividades de instalação e configuração poderão ser realizadas, conforme necessário, em horário comercial, período noturno ou final de semana;

3.3.6. O Contratante disponibilizará a infraestrutura de hardware e software necessária e já existente em seu ambiente, incluindo o ambiente virtualizado, sistema operacional, banco de dados, e outros, para a instalação e configuração da solução durante esta etapa.

3.4. SERVIÇO DE TREINAMENTO

3.4.1. Repasse de conhecimento, na forma de treinamento para técnicos, de forma virtual, para 1 (uma) turma, com carga horária mínima de 20 (vinte) horas, abrangendo todos os softwares integrantes da suíte de solução de segurança;

3.4.2. O conteúdo programático abordará tanto aspectos teóricos quanto práticos, contemplando de maneira abrangente todos os módulos relevantes da solução de segurança;

3.4.3. O treinamento pode ser segmentado de acordo com o produto a ser instalado no ambiente tecnológico, contemplando, no mínimo, os

seguintes módulos:

3.4.3.1. Instalação do módulo de gerenciamento central;

3.4.3.2. Instalação do software de Endpoint Protection em estações de trabalho e servidores;

3.4.3.3. Descrição e configuração de todas as funcionalidades contratadas da solução;

3.4.3.4. Melhores práticas utilizadas no mercado para otimização dos softwares e suas funcionalidades.

3.4.4. A carga horária mínima estabelecida será de 20 (vinte) horas, divididas em expedientes de 4 horas por dia, no horário comercial. A contratada é responsável por fornecer apostilas em formato digital que contemplem o conteúdo referente ao produto, oferecendo suporte ao aprendizado prático e teórico dos participantes;

3.4.5. Este treinamento visa capacitar adequadamente os usuários finais, garantindo que compreendam e aproveitem plenamente as funcionalidades da solução de segurança. O enfoque prático e teórico, aliado às melhores práticas do mercado, promove uma formação abrangente e eficaz.

3.5. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

3.5.1. Requisitos de Capacitação

3.5.1.1. A empresa CONTRATADA deverá realizar o repasse de conhecimento aos funcionários da CONTRATANTE que atuarão, diretamente, com a solução de segurança adquirida, contemplando instalação, parametrização, monitoramento, melhores práticas e atuação de incidentes com carga horária mínima de 20 (vinte) horas ministrado por profissional certificado pelo fabricante.

3.5.1.2. O treinamento será demando à CONTRATADA pela CONTRATANTE após a efetiva implementação e estruturação da solução de segurança em seu parque tecnológico, quando acordarão cronograma para realização do treinamento.

3.5.1.3. O treinamento deverá ser realizado na modalidade remota a participantes da equipe técnica a serem definidos pela CONTRATANTE.

3.5.1.4. Os horários do curso deverão seguir a conveniência do CONTRATANTE, podendo sua realização ocorrer apenas em um dos períodos do dia (manhã ou tarde).

3.5.1.5. Deverá ser fornecido material didático completo e com conteúdo oficial do fabricante em língua portuguesa. Caso seja utilizado material elaborado exclusivamente pelo fabricante e fique demonstrado que este não é oferecido em língua portuguesa, será aceito o fornecimento em língua inglesa.

3.5.1.6. O treinamento deve conter parte teórica e prática, incluindo tópicos sobre a instalação, uso, configuração, resolução de problemas da solução, análise de relatórios, respostas a incidentes e outros.

3.5.1.7. As datas do treinamento devem ser previamente combinadas com o CONTRATANTE.

3.5.1.8. Todos os custos relativos à realização do treinamento são de exclusiva responsabilidade da CONTRATADA.

3.5.1.9. O curso deve ser gravado em arquivos de vídeo para posterior consulta. A CONTRATADA será responsável pela gravação e disponibilização para download pelo período de 1 (um) mês.

3.5.3. Requisitos de manutenção e garantia

3.5.3.1. A empresa contratada é responsável por fornecer suporte técnico e garantia de atualização da solução pelo período de 36 meses, a contar da data de emissão do Termo de Recebimento. É importante ressaltar que essa garantia não se limita ao término da vigência contratual.

3.5.3.2. A garantia deve incluir obrigatoriamente:

3.5.3.2.1. Atualização das versões dos softwares fornecidos, caso sejam disponibilizadas novas versões.

3.5.3.2.2. Atualização dos softwares fornecidos caso haja lançamento de novos softwares que substituam os fornecidos ou se ficar evidente a descontinuidade dos softwares fornecidos, mesmo que não se trate de substituição direta.

3.5.3.2.3. Correções dos softwares fornecidos, incluindo a aplicação de patches para corrigir eventuais falhas (bugs) de software que possam prejudicar o ambiente de produção ou

vulnerabilidades que comprometam a segurança da solução.

3.5.3.3. A garantia deverá ser prestada durante todo o período de contrato e aditivos relacionados à atualização das licenças e proteção.

3.5.3.4. Durante o período de garantia, a empresa contratada compromete-se a substituir, em até 15 dias úteis, os equipamentos que apresentarem, em um período de 60 dias, duas ocorrências de defeitos por inoperância do produto ou 3 ocorrências de deficiência operacional do produto.

3.5.3.5. As ferramentas e equipamentos necessários à manutenção serão de responsabilidade da contratada.

4. REQUISITOS DA CONTRATAÇÃO (Art. 6º, XXIII, alínea "d", Lei nº 14.133/2021)

4.1. Possíveis Impactos Ambientais (Sustentabilidade)

Os elementos que caracterizem possíveis impactos ambientais, se houver, encontram-se pormenorizados em tópico específico do Estudo Técnico Preliminar.

4.2. Subcontratação (artigos 122 e 74, § 4º, Lei nº 14.133/2021)

Não é admitida a subcontratação do objeto contratual.

4.3. Garantia da contratação (art. 96, Lei nº 14.133/2021)

a) Para contratos com valores a partir de R$ 100.000,00 (cem mil reais), será exigida a garantia da contratação de que tratam os artigos 96 e seguintes da Lei nº 14.133/2021, no percentual de 5% do valor contratual, conforme regras previstas no instrumento.

a.1) A garantia nas modalidades caução e fiança bancária deverá ser prestada em até 30 dias após a data de assinatura do contrato ou da emissão da nota de empenho.

a.2) No caso de seguro-garantia sua apresentação deverá ocorrer no prazo mínimo de 1 mês, contado da homologação da licitação e anterior a data de assinatura do contrato. Nesta hipótese, o prazo de

vigência da apólice será do prazo estabelecido no contrato principal acrescido de mais 6 meses e deverá acompanhar as modificações referentes à vigência deste mediante a emissão do respectivo endosso pela seguradora, nos termos do art. 97, I e II, da Lei nº 14.133/2021.

b) O contrato oferece maior detalhamento das regras que serão aplicadas em relação à garantia da contratação.

5. MODELO DE EXECUÇÃO DO OBJETO (Art. 6º, XXIII, alínea "e", Lei nº 14.133/2021)

5.1. Condições de Execução

5.1.1. A execução dos serviços seguirá a seguinte dinâmica:

CRONOGRAMA FÍSICO-FINANCEIRO DE EXECUÇÃO DOS SERVIÇOS			
etapas/medição	**parcela dos serviços**	**prazo de entrega**	**pagamento**
1ª	Procedimento de configuração da central de gerenciamento e instalação das licenças nas máquinas alvo	Início em 15 dias da emissão da O.S. e término em até 45 dias	não aplicavel
2ª	Repasse do conhecimento / Treinamento	10 dias úteis após 1ª etapa	não aplicável
3ª	Emissão de documento oficializando recebimento definitivo	até 10 dias úteis após 2ª etapa	pós recebimento definitivo, o processo de pagamento do valor total irá iniciar

5.1.2. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas, mediante comprovação, com pelo menos 10 dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

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

a) O prazo de garantia contratual dos serviços, complementar à garantia legal, será de, no mínimo, 36 (trinta e seis) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

b) O Contratado deverá realizar a transição contratual com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução dos serviços.

6. MODELO DE GESTÃO DO CONTRATO (Art. 6º, XXIII, alínea "f", Lei nº 14.133/2021)

6.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas do presente instrumento e outras avençadas, bem como de acordo com as normas da Lei nº 14.133/2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

6.2. Em caso de impedimento, ordem de paralisação ou suspensão do contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

6.3. As comunicações entre o órgão ou a entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de ***e-mail*** institucional para esse fim.

6.4. A Câmara Municipal de Goiânia poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

6.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou a entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

6.6. O contrato deverá ter sua execução acompanhada e fiscalizada por fiscais do contrato e deverá ser administrado e acompanhado pela Comissão Gestora de Contratos, de acordo com a Portaria nº 283/2023 da

Câmara Municipal de Goiânia, permitida a contratação de terceiros para assisti-los e subsidiá-los com informações pertinentes a essa atribuição.

6.7. Durante a execução do contrato poderá ser exigida comprovação de que o contratado mantém a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, e a reserva de percentual de 5% (cinco por cento) das vagas de mão de obra para pessoas em situação de rua no cumprimento da legislação específica (Lei Municipal nº 10.462/2020), mediante a indicação dos empregados que preencherem as referidas vagas, conforme disposto no art. 116 da Lei nº 14.13/2021.

6.8. O contratado deverá manter preposto aceito pela Administração no local do serviço para representá-lo na execução do contrato (art. 118, Lei nº 14.133/2021).

6.9. O contratado será obrigado a reparar, corrigir, remover, reconstruir ou substituir, a suas expensas, no total ou em parte, o objeto do contrato em que se verificarem vícios, defeitos ou incorreções resultantes de sua execução ou de materiais nela empregados (art. 119, Lei nº 14.133/2021).

6.10. A fiscalização ou acompanhamento pelo Contratante não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios e, na ocorrência desta, não implica em corresponsabilidade da Administração ou de seus agentes e prepostos.

6.11. O contratado será responsável pelos danos causados diretamente à Administração ou a terceiros em razão da execução do contrato, e não excluirá nem reduzirá essa responsabilidade a fiscalização ou o acompanhamento pelo contratante (Lei nº 14.133/2021, art. 120).

6.12. Somente o contratado será responsável pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato (Lei nº 14.133/2021, art. 121, ***caput***).

6.13. A inadimplência do contratado em relação aos encargos trabalhistas, fiscais e comerciais não transferirá à Administração a responsabilidade pelo seu pagamento e não poderá onerar o objeto do contrato (Lei nº 14.133/2021, art. 121, § 1º).

7. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO (art. 6º, XXIII, alínea

“g”, Lei nº 14.133/2021)

7.1. Da Medição de Serviços

7.1.1. A avaliação da execução do objeto utilizará os critérios:

7.1.1.1. Verificação se as licenças foram ativadas na central de administração da solução .

7.1.1.2. Verificação do processo de instalação dos agentes e dos endpoints, se estão ocorrendo de modo satisfatório(sem falhas).

7.1.1.3. Verificação de todas a configurações solicitadas, se estão preenchidas e operando nos computadores em conformidade.

7.2. Do Recebimento do Objeto (art. 140, I e II, Lei nº 14.133/2021)

a) Os serviços serão recebidos provisoriamente, no prazo de 55 (cinquenta e cinco) dias, contados da O.S. pelo responsável pelo acompanhamento e fiscalização do contrato, mediante Termo de Recebimento Provisório, quando verificado o cumprimento das exigências de caráter técnico e administrativo.

b) Os serviços poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades.

c) O recebimento definitivo ocorrerá no prazo de até 10 (dez) dias úteis, a contar do recebimento provisório, após a verificação da qualidade e quantidade do serviço e consequente aceitação, mediante Termo de Recebimento Definitivo.

d) Na hipótese de a verificação a que se refere o subitem anterior não ser procedida dentro do prazo fixado, reputar-se-á como realizada, consumando-se o recebimento provisório em definitivo no dia do esgotamento do prazo.

e) 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 14.133/2021, 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.

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

g) 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.

7.3. Do Pagamento

a) O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados do recebimento da Nota Fiscal ou Fatura em parcela única, através de ordem bancária, para crédito em banco, agência e conta-corrente indicados pelo contratado.

b) Considera-se ocorrido o recebimento da nota fiscal ou fatura no momento em que o fiscal do contrato atestar a execução do objeto, que ocorrerá após sanadas eventuais irregularidades na Nota Fiscal e documentação exigida para comprovação da execução do contrato ou instrumento equivalente, bem como comprovação de regularidade fiscal da contratada.

c) A nota fiscal ou o instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhada da comprovação da regularidade fiscal, constatada por meio de consulta ***on-line*** ao SICAF ou, na impossibilidade de acesso ao referido sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133/2021.

d) Constatando-se a situação de irregularidade da CONTRATADA, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.

e) Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa.

f) Havendo a efetiva execução do objeto, o pagamento será realizado normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação fiscal.

8. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR (Art. 6º, XXIII, alínea “h”, Lei nº 14.133/2021)

8.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, na forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO.

8.2. As exigências de habilitação jurídica, fiscal, social, trabalhista, econômico-financeira e técnico-profissional ou operacional são as usuais para a generalidade dos objetos, conforme disciplinado no Edital de Licitação, observado o disposto no Capítulo VI, do Título II, da Lei nº 14.133/2021.

8.3. Caso atendidas as condições para contratação, a habilitação do fornecedor será verificada por meio do SICAF, nos documentos por ele abrangidos e demais exigências previstas em contrato ou instrumento equivalente, em especial às relacionadas às habilitações jurídica, social, fiscal e trabalhista.

9. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO (Art. 6º, XXIII, alínea “i”, Lei nº 14.133/2021)

9.1. O valor estimado da contratação, acompanhado dos preços unitários referenciais, das memórias de cálculo e dos documentos que lhe dão suporte, terá caráter sigiloso e consta em documento denominado “ORÇAMENTO ESTIMADO DA CONTRATAÇÃO”.

9.2. Justificativa para o sigilo do valor estimado

A opção pelo orçamento sigiloso se justifica em virtude da busca pela maior vantajosidade da proposta, garantindo a ampla competitividade e economicidade para a Administração, a fim de obter o preço compatível com o praticado no mercado.

10. ADEQUAÇÃO ORÇAMENTÁRIA (Art. 6º, XXIII, alínea “j”, da Lei nº 14.133/2021)

10.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento da Câmara Municipal de Goiânia.

10.2. A Dotação Orçamentária que atenderá a presente contratação será especificada posteriormente, nos autos do processo de contratação, pela Diretoria Financeira da Câmara Municipal de Goiânia.

Goiânia, 12 de dezembro de 2024.

Djalma Rufino Mendes

Diretor Substituto de Tecnologia da Informação

Documento assinado eletronicamente por:

- **DJALMA RUFINO MENDES**, **CD - DVHAR**, em 12/12/2024 09:51:27.

Este documento foi emitido pelo SUAP em 11/12/2024. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.camaragyn.go.gov.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 117472
Código de Autenticação: bd5e9bdddc