TERMO DE REFERÊNCIA

EDR – ENDPOINT DETECTION AND RESPONSE

DIRETORIA DE INFRAESTRUTURA E TECNOLOGIA

Outubro / 2022

Data	Descritivo	autor	Versão
26/10/2022	inicial	WK / JRV / DSE	V01
31/10/2022	Revisão	WK / JRV / DSE	V01.1

ANEXO I

"TERMO DE REFERÊNCIA"

1. CENÁRIO

Com o crescente aumento da necessidade de proteção aos dados corporativos e principalmente alinhado as necessidades de atendimento a LGPD, se faz necessário implementação de ferramentas automatizadas para gerir o fluxo de informações, minimizar riscos de ataques, invasões e de vazamento de dados de forma acidental ou propositada, minimizando a superfície de ataques e ainda, visibilidade de anomalias ou ações suspeitas de abrangência não somente norte-sul, como também Leste-Oeste (dentro da rede local)

Por se tratar de uma Ata de Registro de Preço – ARP, cada ente municipal terá a liberdade de contratação da solução ofertada.

Cada ente deverá definir a quantidade de agentes (quantidade de licenças por computadores a serem contemplados) contratados por comutador conectado a rede corporativa.

Neste cenário a Prodam proverá serviço de monitoramento, dashboards e gestão da solução ofertada, este serviço será cobrado através de horas técnicas negociadas e definidas junto aos clientes.

Esse novo serviço prevê a implementação da solução especializada de prevenção de ameaças de nova geração (EDR - Endpoint Detection and Response), em adição às soluções de cibersegurança atualmente em uso no ambiente de rede das unidades da PMSP, não interferindo na(s) solução(ões) de segurança já implementadas, e imprimindo um nível adicional de segurança computacional, capaz de detectar e

responder a estas novas técnicas de ataques cibernéticos avançados.

“Definição: As soluções de detecção e resposta de endpoint (EDR) facilitam a detecção e investigação de eventos de segurança, identificam ataques e produzem orientações de remediação. Eles devem analisar todas as atividades de usuários, processos, sistemas e relatar a configuração do dispositivo. A detecção de ameaças é combinada com a correção remota. A automação das ações de resposta geralmente é fornecida e a integração com outras ferramentas é fundamental.

Impacto aos negócios:

- O EDR é uma camada de proteção para todos os setores e deve ser aplicado a todos os dispositivos e servidores que se conectam a sistemas corporativos ou manipulam dados.
- A detecção precoce e a resposta rápida são essenciais para lidar com as ameaças mais recentes e explorações furtivas que podem evitar a detecção tradicional.

Pontos de destaque:

- Campanhas furtivas de malware e ransomware, usam técnicas avançadas para permanecer indetectáveis e contornar controles de segurança mais antigos.
- O trabalho remoto acelerou a adoção de soluções gerenciadas em nuvem, que agora representam 80% da base instalada e a maioria das novas implantações.
- Os ataques sem arquivo agora são um componente comum de todos os tipos de malware, tornando a detecção comportamental de ferramentas de EDR essencial para combater ameaças avançadas e campanhas de ransomware operadas por humanos em constante mudança.
- Atanques avançados visando uma organização mostraram que podem desabilitar soluções de proteção, tornando a proteção

anti-adulteração crítica. Alertas abrangentes e telemetria para facilitar a detecção precoce e a resposta rápida também são necessários.

- A resposta rápida em tempo real, à medida que os incidentes se desenrolam, é fundamental para conter uma ameaça e impedir que ela se espalhe.
- Aumentar os programas de gerenciamento de vulnerabilidades existentes e fornecer meios para reduzir a superfície de ataque é cada vez mais necessário para garantir que os sistemas não sejam configurados incorretamente e não tenham vulnerabilidades não corrigidas.
- A correlação de logs e eventos de agentes EDR também pode ser usada para detecção retrospectiva de ameaças e busca de ameaças.
- Ataques sofisticados exigem uma nova geração de ferramentas de EDR que funcionem de forma holística em conjunto com outras ferramentas de segurança como um ecossistema de segurança composto para maximizar a proteção e minimizar a exposição.”

2. OBJETO:

Abertura de processo para futura Ata de Registro de Preços, envolvendo contratação de empresa especializada para o fornecimento de serviço de subscrição de solução corporativa de prevenção de ameaças de nova geração (EDR - Endpoint Detection and Response), contemplando instalação, configuração, treinamento e suporte especializado da solução, pelo período de 36 (trinta e seis) meses, conforme especificações constantes e disposições específicas deste Termo de Referência.

1.1. Tabela de composição de itens:

ITEM	DESCRIÇÃO	UNID.	QUANT.	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
01	Subscrição de solução corporativa de prevenção de ameaças de nova geração (EDR – Endpoint Detection and Response) pelo período de 36 meses, incluindo Suporte da fabricante da solução pelo período contratado.	UN			
02	Serviço de Instalação e Configuração da solução pela Contratada.	UN			
03	Serviço de Suporte 24 x 7 da Contratada	UN			
04	Vagas de Treinamento da solução contratada, ministrado pela Fabricante	UN			
05	Vagas de Treinamento da solução contratada, ministrado pela Contratada.	UN			
VALOR GLOBAL = R$ VALOR A SER POSTADO NO COMPRASNET					

1.2. Vigência:

1.2.1. O Registro de Preços terá vigência de 12 (doze) meses, a contar da data de assinatura, podendo ser prorrogado até o limite de 5 anos, conforme dispõe o artigo 71, da Lei Federal nº 13.303/2016.

1.2.2. As contratações efetuadas durante o período de vigência deste Registro de Preços terão vigência por 36 (trinta e seis) meses.

1.2.3. Durante o período de vigência, estarão inclusas todas as atualizações necessárias para o perfeito funcionamento da solução.

2 ESPECIFICAÇÃO TÉCNICA:

2.1 Serviço de subscrição de solução corporativa de prevenção de ameaças de nova geração – (EDR – Endpoint Detetion and Response)

2.2 Características da Solução

2.2.1 As soluções a serem implantadas nas estações de trabalho e servidores deverão atender, no mínimo, os requisitos técnicos listados abaixo e deverão ser apresentadas na proposta técnica/comercial para efeito de validação e habilitação da LICITANTE.

2.2.1.1 No total de _____ dispositivos estão considerados _____ microcomputadores e/ou notebooks e _____ servidores. Não deverá haver diferenciação

2.2.2 A gerência de administração da solução deve ser centralizada para gerenciar todos os endpoints, independentemente da localização geográfica destes;

2.2.3 A gerência de administração da solução deve ser acessível em qualquer ponto da rede da contratante até mesmo quando estiverem conectados a redes públicas sem a necessidade de uma conexão VPN;

2.2.4 A solução deve ser capaz de detectar e bloquear em tempo real ameaças conhecidas e desconhecidas (zero-day), ataques fileless, ameaças avançadas (APTs), Ransomwares, exploits e outros comportamentos maliciosos, sem depender de base de assinaturas ou heurísticas.

2.2.5 A solução deverá ser baseada em plataforma de nuvem e oferecida como subscrição;

2.2.6 A administração deve estar acessível através de HTTPS usando um dos navegadores abaixo:

2.2.6.1 Edge;

2.2.6.2 Google Chrome;

2.2.6.3 Firefox.

2.2.7 A administração da solução deverá ser 100% em nuvem sem a necessidade de instalação de ferramenta local para o gerenciamento da solução;

2.2.8 A plataforma em nuvem deverá ser atestada e garantir que utiliza controles de segurança, disponibilidade, integridade de processamento, confidencialidade ou privacidade das informações de acordo com os padrões estabelecidos na certificação SOC2 (Padrão de Controle mundial de Organização de Serviços com auditoria que garante que os provedores de serviços gerenciem dados com segurança, para proteger os interesses e a privacidade de seus usuários e clientes);

2.2.9 Não serão aceitas soluções que utilizem base local de assinaturas, também conhecida como base de vacinas, para reconhecer ameaças, mesmo que este seja apenas um dos métodos de detecção da solução;

2.2.10 A gerência de administração da solução deve ter capacidade de separar os endpoints gerenciados através de grupos via seleção manual e a criação de grupos com adição de endpoints de forma automática com base em no mínimo, os critérios abaixo:

2.2.10.1 Domínio;

2.2.10.2 Endereços IP;

2.2.10.3 Endereço de rede (CIDR);

2.2.10.4 Hostname parcial ou completo;

2.2.10.5 Versão de sistema operacional;

2.2.10.6 Unidade Organizacional do Active Directory;

2.2.10.7 Versão do agente.

2.2.11 A gerência deve permitir aplicação de políticas para grupos de máquinas ou máquinas individuais;

2.2.12 Deve ser utilizado um fator de dupla autenticação, para autenticação na gerência de administração da solução;

2.2.13 Deve ser possível a definição de perfis (RBAC) para os usuários dentro da gerência de administração da solução delimitando as permissões e/ou acesso as funcionalidades e capacidades disponíveis dentro da plataforma;

2.2.14 A gerência de administração da solução deve oferecer suporte Single Sign On com compatibilidade de provedor de identidade (IdP);

2.2.15 A gerência de administração da solução deve contemplar, no mínimo, as seguintes visualizações:

2.2.15.1 Agentes ativos;

2.2.15.2 Agentes por sistema operacional;

2.2.15.3 Detecções por objetivo do ataque;

2.2.15.4 Detecções por tática do ataque;

2.2.15.5 Detecções por severidade do ataque;

2.2.15.6 Top 10 de detecções por máquina;

2.2.15.7 Top 10 de detecções por usuário.

2.2.16 A gerência da solução deve prover auditoria detalhada com, no mínimo, as seguintes ações administrativas:

2.2.16.1 Criação de grupos;

2.2.16.2 Adição de exclusões;

2.2.16.3 Autenticação por SSO;

2.2.16.4 Autenticação de usuário;

2.2.16.5 Autenticação de dois fatores;

2.2.16.6 Troca de senha da interface de gerenciamento;

2.2.16.7 Criação de usuários;

2.2.16.8 Deletar grupos;

2.2.16.9 Deletar políticas;

2.2.16.10 Revelar senha para desinstalação;

2.2.16.11 Iniciar isolamento de rede;

2.2.16.12 Atualizar permissões de usuário;

2.2.17 A administração da solução deve ser feita de forma centralizada, totalmente integrada e de um único fabricante. A visibilidade de ameaças (detecções ou incidentes) deve ser unificada, permitindo o diagnóstico e remediação das ameaças em toda a planta protegida;

2.2.18 As políticas de instalação (rollout) devem ser capazes de atualizar os agentes de forma automática considerando no mínimo as seguintes opções:

2.2.18.1 Versão mais recente;

2.2.18.2 Versão específica;

2.2.18.3 Uma versão anterior a mais recente (N-1);

2.2.18.4 Duas versões anteriores a mais recente (N-2).

2.3 Características dos Agentes ou Sensores

2.3.1 A solução deve possuir apenas um único software agente, ou sensor, instalado em cada dispositivo de computação (microcomputador ou servidor) para prover todas as funcionalidades descritas neste documento e que serão administradas através da conexão com a gerência de administração da solução. Não será aceita a instalação de componentes adicionais como agentes de comunicação com múltiplos subagentes, plug-ins e softwares de terceiros para o atendimento dos requisitos;

2.3.2 O agente deve suportar os seguintes sistemas operacionais:

2.3.2.1 Windows:

Windows Server 2019; Windows Server 2016; Windows Server 2012 e 2012 R2; Windows 2008 R2; Windows 7 SP1; Windows 8; Windows 10; e versões superiores;

2.3.2.2 Linux:

CentOS a partir da versão 6; Oracle Linux a partir da versão 7; Red Hat Enterprise Linux (RHEL) a partir da versão 7; SUSE Linux Enterprise 12.2 – 12.5 e 15.3; Ubuntu LTS a partir da versão 18.04; e versões superiores.

2.3.3 A comunicação entre os agentes e a gerência de administração da solução deve utilizar um túnel de segurança TLS criptografado utilizando certificate pinning;

2.3.4 O agente deve suportar comunicação com a gerência de administração da solução através de proxy.

2.3.5 A instalação do agente para desktop e servidores deve ser feita através de política no AD utilizando a permissão de administrador do domínio para instalação.

2.3.6 Para instalação do agente em desktops e servidores que não estejam no domínio corporativo, a CONTRATADA deverá fornecer junto a solução ferramenta de deployment para instalação do agente. Esta solução tem que ser configurada com a senha administrativa destes desktops ou servidores para a instalação do agente.

2.3.7 A solução contratada não pode ter incompatibilidade com a solução existente de Endpoint Protect da Trellix existentes nos Desktop e Servidores corporativos.

2.4 Características específicas para sistemas operacionais Windows

2.4.1 O agente deve implementar proteção de desinstalação através de senha ou token específica para cada endpoint gerenciado.

2.4.2 O agente deve conter mecanismos que garantam que seu funcionamento não possa ser interrompido por usuários sem privilégios administrativos;

2.4.3 Deve detectar tentativas de manipulação indevida dos componentes do agente;

2.4.4 A solução deve incorporar técnicas de aprendizado de máquina (Machine Learning) para detecção e prevenção de ataques;

2.4.5 Os motores de ML (Machine Learning) devem realizar a detecção e prevenção de artefatos maliciosos conhecidos e desconhecidos não somente na tentativa de execução, como também na tentativa de escrita do binário em disco, ou seja, se um binário considerado malicioso pelo motor de ML for escrito em disco deverá resultar em uma detecção e prevenção no momento da operação de escrita em disco.

2.4.5.1 Caso seja configurado para bloqueio o arquivo deverá ser quarentenado.

2.4.5.2 O motor de machine learning dessa capacidade deverá respeitar os níveis de sensibilidade configurados.

2.4.6 A solução deve permitir níveis de sensibilidade diferentes para detecção e prevenção de ataques através do componente de aprendizado de máquina;

2.4.7 Deve ser capaz de detectar Adware e programas potencialmente indesejados;

2.4.8 Deve ser capaz de detectar ameaças mesmo que o endpoint não esteja conectado à Internet;

2.4.9 Deve efetuar bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos;

2.4.10 Deve efetuar bloqueio de scripts e comandos em PowerShell considerados suspeitos;

2.4.11 Deve efetuar bloqueio automático de processos suspeitos;

2.4.12 Deve efetuar bloqueio baseado em análise do centro de inteligência do fabricante;

2.4.13 Deve efetuar bloqueio de operações em registro suspeitas;

2.4.14 Deve garantir que arquivos maliciosos sejam movidos para uma área de quarentena;

2.4.15 Deve ser capaz de forçar a utilização de ASLR, de modo a mitigar ataques que exploram corrupção de memória;

2.4.16 Deve ser capaz de forçar Data Execution Prevention de forma a impedir ataques que utilizem espaço de memória para execução de códigos em região de memória não executável;

2.4.17 Deve ser capaz de impedir ataques que utilizem a técnica de Heap Spray Preallocation;

2.4.18 Deve ser capaz de impedir ataques que sobrescrevam SEH (Structured Exception Handling);

2.4.19 Deve ser capaz de impedir ataques que explorem vulnerabilidades causadas por ponteiros nulos;

2.4.20 Deve ser capaz de detectar malwares do tipo Ransomware com base em, no mínimo, os comportamentos abaixo:

2.4.20.1 Deletar backups;

2.4.20.2 Operações em excesso ao sistema de arquivos;

2.4.20.3 Criptografia de arquivos;

2.4.20.4 Processos associados a malwares de ransomware tais como: Cryptowall, Wannacry, Locky;

2.4.21 Deve ser capaz de detectar exploração baseado em, no mínimo, os seguintes comportamentos:

2.4.21.1 Criação de processos suspeitos originados de navegadores;

2.4.21.2 Detecção de comprometimento de servidores Web através de webshell;

2.4.21.3 Detecção de arquivos suspeitos baixados ou escritos por um navegador que iniciaram a sua execução;

2.4.21.4 Injeção de código não esperada de um processo a outro;

2.4.21.5 Execução de Java Script através do executável Rundll32.

2.4.22 Deve ser capaz de detectar movimentação lateral através de burlar o processo de logon do Windows;

2.4.23 Deve ser capaz de detectar processos que tentam obter credenciais de login;

2.4.24 A solução deverá ter sido avaliada pelo MITRE e atender ao menos as seguintes técnicas dentro da avaliação do MITRE ATT&CK:

T1003, T1003.001, T1003.002, T1012, T1018, T1021, T1021.001, T1021.002, T1021.004, T1021.006, T1026, T1027, T1027.002, T1027.003, T1036, T1036.002, T1036.003, T1036.004, T1036.005, T1047, T1048, T1048.003, T1049, T1053, T1053.005, T1055, T1055.012, T1059, T1059.001, T1059.003, T1059.005, T1059.007, , T1069.001, T1070, T1070.004, T1070.005, T1070.006, T1071.004, T1074.002, T1078.003, T1087, T1087.001, T1087.002, T1095, T1102, T1110, T1110.003, T1112, T1114.001, T1132, T1132.001, T1134.002, T1136, T1136.001, T1204, T1204.002, T1218, T1218.005, T1218.011, T1219, T1222, T1222.001, T1543, T1543.003, T1546.003, T1546.008, T1546.015, T1547, T1547.001, T1548, T1548.002, T1550, T1550.002, T1550.003, T1552.001, T1559, T1559.001, T1560, T1560.001, T1562, T1562.004, T1564, T1564.004, T1567, T1567.002, T1570, T1574, T1574.001

2.4.25 O agente para estações Windows deve suportar a RFC 5246;

2.4.26 Deve prover recursos para que administradores possam executar ações de remediação remotamente, sem necessidade ou integração com soluções de terceiros e sem a instalação de softwares adicionais no endpoint gerenciado;

2.4.27 Deve efetuar exclusão de arquivos e pastas utilizando caracteres coringa (Wildcard);

2.4.28 Deve bloquear a execução conforme definição granular de no mínimo, os seguintes comandos de alto risco sendo executados de forma remota no endpoint via gerência de administração da solução:

2.4.28.1 Extração de arquivos;

2.4.28.2 Envio de arquivos para um repositório externo;

2.4.28.3 Iniciar execução de um processo;

2.4.28.4 Dump de memória do endpoint;

2.4.28.5 Dump de memória de um processo específico no endpoint.

2.4.29 Deve permitir que scripts PowerShell possam ser adicionados à solução para que possam ser executados remotamente em resposta à um incidente de segurança;

2.4.30 Deve permitir que o acesso remoto seja desabilitado globalmente em endpoints específicos;

2.4.31 Deve implementar permissões específicas de forma a impedir que o acesso remoto esteja disponível somente para usuários específicos;

2.4.32 Deve permitir que administradores possam interromper ou bloquear tráfego de rede de endpoints classificados como comprometidos. O tráfego deve ser restrito somente com a gerência de administração da solução para efetuar análise e diagnóstico aprofundado, e posteriormente readmitir o endpoint quando ele estiver saneado;

2.4.33 A solução deve prover a capacidade de adição de endereços específicos para mesmo quando o endpoint esteja em quarentena sejam alcançáveis, ou seja, quando houver o isolamento do endpoint o mesmo deverá ter a possibilidade de comunicar com endereços especificados em política ademais da comunicação com a gerência de administração da solução;

2.4.34 A solução deve permitir que a proteção de dispositivos seja habilitada em modos de detecção somente, sem bloqueio efetivo;

2.4.35 Deve permitir bloqueio de dispositivos USB baseado em, no mínimo, as seguintes classes de dispositivo:

2.4.35.1 Dispositivos de imagem;

2.4.35.2 Dispositivos de áudio e vídeo;

2.4.35.3 Dispositivos de armazenamento em massa;

2.4.35.4 Dispositivos móveis (MTP/PTP);

2.4.35.5 Impressoras;

2.4.35.6 Adaptadores de rede wireless.

2.4.36 Para dispositivos de armazenamento em massa, deve permitir acesso granular com no mínimo, as seguintes permissões:

2.4.36.1 Leitura somente;

2.4.36.2 Escrita e leitura;

2.4.36.3 Escrita leitura e execução;

2.4.36.4 Bloqueio total.

2.4.37 A proteção de dispositivos deve permitir exceções baseadas no Vendor ID e Product ID, número serial e classe;

2.4.38 Deve permitir a criação de regras, grupos de regras e políticas de firewall para definir com precisão qual tráfego de rede é permitido e bloqueado no host;

2.4.39 A política de firewall deve permitir a utilização de múltiplas regras de firewall;

2.4.40 As regras de firewall devem ser agrupáveis, ou seja, as regras de firewall utilizadas em uma política devem ser configuradas de forma a ser possível de selecionar um grupo de regras a serem usadas em uma política;

2.4.41 Regras de firewall devem suportar minimamente as seguintes características:

2.4.41.1 IPv4;

2.4.41.2 IPv6;

2.4.41.3 Protocolos:

a) Any;

b) TCP;

c) UDP;

d) ICMP;

e) Avançado (permitindo especificar o protocolo).

2.4.41.4 Endereço local;

2.4.41.5 Porta local;

2.4.41.6 Endereço remoto;

2.4.41.7 Porta remota;

a) Ação:

b) Permitir;

c) Bloquear.

d) Direção da conexão:

e) Inbound;

f) Outbound;

g) Inbound e Outbound.

2.4.42 Deve ser possível a configuração de regras de firewall em modo observação, gerando assim registros de qual seria a ação/impacto caso a regra fosse aplicada;

2.4.43 As regras dentro de um grupo podem ser habilitadas ou desabilitadas de forma independente.

2.5 Características específicas para sistemas operacionais Linux

2.5.1 Deve incorporar técnicas de aprendizado de máquina (Machine Learning) para detecção e prevenção de ataques;

2.5.2 Deve suportar níveis de sensibilidade diferentes para detecção e prevenção de ataques através do componente de aprendizado de máquina;

2.5.3 Deve suportar níveis de sensibilidade diferentes para detecção de ataques através do componente de aprendizado de máquina;

2.5.4 Deve efetuar bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos;

2.5.5 Deve prover recursos para que administradores possam executar ações de remediação remotamente, sem necessidade ou integração com soluções de terceiros e sem a instalação de softwares adicionais no endpoint gerenciado;

2.5.6 Deve bloquear a execução conforme definição granular de no mínimo, os seguintes comandos de alto risco sendo executados de forma remota no endpoint via gerência de administração da solução:

2.5.6.1 Extração de arquivos;

2.5.6.2 Envio de arquivos para um repositório externo;

2.5.6.3 Iniciar execução de um processo.

2.5.6.4 Deve permitir que scripts bash possam ser adicionados à solução para que possam ser executados remotamente em resposta a um incidente de segurança. Deve permitir que administradores possam interromper ou bloquear tráfego de rede de endpoints classificados como comprometidos. O tráfego deve ser restrito somente com a gerência de administração da solução, para efetuar análise e diagnóstico aprofundando, e posteriormente readmitir o endpoint quando ele estiver saneado;

2.6 Relatórios e Dashboard

2.6.1 A solução deverá prover Dashboard trazendo as detecções mais recentes, número de novas detecções e detecções por táticas nos últimos 30 dias.

2.6.2 A plataforma deverá ter a capacidade de reportar as detecções de forma agrupada tendo como opções de agrupamento no mínimo os seguintes critérios:

2.6.2.1 Por máquina;

2.6.2.2 Por tática;

2.6.2.3 Por técnica;

2.6.2.4 Por Severidade.

2.6.3 A plataforma deverá ter a capacidade de reportar as detecções, permitindo organizar com a mais recente no topo, ou a mais antiga no topo.

2.6.4 A plataforma deverá ter a capacidade de reportar as deteções, permitindo filtrar minimamente com base aos seguintes filtros:

2.6.4.1 Severidade;

2.6.4.2 Tática;

2.6.4.3 Técnica;

2.6.4.4 Usuário;

2.6.4.5 Host;

2.6.4.6 Tipo de sistema operacional;

2.6.4.7 Versão do sistema operacional;

2.6.4.8 Última hora;

2.6.4.9 Último dia;

2.6.4.10 Última semana;

2.6.4.11 Últimos 30 dias;

2.6.4.12 Nome de arquivo;

2.6.4.13 Hash do processo.

2.6.5 A solução deve prover a capacidade de visibilidade da solução em dispositivos de computação (microcomputadores e servidores), contendo minimamente as seguintes informações que não deverão ser passiveis de exclusão ou limpeza, garantindo assim o não-repúdio:

2.6.5.1 Login do administrador/operador que realizou a operação;

2.6.5.2 Nome do endpoint;

2.6.5.3 Duração da sessão;

2.6.5.4 Data e hora do início da sessão;

2.6.5.5 Arquivos copiados desde a máquina;

2.6.5.6 Comandos executados na máquina;

2.6.5.7 Caminho completo do arquivo copiado da máquina;

2.6.5.8 Data e hora de cada comando executado.

2.6.6 A plataforma deverá gerar relatório das máquinas contendo minimamente as seguintes informações, podendo ser exportada em CSV:

2.6.6.1 Hostname;

2.6.6.2 Data e hora da primeira comunicação;

2.6.6.3 Data e hora da última comunicação;

2.6.6.4 Versão do sistema operacional;

2.6.6.5 Modelo;

2.6.6.6 Tipo;

2.6.6.7 Unidade organizacional (OU);

2.6.6.8 Site;

2.6.6.9 Política de proteção aplicada;

2.6.6.10 Política de resposta aplicada;

2.6.6.11 Política de atualização aplicada;

2.6.6.12 Política de controle de dispositivos USB aplicada;

2.6.6.13 Política de firewall aplicada;

2.6.6.14 Identificação do host (UID/GUID);

2.6.6.15 IP local da máquina;

2.6.6.16 IP público da máquina;

2.6.6.17 MAC Address;

2.6.6.18 Versão do sensor/agente instalado.

2.6.7 A solução deve prover a capacidade de visibilidade em dispositivos de computação (microcomputadores e

servidores) em síntese de ativos e políticas, contendo minimamente as seguintes informações:

2.6.7.1 Domínio;

2.6.7.2 Grupo;

2.6.7.3 Identificação do host (UID/GUID);

2.6.7.4 Hostname;

2.6.7.5 IP local da máquina;

2.6.7.6 MAC Address;

2.6.7.7 Subnet da máquina;

2.6.7.8 Versão do sistema operacional;

2.6.7.9 Unidade organizacional (OU);

2.6.7.10 Plataforma;

2.6.7.11 Política de proteção aplicada;

2.6.7.12 Política de resposta aplicada;

2.6.7.13 Política de atualização aplicada;

2.6.7.14 Versão do sensor/agente instalado.

2.6.8 A solução deve prover a capacidade de visibilidade da solução em dispositivos de computação (microcomputadores e servidores) em síntese de ativos, contendo minimamente as seguintes informações:

2.6.8.1 Total de hosts vistos nas últimas 24 horas;

2.6.8.2 Total de estações vistos nas últimas 24 horas;

2.6.8.3 Total de servidores vistos nas últimas 24 horas;

2.6.8.4 Hosts comunicando na última hora;

2.6.8.5 Hosts off-line;

2.6.8.6 Hosts isolados/quarentenados;

2.6.8.7 Hosts com sensor sem proteção para desinstalação;

2.6.8.8 Total de máquinas em cada política de proteção;

2.6.8.9 Total de máquinas em cada política de resposta;

2.6.8.10 Total de máquinas em cada política de atualização do sensor;

2.6.8.11 Total de máquinas em cada política de controle USB.

2.6.9 Deve permitir a criação de fluxo de trabalho (Workflow) para automatização de processos, os quais devem incluir os seguintes recursos:

2.6.9.1 Verificação da cadeia de execução do Workflow;

2.6.9.2 Compreender gatilhos de execução baseados em:

a) Novos Incidentes;

b) Novas detecções;

c) Eventos de auditoria incluindo os parâmetros: atribuição, status, comentários e políticas.

2.7 Investigação e detecção de ameaças

2.7.1 A solução deve ser composta de módulo de software com serviço gerenciado de detecção de invasor infiltrados no ambiente e acionamento imediato do cliente via gerência de administração da solução;

2.7.2 O Serviço deve analisar campanhas de malwares e de incidentes gerados na gerência de administração da solução;

2.7.3 O serviço deve fornecer notas explicativas ou recomendações para remediação baseado nas atividades encontradas;

2.7.4 A solução deve notificar os incidentes por e-mail ou gerência de administração da solução;

2.7.5 Capacidade de processamento de dados massivos em busca de atividades maliciosas;

2.7.6 Capacidade de reportar informações referentes ao incidente na própria gerência de administração da solução;

2.8 Capacidades de inteligência de ameaças

2.8.1 A Ferramenta deverá monitorar ameaças e contextos políticos e globais que possam influenciar na incidência de ataques de cibersegurança;

2.8.2 A inteligência de ameaças deve mapear atores maliciosos e dar visibilidade de países e indústrias alvo, pais de origem e última atividade;

2.8.3 Para atores maliciosos, o serviço de inteligência deve fornecer, quando aplicável, informações tais como vulnerabilidades utilizadas, métodos de instalação, ações e objetivos, métodos de entrega e breve descrição do grupo;

2.8.4 Deve associar, quando pertinente, detecções presentes no ambiente aos atores maliciosos;

2.8.5 Deve permitir extração de indicadores de comprometimento como hashes MD5, SHA1, SHA256, domínios, endereços IP, endereços de email, nomes de arquivos associados às atividades maliciosas;

2.9 Capacidades de emulação de execução de código

2.9.1 A solução deve prover, integrada à gerência de administração da solução, capacidades de emulação de execução de arquivos, sem instalação de componentes adicionais ou softwares de terceiros;

2.9.2 Deve se integrar ao agente instalado em endpoints para permitir que arquivos suspeitos sejam enviados de forma automática ao serviço de emulação de execução;

2.9.3 A solução deve emular execução, no mínimo, nos seguintes sistemas operacionais:

2.9.3.1 Windows 10;

2.9.3.2 LINUX Ubuntu, Red Hat, CentOS

2.9.3.3 Windows Server 2012

2.9.4 A solução deve incluir na análise de execução, no mínimo, as seguintes características:

2.9.4.1 Táticas e técnicas de acordo como modelo de ameaças MITRE ATT&CK;

2.9.4.2 Características comportamentais suspeitas;

2.9.4.3 Imagens de execução, quando aplicável;

2.9.4.4 Detalhes do arquivo como nome, hash, tamanho, tipo;

2.9.4.5 Atividade de rede incluindo conexões, endereços IP de destino, domínios, portas;

2.9.4.6 Leitura e escrita de arquivos em disco;

2.9.4.7 Leitura e alteração de chaves de registro;

2.9.4.8 Detalhes de processos iniciados durante a execução.

2.10 Capacidades de detecção, visibilidade e investigação

2.10.1 As informações de telemetria dos incidentes e ações ocorridas nos endpoints deverão estar disponíveis na gerência de administração da solução independentemente do status operacional dos endpoints, ou seja, caso o endpoint esteja inoperante, a investigação dos incidentes e eventos deverá ser possível;

2.10.2 A solução deve ser capaz de coletar e enviar à gerência de administração da solução os dados de telemetria das ações realizadas nos endpoints incluindo, no mínimo, as seguintes atividades:

2.10.2.1 Endereços de rede obtidos;

2.10.2.2 Login de usuários;

2.10.2.3 Informações de sistema operacional, modelo e última atividade;

2.10.2.4 Número de executáveis únicos;

2.10.2.5 Processos que foram executados;

2.10.2.6 Utilização de ferramentas administrativas;

2.10.2.7 Requisições DNS;

2.10.2.8 Conexões de rede incluindo portas e processos associados;

2.10.2.9 Arquivos compactados escritos;

2.10.2.10 Scripts escritos em disco;

2.10.2.11 Mapa de geolocalização de conexões de rede.

2.10.3 Deve permitir visibilidade sobre parâmetros de execução de um processo;

2.10.4 Deve permitir visibilidade sobre parâmetros de execução de um processo;

2.10.5 A solução deve permitir busca dos metadados coletados através de sintaxes que filtrem a busca, concatenando critérios;

2.10.6 Deve permitir a busca por hashes MD5 e SHA256;

2.10.7 Deve permitir buscas por nomes de arquivo;

2.10.8 Deve permitir a busca por atividades de usuário;

2.10.9 Deve permitir extração de dados em formato CSV e JSON.

2.11 Gerenciamento de vulnerabilidades

2.11.1 A solução deverá identificar vulnerabilidades em hosts Windows, macOS e Linux, incluindo vulnerabilidades do sistema operacional e de aplicações comuns.

2.11.2 Deverá usar frameworks da indústria, tais como:

2.11.2.1 NIST's National Vulnerability Database (NVD);

2.11.2.2 Mitre's Common Vulnerabilities and Exposures (CVE);

2.11.2.3 Common Vulnerability Scoring System (CVSS) score;

2.11.3 As vulnerabilidades identificadas deverão mostrar sua severidade usando não apenas conforme definido pelo Common Vulnerability Scoring System (CVSS) v2 e v3, mas também deverá contemplar definição de severidade com

base em modelo de inteligência artificial composto de ao menos três componentes:

2.11.3.1 Múltiplas origens de dados, tais como: CVSS, inteligência de ameaças, idade das vulnerabilidades, entre outras;

2.11.3.2 Atualização continua, onde o modelo poderá atualizar as severidades e predizer as ameaças durante atualizações regulares;

2.11.3.3 Transparência do modelo, trazendo assim visibilidade de quais fatores levados em conta, para a avaliação de risco, foram usados;

2.11.4 Além de permitir a criação de dashboards personalizados, deverá contemplar ao menos um dashboard inicial contendo as seguintes informações:

2.11.4.1 Total de vulnerabilidades presentes no ambiente;

2.11.4.2 Principais remediações recomendadas para o ambiente;

2.11.4.3 Lista de hosts mais vulneráveis presentes no ambiente;

2.11.4.4 Lista de produtos mais vulneráveis presentes no ambiente;

2.11.4.5 Quantidade de vulnerabilidades abertas e fechadas por dia;

2.11.4.6 Hosts com detecções críticas ou altas nos últimos 90 dias;

2.11.5 A solução deverá permitir a criação de regras de supressão, a fim de permitir filtrar vulnerabilidades que ficarão fora do escopo de correção e controle.

2.11.6 As regras de supressão deverão permitir ao menos o uso dos seguintes filtros:

2.11.6.1 CVE ID: Identificador de Vulnerabilidades e Exposições Comuns (CVE) de uma vulnerabilidade;

2.11.6.2 Grupo: nome do grupo de hosts;

2.11.6.3 ID do host: identificador exclusivo de um host;

2.11.6.4 Nome do host: nome de um host;

2.11.6.5 IP/CIDR local: IP do host ou endereço CIDR de um host;

2.11.6.6 Produto: Aplicativo ou sistema operacional (SO) instalado em um host;

2.11.6.7 Versão do produto: Versão de um produto instalado;

2.11.6.8 Tags: Marcações definidas para um host;

2.11.6.9 Fabricante e produto: Produto, incluindo o nome do fabricante, instalado em um host;

2.11.7 A regra de supressão deverá permitir declarar uma razão para as vulnerabilidades que serão filtradas, permitindo ao menos as seguintes razões:

2.11.7.1 Aceite de risco;

2.11.7.2 Controle compensatório;

2.11.7.3 Falso positivo;

2.11.8 Deverá ser possível saber o número de vulnerabilidades suprimidas por uma regra;

2.11.9 Deve ser possível a criação de uma regra de supressão a partir dos detalhes de visualização de uma vulnerabilidade;

2.11.10 A solução deve permitir a identificação de hosts com patches pendentes que exigem uma reinicialização;

2.11.11 A solução deve mostrar patches já instalados nos hosts;

2.11.12 A solução deverá monitorar continuamente o host permitindo a detecção de quando um update ou uma aplicação é instalada;

2.11.13 Para atualizações de segurança do sistema operacional Windows, a solução deverá permitir via botão na console acionar o Windows Update para que instale o KB em questão;

2.11.14 Deverá fornecer o status do exploit de uma vulnerabilidade com ao menos os seguintes status:

2.11.14.1 Não provado;

2.11.14.2 Disponível;

2.11.14.3 Fácil acesso;

2.11.14.4 Usado ativamente;

2.12 Inventário de ativos, usuários e aplicações

2.12.1 A solução deverá permitir encontrar ativos potencialmente desatualizados ou suspeitos em sua rede, mesmo que eles não tenham a tecnologia em questão instalada, permitindo assim expandir a cobertura do sensor para ativos corporativos não gerenciados;

2.12.2 Deverá permitir o acompanhamento das alterações de senha e a atividade de login junto com o uso de outras contas;

2.12.3 A solução deverá obter informações sobre o uso de aplicativos, por exemplo, os aplicativos que estão instalados—incluindo onde e quem os está usando—para orientar decisões sobre quais manter e quais desinstalar.

2.12.4 O monitoramento de dispositivos deverá trazer ao menos os seguintes controles:

2.12.4.1 Visualizar os ativos que foram adicionados ou removidos;

2.12.4.2 Localizar novos ativos sem presença do sensor;

2.12.4.3 Mapear relacionamentos entre ativos gerenciados;

2.12.4.4 Revisar o status de criptografia de disco;

2.12.4.5 Acompanhar o uso de recursos do sistema ao longo do tempo;

2.12.5 O monitoramento de credencias deverá trazer ao menos os seguintes controles:

2.12.5.1 Monitorar o uso de credenciais e quais ativos eles estão acessando;

2.12.5.2 Acompanhe se as credenciais de domínio ou locais são usadas;

2.12.5.3 Ver quando as senhas foram alteradas pela última vez;

2.12.5.4 Monitorar a atividade de login bem-sucedida e com falha;

2.12.6 O monitoramento de aplicações deverá trazer ao menos os seguintes controles:

2.12.6.1 Rastrear aplicativos instalados;

2.12.6.2 Listar quais máquinas estão;

2.12.7 O monitoramento de dispositivos deverá filtrar em ao menos três categorias os dispositivos encontrados, sendo elas:

2.12.7.1 Ativo gerenciado: Um ativo que possui a solução instalada;

2.12.7.2 Ativo não gerenciado: um ativo que poderia ter a solução instalada;

2.12.7.3 Ativo não suportado: um ativo que não pode ter a solução instalada;

3 Suporte, Manutenção e Garantia

3.1 Suporte especializado do fabricante das soluções (Nível 3)

3.1.1 Possuir portal de suporte para abertura de chamados, acesso a base de conhecimento;

3.1.2 O suporte deverá atender via telefone em escala 24x7x365;

3.1.3 Definição de contatos autorizados do cliente para acesso ao suporte técnico do fabricante, por telefone e portal Web;

3.1.4 Relatórios trimestrais;

3.1.5 Revisão trimestral de saúde do ambiente;

3.1.6 Apresentação de roadmap;

3.1.7 O suporte deverá prover minimamente os seguintes canais de comunicação para abertura de chamados:

3.1.7.1 Chat;

3.1.7.2 Portal web.

3.1.8 O fabricante deverá realizar sessão de apresentação do serviço de suporte contemplando minimamente os seguintes tópicos:

3.1.8.1 Processo de abertura de chamado;

3.1.8.2 Processo de escalamento de chamado;

3.1.9 Recomendações e melhores práticas específicas para o ambiente;

3.1.10 Envio pró-ativo de informativos sobre novas ameaças por email e/ou SMS;

3.1.11 Serviços de Suporte Técnico e Garantia do Fabricante:

3.1.11.1 Os serviços de suporte técnico e garantia do fabricante abrangem manutenção corretiva, esclarecimento de dúvidas, reparação de problemas na solução, elaboração de relatórios, estudos e diagnósticos sobre o ambiente monitorado;

3.1.11.2 Os serviços de suporte técnico e garantia abrangem as soluções fornecidas pela CONTRATADA no âmbito dessa contratação;

3.1.11.3 Os serviços de suporte técnico e garantia de toda a solução deverão ser prestados por um período de 36 (trinta e seis) meses e deverão ser iniciados a partir da aquisição das subscrições da solução pela CONTRATANTE;

3.1.11.4 Os serviços de suporte técnico do software poderão ser prestados de forma remota;

3.1.11.5 Os bens e produtos adquiridos devem ser licenciados de forma que o suporte e a garantia permitam as atualizações dos sistemas e ferramentas durante a vigência do contrato. Deverão estar

incluídas tanto as atualizações de segurança, quanto as atualizações para novas versões dos softwares licenciados, quando disponibilizadas.

3.1.11.6 Todos os sistemas ou ferramentas que fazem parte da solução deverão ser disponibilizados na versão mais recente disponibilizada pela fabricante;

3.1.11.7 A CONTRATADA deve garantir que todas as personalizações e configurações realizadas sejam automaticamente portadas para novas versões em caso de atualização, reinstalação ou upgrade, dispensando a necessidade de migrações ostensivas e onerosas;

3.1.11.8 Detalhamento de um plano de ação para correção dos problemas identificados, e será executado pela equipe interna da CONTRATANTE, por meio de orientações da Prefeitura.

3.1.11.9 A CONTRATADA deverá elaborar, a cada 4 meses, a partir do início do serviço de suporte técnico, relatório sobre a saúde dos produtos fornecidos, suportados e contratados pela CONTRATANTE, utilizando informações fornecidas pela solução contratada. O relatório deve contemplar, no mínimo, as seguintes informações:

a) Saúde do ambiente de EDR;

b) Evolução em relação a informações de relatórios anteriores;

3.1.11.10 O relatório descrito no item anterior deverá ser confeccionado e finalizado durante o mês em que se completa cada quadrimestre;

3.1.11.11 A CONTRATADA deverá disponibilizar um especialista técnico na CONTRATANTE uma vez por semana, de forma presencial, para análise do

ambiente, discussão e implementação das melhores práticas ;

3.1.11.12 Os serviços deverão ser prestados em conformidade com os seguintes prazos máximos de atendimento inicial:

Severidade	Tempo de Atendimento
1	1 Hora
2	4 horas
3	24 horas

3.1.11.13 A severidade do chamado que gera um incidente depende do impacto gerado no contexto do provimento dos serviços de TIC (e portanto, às funções do negócio) pela sua ocorrência:

a) Severidade 1 (Criticidade mais alta):

- ✓ Os negócios são severamente afetados.
- ✓ Um produto não está funcionando e nenhuma solução viável está disponível.
- ✓ Ambiente comprometido ou em risco de corrupção significativa de dados.
- ✓ O aplicativo de missão crítica está inativo ou a maioria dos usuários não consegue realizar negócios.

b) Severidade 2:

- ✓ Os negócios estão interrompidos, mas funcionando.
- ✓ A funcionalidade de um produto é severamente afetada.
- ✓ Aplicativos de missão crítica ou a maioria dos usuários são afetados.

c) Severidade 3:

- ✓ Os negócios não são afetados, mas existem sintomas.
- ✓ Um produto está funcionando de forma restrita, e existe uma solução alternativa.
- ✓ Os aplicativos de missão crítica estão funcionais, com alguns dos usuários finais afetados.

3.2 Suporte 24 x 7 da Contratada (Níveis 1 e 2)

3.2.1 Suporte 24 x 7, contratado por 36 (trinta e seis) meses;

3.2.2 Suporte ao ambiente já implementado da ferramenta;

3.2.3 Atendimento em idioma português;

3.2.4 Abertura de chamado através de e-mail e/ou telefone;

3.2.5 Elaboração de relatórios mensais acerca da saúde do ambiente;

3.2.6 Sugestão de melhorias na ferramenta e/ou no processo de proteção dos Endpoints;

3.2.7 Intermediação no processo de abertura e tratativa de chamado aberto junto à fabricante;

3.2.8 Reunião mensal de status report;

3.2.9 Gerente Técnico dedicado.

3.2.10 Os serviços deverão ser prestados em conformidade com os seguintes prazos máximos de atendimento:

Severidade	Tempo de Atendimento
1	30 minutos
2	2 horas corridas
3	8 horas, em horário comercial
4	2 dias úteis

3.2.10.1 A severidade do chamado que gera um incidente depende do impacto gerado no contexto do provimento dos serviços de TIC (e portanto, às funções do negócio) pela sua ocorrência:

a) Severidade 1 (Criticidade Alta): o problema causa perda ou paralisação total do serviço. O trabalho não pode ter uma sequência razoável, a operação passa a ser crítica para o negócio e a situação constitui-se em uma emergência.

b) Severidade 2 (Criticidade Média): o problema causa uma grave redução da funcionalidade ou do desempenho do serviço. Não existe nenhuma alternativa aceitável, mas as operações podem continuar ainda que de modo restrito.

c) Severidade 3 (Criticidade Baixa): o problema causa uma redução menor da funcionalidade ou do desempenho do serviço. O impacto constitui uma inconveniência que exige uma alternativa para restaurar a funcionalidade ou o desempenho.

d) Severidade 4 (Um pedido de informação): Solicitação de informações sobre o produto, ou dúvidas sobre como usar o produto. Impacto mínimo no negócio.

4 Treinamento da Fabricante – Certificação Oficial

4.1 Treinamento Oficial da Fabricante da Solução – Certificação Oficial (Em Inglês)

4.1.1 A CONTRATADA deverá disponibilizar à CONTRATANTE ____ vagas de treinamento oficial da fabricante da solução;

4.1.2 O treinamento deverá ser ministrado on-line, via e-learning, satisfazendo todos os requisitos, incluindo laboratórios

virtuais e demais ferramentas para o bom aproveitamento do curso;

4.1.3 A CONTRATANTE deverá informar à CONTRATADA os nomes e e-mails dos funcionários que participarão do treinamento;

4.1.4 O treinamento será ministrado em idioma inglês;

4.1.5 O material didático será fornecido em idioma inglês;

4.1.6 O treinamento deverá ser capaz de instruir os alunos a administrar e operar a solução adquirida;

4.1.7 Deverá ser fornecido certificado de conclusão ao final do treinamento.

4.1.8 O Treinamento caso presencial deverá ser ministrado dentro do município de São Paulo, caso contrário, todos os custos de transporte, hospedagem e alimentação correrá por conta da CONTRATADA.

4.1.9 A critério da CONTRATANTE serão aceitos vouchers para turmas abertas.

5 Treinamento da solução ministrado pela CONTRATADA

5.1.1 A CONTRATADA deverá disponibilizar à CONTRATANTE ____ vagas de treinamento da solução contratada;

5.1.2 O treinamento deverá ser ministrado on-line, em turmas fechadas de, no mínimo, 10 alunos, por instrutor certificado pela fabricante da solução, satisfazendo todos os requisitos, incluindo laboratórios virtuais e demais ferramentas para o bom aproveitamento do curso;

5.1.3 A CONTRATANTE deverá informar à CONTRATADA os nomes e e-mails dos funcionários que participarão do treinamento;

5.1.4 O treinamento deverá ser ministrado em idioma português;

5.1.5 O material didático deverá ser fornecido em idioma português;

5.1.6 O treinamento deverá ser capaz de instruir os alunos a administrar e operar a solução adquirida;

5.1.7 Deverá ser fornecido certificado de conclusão ao final do treinamento.

5.1.8 O Treinamento caso presencial deverá ser ministrado dentro do município de São Paulo, caso contrário, todos os custos de transporte, hospedagem e alimentação correrá por conta da CONTRATADA.

5.1.9 A critério da CONTRATANTE serão aceitos vouchers para turmas abertas.

6 Documentação Técnica

6.1 Deverão ser fornecidos juntamente com os produtos e licenças os manuais técnicos de referência, contendo todas as informações sobre os produtos com as instruções para instalação, configuração e operação, preferencialmente em Português (Brasil), ou, na inexistência de tradução em Português, podem ser escritos em Língua Inglesa.

7 REQUISITOS DE PROJETO E DE IMPLEMENTAÇÃO

A empresa vencedora da licitação deverá apresentar um projeto para instalação da solução de EDR em toda as Secretarias aderentes à ARP;

7.1 O projeto deverá ser conduzido em fases:

7.1.1 Iniciação: a CONTRATADA deverá criar a visão do projeto e definirá o escopo de trabalho necessário para trazê-la para a realidade;

7.1.2 Planejamento: deverá consistir na elaboração dos processos detalhados a serem utilizados na implantação do projeto;

7.1.3 Execução: consistirá na execução das atividades definidas na fase de planejamento, podendo ser dividida em sub-bases para melhor controle;

7.1.4 Estabilização: a solução deverá ser disponibilizada para os usuários do ambiente de produção, sendo efetuados os ajustes necessários para a estabilização da mesma;

7.1.5 Encerramento: Deverá ser entregue a documentação do projeto, e coletada a aprovação formal do cliente;

7.2 Da inicialização e planejamento

7.2.1 Reunião de startup:

7.2.1.1 Apresentação de cronograma;

7.2.1.2 Levantamento de requisitos;

7.2.1.3 Informações de ambiente;

7.2.1.4 Configurações de políticas para planejamento de implementação e configurações.

7.2.2 Levantamento de informações do ambiente pertinentes ao projeto de implementação;

7.2.3 Alinhamento de requisitos necessários para implementação das soluções;

7.2.4 Definição de papeis e responsabilidades;

7.2.5 Levantamento de políticas e regras para solução de EDR;

7.2.6 Definição e alinhamento de cronograma para implementação das soluções;

7.2.7 O prazo da CONTRATADA para o planejamento de implementação das licenças de EDR devem ser de 25 (vinte e cinco) dias da assinatura do contrato e a CONTRATANTE tem 5 (cinco) dias para dar o aceite no projeto;

7.2.7.1 A partir da data de aceite, por parte da CONTRATANTE, ao projeto e cronograma entregues pela CONTRATADA. Esse prazo é referente às

atividades da CONTRATADA. Não estarão aí contabilizadas as atividades de responsabilidade da CONTRATANTE;

7.2.8 Não serão considerados responsabilidade da CONTRATADA implementação de agentes em equipamentos fora de pré-requisitos estabelecidos pelo fabricante, sem conectividade com a console central de administração da solução.

7.3 Responsabilidade do Fabricante das soluções vencedoras:

7.3.1 Deverão acompanhar 30% de implementação nas dependências da PRODAM e conjunto com a equipe de analistas de segurança da informação da PRODAM;

7.3.2 Deverão executar Health Check (saúde das consoles) nas soluções de EDR e servidores trimestralmente;

7.3.3 Os profissionais deverão ter um contrato de trabalho com o CNPJ do mesmo no Brasil.

7.4 Implementação da solução de EDR

7.4.1 Setup de implantação com escopo fechado;

7.4.2 Setup da solução seguindo as melhores práticas do fabricante de solução;

7.4.3 Configuração de acesso a console para os administradores;

7.4.4 Configuração de no mínimo 10 políticas de prevenção;

7.4.5 Configuração de no mínimo 10 políticas para atualização dos agentes, ou sensores;

7.4.6 Configuração de no mínimo 6 grupos para organização e gerenciamento dos dispositivos;

7.4.7 Configuração de no mínimo 10 políticas de firewall;

7.4.8 Configuração de no mínimo 10 políticas de controle de dispositivos;

7.4.9 Configuração de no mínimo 10 políticas de exceção (ML/IOA/VL);

7.4.10 Configuração de no mínimo 10 políticas de bloqueio (hash/IOA);

7.4.11 Confecção de script se necessário para deploy dos agentes, ou sensores, no parque;

7.4.12 Homologação do processo de deploy dos agentes, ou sensores, para as plataformas selecionadas;

7.4.13 Customização de scrips e APIs para distribuição do agente, ou sensor, e coleta de informações da solução;

7.4.14 Instalação dos agentes, ou sensores, em todos os dispositivos que estiverem de acordo com os requisitos técnicos e forem alcançáveis dentro do prazo do projeto;

7.4.15 Integração com SIEM;

7.4.16 Validação do funcionamento dos agentes, ou sensores, e das funcionalidades através da análise dos relatórios e dashboards padrões.

7.5 Fase de homologação

7.5.1 Para homologação das soluções, o projeto de implementação deverá possuir uma fase inicial ou fase piloto contemplando a instalação (deploy) dos agentes em 1% (1 por cento) do número de computadores a serem protegidos pela solução de EDR contratada, contemplando infraestruturas diversificadas, assim como sistemas operacionais e equipamentos de hardware diferentes nos ambientes da PRODAM.

7.6 Fase de Rollout

7.6.1 A instalação das soluções ocorrerá em estações de trabalho e servidores instalados na rede da Prefeitura Municipal de São Paulo administrados pela PRODAM;

7.6.2 Deverá ser utilizada como método de instalação (deploy) dos agentes em desktops e notebooks, a instalação remota via console da solução contratada ou solução de distribuição sem custos adicionais. A PRODAM fornecerá os pré-requisitos para viabilidade da instalação remota via console da solução;

7.6.3 A instalação (deploy) dos agentes deve ser realizada pela CONTRATADA nas dependências da PRODAM, de forma presencial e nas demais localidades por meio remoto ou presencial desde que seja comprovada a necessidade técnica ou acordado com a equipe técnica da PRODAM;

7.6.4 Será considerada concluída a implementação dos agentes nas estações de trabalho e servidores quando o número de computadores protegidos for igual ou superior a 80% do volume de licenças contratadas;

7.6.5 A CONTRATADA deverá apresentar solução para instalação (deploy) dos agentes da solução em desktops e notebooks, que não fazem parte do domínio local (Active Diretory), porém possuem comunicação de rede com a rede principal da PRODAM;

7.6.6 Durante a fase de rollout a CONTRATADA deverá disponibilizar técnicos capacitados para acompanhamento da equipe de implantação, com objetivo de resolver problemas de acesso físico e logico às localidades;

7.6.7 Instalação de console centralizada para gestão de todos os itens da solução ofertada nesta licitação;

7.6.8 Integração de todos os itens que compõem a solução de modo a permitir a visão e o gerenciamento em uma única console;

7.6.9 Serviço inicial de instalação, devendo a CONTRATADA fornecer mão de obra especializada e própria para realizar as seguintes atividades no início do contrato.

7.7 Execução

7.7.1 Embora conste previsto que os trabalhos terão o acompanhamento por parte da equipe técnica da CONTRATANTE, cabe intensificar o entendimento que a CONTRATADA terá exclusiva responsabilidade quanto à entrega dos serviços destacados, uma vez que estejam em plenas condições de operação munidos de todos os

requisitos fornecidos pelo CONTRATANTE e de acordo com os prazos estabelecidos;

7.7.2 As condições de execução remota das ações da CONTRATADA visam agilizar e facilitar o projeto, no entanto, eventuais visitas presenciais de técnicos nas unidades da Prefeitura de São Paulo deverão ocorrer sem qualquer ônus para a CONTRATANTE;

7.7.3 Em caso da necessidade de ajustes nas ações e responsabilidades listadas nos quadros anteriores, estas deverão ser prévia e obrigatoriamente aprovadas pela área técnica da CONTRATANTE;

7.7.4 A comunicação às unidades da Prefeitura de São Paulo, bem como o agendamento dos trabalhos deverão ser articulados por equipe própria de gestão do projeto da CONTRATANTE.

8 DAS OBRIGAÇÕES DA CONTRATADA

8.1 A Contratada deverá oferecer garantia, suporte e licenças da solução e suas funcionalidades contratadas por um prazo mínimo de 36 (trinta e seis) meses, a contar da data de sua efetiva instalação. Durante o período de cobertura, a CONTRATADA deverá prestar suporte para todos os componentes do objeto deste edital, incluindo configuração técnica do produto;

8.2 Disponibilizar profissionais certificados pelos fabricantes da solução para sua implementação;

8.2.1 Durante todo o período de implementação, a CONTRATADA deverá disponibilizar profissional certificado para prestação de serviço de Operação Assistida;

8.2.2 A Operação Assistida consiste em suporte presencial ou remoto que garanta o bom funcionamento da solução durante toda implementação;

8.3 Indicar preposto apto a representá-lo junto à Contratante;

8.4 Instalar, configurar e acompanhar os testes de funcionamento antes da entrada da solução em produção;

8.5 Orientar tecnicamente os responsáveis técnicos, da CONTRATANTE, pela operação dos equipamentos, fornecendo os esclarecimentos necessários ao seu perfeito funcionamento;

8.6 Disponibilizar número de telefone (local ou DDG) para suporte telefônico (24x7x365) e abertura de chamados técnicos;

8.7 Ao final da abertura de cada atendimento de suporte, a CONTRATADA deverá emitir um ticket do chamado técnico contendo, no mínimo:

8.7.1 Número do chamado;

8.7.2 Data e hora de abertura do chamado;

8.7.3 Previsão de conclusão do atendimento;

8.7.4 Severidade do erro;

8.7.5 Descrição da solicitação.

8.8 Depois de concluído o chamado, a CONTRATADA comunicará o fato à equipe técnica da CONTRATANTE e solicitará autorização para o fechamento deste. Caso a CONTRATANTE não confirme a solução definitiva do problema, o chamado permanecerá aberto até que seja efetivamente solucionado pela CONTRATADA. Nesse caso, a CONTRATANTE fornecerá as pendências relativas ao chamado aberto.

8.9 A CONTRATANTE poderá registrar um número ilimitado de chamados de suporte durante a vigência do Contrato.

8.10 Caso necessário, toda infraestrutura para o pleno funcionamento da solução, como servidores, sistemas operacionais, banco de dados, licenças, entre outros hardwares e softwares, devem ser disponibilizados pela CONTRATADA;

8.10.1 Proceder à entrega dos equipamentos, devidamente embalados, de forma a não serem danificados durante a operação de transporte e de carga e descarga, com as especificações detalhadas para conferência;

8.11 O tempo máximo de atendimento para os chamados de defeitos deverá ser atendido conforme sua severidade, a contar do registro de abertura do chamado no Centro de Atendimento Técnico da Contratada, com realização de testes e correção de defeitos, durante o período de garantia;

8.12 A cada visita técnica realizada nas dependências da CONTRATANTE a CONTRATADA deverá emitir um relatório de execução das atividades, relacionando os serviços executados;

8.13 A Contratada deverá acompanhar com pessoal in loco os primeiros 5 dias úteis de operação do ambiente em produção;

8.13.1 A critério da CONTRATANTE este acompanhamento poderá ser híbrido (presencial+remoto);

8.14 Prover manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução;

8.15 Os serviços de suporte técnico e garantia abrangem todas as soluções fornecidas pela contratada no âmbito dessa contratação.

8.16 Manutenção preventiva, manutenção corretiva, esclarecimento de dúvidas e reparação de problemas na solução;

8.17 Instalar o agente em todo os computadores/servidores contratados, seja de forma remota ou presencial, dentro do prazo estabelecido neste Termo de Referência.

9 CONFIDENCIALIDADE:

9.1 A CONTRATADA deverá zelar pelo sigilo de quaisquer informações referentes à estrutura, sistemas, usuários, contribuintes, topologia, e ao modo de funcionamento e tratamento das informações da CONTRATANTE, durante e após fim do contrato, salvo se houver autorização expressa da Contratante para divulgação;

9.2 Não haverá nenhum tipo de facilidade de acesso remoto, tão menos envio de forma automática ou controlada de informações (backdoor) originadas de software/hardware contratado ou adquirido sem o conhecimento e formal autorização da Contratante. A não

observância desse fato poderá ser considerada espionagem e será motivo de processo civil e criminal conforme legislação vigente.

10 PENALIDADES

10.1 Caso haja atraso no período de resposta da abertura de um chamado (2 horas), haverá multa de 0,1% por hora de atraso, calculado sobre o contrato;

10.2 Caso o tempo para atendimento de suporte do fabricante ultrapasse as horas, contadas a partir da abertura do chamado, haverá multa de:

10.2.1 Severidade 1: 2% por hora de atraso, calculado sobre o valor mensal do contrato;

10.2.2 Severidade 2: 1% por hora de atraso, calculado sobre o valor mensal do contrato;

10.2.3 Severidade 3: 0,5% por hora de atraso, calculado sobre o valor mensal do contrato;

10.3 Caso o tempo para atendimento de suporte da CONTRATADA ultrapasse as horas, contadas a partir da abertura do chamado, haverá multa de:

10.3.1 Severidade 1: 2% por hora de atraso, calculado sobre o valor mensal do contrato;

10.3.2 Severidade 2: 1% por hora de atraso, calculado sobre o valor mensal do contrato;

10.3.3 Severidade 3: 0,5% por hora de atraso, calculado sobre o valor mensal do contrato;

10.3.4 Severidade 4: 0,1% por hora de atraso, calculado sobre o valor mensal do contrato;

10.4 Caso haja atraso na disponibilização de profissionais para suporte on site, haverá multa de 1% ao dia de atraso, calculado sobre o valor mensal do contrato;

10.5 Caso haja atraso na instalação da solução, haverá multa de 1% ao dia de atraso, calculado sobre o valor do contrato;

10.6 Caso não ocorra a visita semestral estabelecido, haverá multa de 1% ao dia de atraso, calculado sobre o valor do contrato;

11 OBRIGAÇÕES DA CONTRATANTE

11.1 Os serviços da CONTRATANTE deverão abranger:

11.1.1 Prover acesso a rede física ou lógica sob demanda;

11.1.2 Ajustes na rede lógica da Prodam quando necessário;

11.1.3 Prover informações do ambiente de infraestrutura da Prodam para colaborar na solução de problemas.

12 CONDIÇÕES DE FATURAMENTO

12.1 O pagamento das Subscrições será efetuado em parcelas mensais de igual valor, a partir da emissão do termo de aceite pela CONTRATANTE.

12.2 O pagamento dos Serviços de Instalação e Configuração da solução, será efetuado em parcela única, após o termo de aceite da instalação e configuração da solução realizada em cada órgão participante desta Ata, emitido pelo respectivo órgão.

12.3 O pagamento do da Subscrição das Licenças e o Serviço de Suporte e Garantia, será efetuado pago em parcelas mensais de igual valor, a partir da emissão do termo de aceite da instalação e configuração, pela CONTRATANTE.

12.4 O pagamento dos Treinamentos ministrados pela CONTRATADA, será efetuado ao término de cada turma de treinamento.

12.5 Nos preços já estão incluídos todos os custos, eventuais ou não, incidentes direta ou indiretamente sobre o objeto desta contratação.

13 PROPOSTA PARA CONDIÇÕES DE FATURAMENTO

13.1 A Nota Fiscal Eletrônica de Serviços deverá ser emitida e encaminhada à CONTRATANTE, através do setor de Expediente, por meio do endereço eletrônico gfl@prodam.sp.gov.br.

13.1.1 Após o recebimento da Nota Fiscal Eletrônica de Serviços, a CONTRATANTE disporá de até 05 (cinco) dias úteis para emissão do Termo de Aceite, aprovando os serviços prestados.

13.1.2 O pagamento será realizado por intermédio de crédito em conta corrente ou por outra modalidade que possa vir a ser determinada pela Gerência de Planejamento e Controle Financeira (GFP), em 30 (trinta) dias corridos a contar da data de emissão do Termo de Aceite;

13.2 Caso a Nota Fiscal Eletrônica de Serviços contenha divergências com relação ao estabelecido no Instrumento Contratual, a CONTRATANTE ficará obrigada a comunicar a empresa CONTRATADA, formalmente, o motivo da não aprovação no prazo de 05 (cinco) dias úteis. A devolução da Nota Fiscal Eletrônica de Serviços, devidamente, regularizada pela CONTRATADA, deverá ser efetuada em até 05 (cinco) dias úteis da data de comunicação formal realizada pela CONTRATANTE;

13.3 Em caso de atraso de pagamento dos valores devidos à CONTRATADA, mediante requerimento formalizado por esta, incidirão juros moratórios calculados utilizando-se o índice oficial de remuneração básica da caderneta de poupança e de juros simples no mesmo percentual de juros incidentes sobre a caderneta de poupança, para fins de compensação da mora (TR + 0,5% “pro-rata tempore”), observando-se para tanto, o período correspondente à data prevista para o pagamento e aquela data em que o pagamento efetivamente ocorreu.

14 QUALIFICAÇÃO TÉCNICA

14.1 A CONTRATADA deverá apresentar, em seu nome, atestado (s) de capacidade técnica operacional, emitido por pessoa jurídica de direito público ou privado, comprovando a execução de atividade pertinente e compatível em características e quantidades, com o objeto a ser contratado.

14.2 Será considerado o atestado compatível se comprovado no mínimo a execução, e fornecimento de serviço para soluções de segurança composta de solução EDR, de mesma característica descrita neste edital, contemplando ____ licenças , suporte técnico, manutenção e garantia.

14.3 Atestado(s) Técnico(s) deve ser apresentado em papel timbrado, datado e assinado com identificação do atestante (nome, cargo, e-mail e telefone), contendo descrição dos itens e quantidades fornecidas.

14.4 Comprovação de que a LICITANTE possui autorização do fornecedor da solução para comercializar, instalar e prestar suporte no Brasil para o produto especificado. A comprovação deverá ser feita por meio de declaração do fornecedor oficial dos produtos que compõem a solução e destinada a PRODAM e com referência explícita a este processo de aquisição.

14.5 A habilitação da empresa melhor classificada ficará condicionada, ainda, à comprovação das especificações gerais e funcionalidades deste Termo de Referência. Para tanto, deverá executar um Teste de Bancada, disponibilizando-o à CONTRATANTE;

14.6 Caso a licitante não atenda as exigências de habilitação do Teste de Bancada ou qualquer dos documentos de habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que melhor atenda este Edital.

14.7 A licitante melhor classificada deverá prestar apoio e esclarecimentos necessários durante a apresentação e execução do Teste de Bancada, dando subsídios para que a CONTRATANTE possa homologar a solução proposta.

14.8 Teste de Bancada será realizado no endereço da PRODAM – Rua Pedro de Toledo, 983, Vila Clementino, São Paulo, ou em endereço a ser definido pela CONTARTANTE dentro do município de São Paulo, em horário comercial, de segunda a sexta-feira, das 8h às 12h e das 13h às 17h.

14.9 Após a análise da documentação, respeitada a ordem de classificação do certame, o pregoeiro comunicará, via chat, a licitante que atenda ao edital quanto à documentação habilitatória, para que proceda ao agendamento do Teste de Bancada junto à área técnica através do e-mail licitacao@prodam.sp.gov.br, conforme disposto a seguir:

14.10 A empresa convocada via chat na sessão do Pregão, terá 2 dias úteis para agendamento através do e-mail licitacao@prodam.sp.gov.br, sob pena de desclassificação pelo não cumprimento deste prazo;

14.11 O prazo para início do Teste de Bancada não será superior a 5 dias úteis após o agendamento;

14.12 Caso a empresa convocada não atenda os prazos, será considerada desclassificada;

14.13 As demais empresas, interessadas em assistir ao Teste de Bancada terão dois dias úteis para agendamento através do e-mail licitacao@prodam.sp.gov.br, a partir da convocação do pregoeiro à empresa que realizará o teste, indicando até 2 (dois) técnicos ou representantes legais da licitante, devidamente identificados por meio de vínculo contratual ou procuração, como “Técnico de Acompanhamento da Licitante Participante”. O não cumprimento deste prazo, ensejará na queda do direito de assistir à realização do teste;

14.14 Não será permitida a substituição de qualquer Técnico de Acompanhamento da licitante participante sem a autorização prévia da PRODAM;

14.15 Não será permitida a comunicação direta entre qualquer Técnico de Acompanhamento da licitante participante e a Equipe Técnica da

licitante convocada. Qualquer comunicação ou questionamento deve ser dirigido unicamente à Equipe Técnica da PRODAM;

14.16 A não observância dessa regra de comunicação poderá causar o descredenciamento da Equipe Técnica da licitante convocada ou de qualquer técnico de acompanhamento da licitante participante;

14.17 Os testes de bancada deverão atender, no mínimo, aos seguintes requisitos:

14.17.1

ID	Descrição Requisitos	Atende?	Observação
1	**Características da Solução**		
1.1	A gerência de administração da solução deve ser centralizada para gerenciar todos os endpoints, independentemente da localização geográfica destes;		
1.3	A gerência de administração da solução deve ser acessível em qualquer ponto da rede da contratante até mesmo quando estiverem conectados a redes públicas sem a necessidade de uma conexão VPN;		
1.4	A solução deve ser capaz de detectar e bloquear em tempo real ameaças conhecidas e desconhecidas (zero-day), ataques fileless, ameaças avançadas (APTs), Ransomwares, exploits e outros comportamentos maliciosos, sem depender de base de assinaturas ou heurísticas		
1.5	A solução deverá ser baseada em plataforma de nuvem e oferecida como subscrição;		
1.6	A administração deve estar acessível através de HTTPS usando um dos navegadores abaixo:		
1.6.1	Edge;		
1.6.2	Google Chrome;		
1.6.3	Firefox.		
1.7	A administração da solução deverá ser 100% em nuvem sem a necessidade de instalação de ferramenta local para o gerenciamento da solução;		
1.9	Não serão aceitas soluções que utilizem base local de assinaturas, também conhecida como Base de Vacinas, para reconhecer ameaças, mesmo que este seja apenas um dos métodos de detecção da solução;		
1.10	A gerência de administração da solução deve ter capacidade de separar os endpoints gerenciados através de grupos via seleção manual e também a criação de grupos com adição de endpoints de forma automática com base em no mínimo, os critérios abaixo:		
1.10.1	Domínio;		

1.10.2	Endereços IP;		
1.10.3	Endereço de rede (CIDR);		
1.10.4	Hostname parcial ou completo;		
1.10.5	Versão de sistema operacional;		
1.10.6	Unidade Organizacional do Active Directory;		
1.10.7	Versão do agente.		
1.11	A gerência deve permitir aplicação de políticas para grupos de máquinas ou máquinas individuais;		
1.12	Deve ser utilizado um fator de dupla autenticação, para autenticação na gerência de administração da solução;		
1.13	Deve ser possível a definição de perfis (RBAC) para os usuários dentro da gerência de administração da solução delimitando as permissões e/ou acesso as funcionalidades e capacidades disponíveis dentro da plataforma;		
1.14	A gerência de administração da solução deve oferecer suporte Single Sign On com compatibilidade de provedor de identidade (IdP);		
1.15	A gerência de administração da solução deve contemplar, no mínimo, as seguintes visualizações:		
1.15.1	Agentes ativos;		
1.15.2	Agentes por sistema operacional;		
1.15.3	Detecções por objetivo do ataque;		
1.15.4	Detecções por tática do ataque;		
1.15.5	Detecções por severidade do ataque;		
1.15.6	Top 10 de detecções por máquina;		
1.15.7	Top 10 de detecções por usuário.		
1.16	A gerência da solução deve prover auditoria detalhada com, no mínimo, as seguintes ações administrativas:		
1.16.1	Criação de grupos;		
1.16.2	Adição de exclusões;		
1.16.3	Autenticação por SSO;		
1.16.4	Autenticação de usuário;		
1.16.5	Autenticação de dois fatores;		
1.16.6	Troca de senha da interface de gerenciamento;		
1.16.7	Criação de usuários;		
1.16.8	Deletar grupos;		
1.16.9	Deletar políticas;		
1.16.10	Revelar senha para desinstalação;		
1.16.11	Iniciar isolamento de rede;		
1.16.12	Atualizar permissões de usuário;		
1.17	A administração da solução deve ser feita de forma centralizada, totalmente integrada e de um único fabricante. A visibilidade de ameaças (detecções ou incidentes) deve ser unificada, permitindo o diagnóstico e remediação das ameaças em toda a planta protegida;		

1.18	As políticas de instalação (rollout) devem ser capazes de atualizar os agentes de forma automática considerando no mínimo as seguintes opções:		
1.18.1	Versão mais recente;		
1.18.2	Versão específica;		
1.18.3	Uma versão anterior a mais recente (N-1);		
1.18.4	Duas versões anteriores a mais recente (N-2).		
2	**Características dos Agentes ou Sensores**		
2.1	A solução deve possuir apenas um único software agente, ou sensor, instalado em cada dispositivo de computação (microcomputador ou servidor) para prover todas as funcionalidades descritas neste documento e que serão administradas através da conexão com a gerência de administração da solução. Não será aceita a instalação de componentes adicionais como agentes de comunicação com múltiplos subagentes, plug-ins e softwares de terceiros para o atendimento dos requisitos;		
2.2	O agente deve suportar os seguintes sistemas operacionais:		
2.2.1	Windows: Windows Server 2019; Windows Server 2016; Windows Server 2012 e 2012 R2; Windows 2008 R2; Windows 7 SP1; Windows 10; e versões superiores;		
2.2.2	Linux: CentOS 7.4 – 8.5, Oracle Linux 7, 7.9 e 8; Red Hat Enterprise Linux (RHEL) 7.4 – 8.0; SUSE Linux Enterprise 12.2 – 12.5 e 15.3; Ubuntu 16.04 LTS; Ubuntu 18.04, Ubuntu 20.04; e versões superiores.		
2.3	A comunicação entre os agentes e a gerência de administração da solução deve utilizar um túnel de segurança TLS criptografado utilizando certificate pinning;		
2.4	O agente deve suportar comunicação com a gerência de administração da solução através de proxy.		
2.5	A capacidade de AV, ou NGAV, deve estar completamente operacional após instalação do agente no endpoint, sem a necessidade de reinicialização do sistema operacional.		
3	**Características específicas para sistemas operacionais Windows**		
3.1	O agente deve implementar proteção de desinstalação através de senha ou token específica para cada endpoint gerenciado.		
3.2	O agente deve conter mecanismos que garantam que seu funcionamento não possa ser interrompido por usuários sem privilégios administrativos;		
3.3	Deve detectar tentativas de manipulação indevida dos componentes do agente;		
3.4	A solução deve incorporar técnicas de aprendizado de máquina (Machine Learning) para detecção e prevenção de ataques;		

3.5	Os motores de ML (Machine Learning) devem realizar a detecção e prevenção de artefatos maliciosos conhecidos e desconhecidos não somente na tentativa de execução, como também na tentativa de escrita do binário em disco, ou seja, se um binário considerado malicioso pelo motor de ML for escrito em disco deverá resultar em uma detecção e prevenção no momento da operação de escrita em disco.		
3.5.1	Caso seja configurado para bloqueio o arquivo deverá ser quarentenado.		
3.5.2	O motor de machine learning dessa capacidade deverá respeitar os níveis de sensibilidade configurados.		
3.6	A solução deve permitir níveis de sensibilidade diferentes para detecção e prevenção de ataques através do componente de aprendizado de máquina;		
3.7	Deve ser capaz de detectar Adware e programas potencialmente indesejados;		
3.8	Deve ser capaz de detectar ameaças mesmo que o endpoint não esteja conectado à Internet;		
3.9	Deve efetuar bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos;		
3.10	Deve efetuar bloqueio de scripts e comandos em PowerShell considerados suspeitos;		
3.11	Deve efetuar bloqueio automático de processos suspeitos;		
3.12	Deve efetuar bloqueio baseado em análise do centro de inteligência do fabricante;		
3.13	Deve efetuar bloqueio de operações em registros suspeitos;		
3.14	Deve garantir que arquivos maliciosos sejam movidos para uma área de quarentena;		
3.15	Deve possuir integração com o Windows Security Center para ser reconhecido como uma solução de proteção válida para antimalware;		
3.16	Deve ser capaz de forçar a utilização de ASLR, de modo a mitigar ataques que exploram corrupção de memória;		
3.17	Deve ser capaz de forçar Data Execution Prevention de forma a impedir ataques que utilizem espaço de memória para execução de códigos em região de memória não executável;		
3.18	Deve ser capaz de impedir ataques que utilizem a técnica de Heap Spray Preallocation;		
3.19	Deve ser capaz de impedir ataques que sobrescrevam SEH (Structured Exception Handling);		
3.20	Deve ser capaz de impedir ataques que explorem vulnerabilidades causadas por ponteiros nulos;		

3.21	Deve ser capaz de detectar malwares do tipo Ransomware com base em, no mínimo, os comportamentos abaixo: a) Deletar backups; b) Operações em excesso ao sistema de arquivos; c) Criptografia de arquivos; d) Processos associados a malwares de ransomware tais como: Cryptowall, Wannacry, Locky;		
3.22	Deve ser capaz de detectar exploração baseado em, no mínimo, os seguintes comportamentos: a) Criação de processos suspeitos originados de navegadores; b) Detecção de comprometimento de servidores Web através de webshell; c) Detecção de arquivos suspeitos baixados ou escritos por um navegador que iniciaram a sua execução; d) Injeção de código não esperada de um processo a outro; e) Execução de Java Script através do executável Rundll32.		
3.23	Deve ser capaz de detectar movimentação lateral através de circunvenção do processo de logon do Windows;		
3.24	Deve ser capaz de detectar processos que tentam obter credenciais de login;		
3.25	Deve prover recursos para que administradores possam executar ações de remediação remotamente, sem necessidade ou integração com soluções de terceiros e sem a instalação de softwares adicionais no endpoint gerenciado;		
3.26	Deve efetuar exclusão de arquivos e pastas utilizando caracteres coringa (Wildcard);		
3.27	Deve bloquear a execução conforme definição granular de no mínimo, os seguintes comandos de alto risco sendo executados de forma remota no endpoint via gerência de administração da solução: a) Extração de arquivos; b) Envio de arquivos para um repositório externo; c) Iniciar execução de um processo; d) Dump de memória do endpoint; e) Dump de memória de um processo específico no endpoint		
3.28	Deve permitir que scripts PowerShell possam ser adicionados à solução para que possam ser executados remotamente em resposta à um incidente de segurança;		
3.29	Deve permitir que o acesso remoto seja desabilitado globalmente em endpoints específicos;		
3.30	Deve implementar permissões específicas de forma a impedir que o acesso remoto esteja disponível somente para usuários específicos;		

3.31	Deve permitir que administradores possam interromper ou bloquear tráfego de rede de endpoints classificados como comprometidos. O tráfego deve ser restrito somente com a gerência de administração da solução para efetuar análise e diagnóstico aprofundado, e posteriormente readmitir o endpoint quando ele estiver saneado;		
3.32	A solução deve prover a capacidade de adição de endereços específicos para mesmo quando o endpoint esteja em quarentena sejam alcançáveis, ou seja, quando houver o isolamento do endpoint o mesmo deverá ter a possibilidade de comunicar com endereços especificados em política ademais da comunicação com a gerência de administração da solução;		
3.33	A solução deve permitir que a proteção de dispositivos seja habilitada em modos de detecção somente, sem bloqueio efetivo;		
3.34	Deve permitir bloqueio de dispositivos USB baseado em, no mínimo, as seguintes classes de dispositivo: a) Dispositivos de imagem; b) Dispositivos de áudio e vídeo; c) Dispositivos de armazenamento em massa; d) Dispositivos móveis (MTP/PTP); e) Impressoras; f) Adaptadores de rede wireless.		
3.35	Para dispositivos de armazenamento em massa, deve permitir acesso granular com no mínimo, as seguintes permissões: a) Leitura somente; b) Escrita e leitura; c) Escrita leitura e execução; d) Bloqueio total.		
3.36	A proteção de dispositivos deve permitir exceções baseadas no Vendor ID e Product ID, número serial e classe;		
3.37	Deve permitir a criação de regras, grupos de regras e políticas de firewall para definir com precisão qual tráfego de rede é permitido e bloqueado no host;		
3.38	A política de firewall deve permitir a utilização de múltiplas regras de firewall;		
3.39	As regras de firewall devem ser agrupáveis, ou seja, as regras de firewall utilizadas em uma política devem ser configuradas de forma a ser possível de selecionar um grupo de regras a serem usadas em uma política;		
3.40	Deve ser possível a configuração de regras de firewall em modo observação, gerando assim registros de qual seria a ação/impacto caso a regra fosse aplicada;		
3.41	As regras dentro de um grupo podem ser habilitadas ou desabilitadas de forma independente.		
4	**Características específicas para sistemas operacionais Linux**		

4.1	Deve incorporar técnicas de aprendizado de máquina (Machine Learning) para detecção e prevenção de ataques;		
4.2	Deve suportar níveis de sensibilidade diferentes para detecção e prevenção de ataques através do componente de aprendizado de máquina;		
4.3	Deve suportar níveis de sensibilidade diferentes para detecção de ataques através do componente de aprendizado de máquina;		
4.4	Deve efetuar bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos;		
4.5	Deve prover recursos para que administradores possam executar ações de remediação remotamente, sem necessidade ou integração com soluções de terceiros e sem a instalação de softwares adicionais no endpoint gerenciado;		
4.6	Deve bloquear a execução conforme definição granular de no mínimo, os seguintes comandos de alto risco sendo executados de forma remota no endpoint via gerência de administração da solução:		
4.6.1	Extração de arquivos;		
4.6.2	Envio de arquivos para um repositório externo;		
4.6.3	Iniciar execução de um processo.		
4.7	Deve permitir que scripts bash possam ser adicionados à solução para que possam ser executados remotamente em resposta a um incidente de segurança. Deve permitir que administradores possam interromper ou bloquear tráfego de rede de endpoints classificados como comprometidos. O tráfego deve ser restrito somente com a gerência de administração da solução, para efetuar análise e diagnóstico aprofundando, e posteriormente readmitir o endpoint quando ele estiver saneado;		
5	**Relatórios e Dashboard**		
5.1	A solução deverá prover Dashboard trazendo as detecções mais recentes, número de novas detecções e detecções por táticas nos últimos 30 dias.		
5.2	A plataforma deverá ter a capacidade de reportar as detecções de forma agrupada tendo como opções de agrupamento no mínimo os seguintes critérios: a. Por máquina; b. Por tática; c. Por técnica; d. Por Severidade.		
5.3	A plataforma deverá ter a capacidade de reportar as detecções, permitindo organizar com a mais recente no topo, ou a mais antiga no topo.		

5.4	A plataforma deverá ter a capacidade de reportar as deteções, permitindo filtrar minimamente com base aos seguintes filtros: a. Severidade; b. Tática; c. Técnica; d. Usuário; e. Host; f. Tipo de sistema operacional; g. Versão do sistema operacional; h. Última hora; i. Último dia; j. Última semana; k. Últimos 30 dias; l. Nome de arquivo; m. Hash do processo.		
5.5	A solução deve prover a capacidade de visibilidade da solução em dispositivos de computação (microcomputadores e servidores), contendo minimamente as seguintes informações que não deverão ser passiveis de exclusão ou limpeza, garantindo assim o não-repúdio: a) Login do administrador/operador que realizou a operação; b) Nome do endpoint; c) Duração da sessão; d) Data e hora do início da sessão; e) Arquivos copiados desde a máquina; f) Comandos executados na máquina; g) Caminho completo do arquivo copiado da máquina; h) Data e hora de cada comando executado.		
5.6	A plataforma deverá gerar relatório das máquinas contendo minimamente as seguintes informações, podendo ser exportada em CSV: a) Hostname; b) Data e hora da primeira comunicação; c) Data e hora da última comunicação; d) Versão do sistema operacional; e) Modelo; f) Tipo; g) Unidade organizacional (OU); h) Site; i) Política de proteção aplicada; j) Política de resposta aplicada; k) Política de atualização aplicada; l) Política de controle de dispositivos USB aplicada; m) Política de firewall aplicada; n) Identificação do host (UID/GUID); o) IP local da máquina; p) IP público da máquina; q) MAC Address; r) Versão do sensor/agente instalado.		

5.7	A solução deve prover a capacidade de visibilidade em dispositivos de computação (microcomputadores e servidores) em síntese de ativos e políticas, contendo minimamente as seguintes informações: a) Domínio; b) Grupo; c) Identificação do host (UID/GUID); d) Hostname; e) IP local da máquina; f) MAC Address; g) Subnet da máquina; h) Versão do sistema operacional; i) Unidade organizacional (OU); j) Plataforma; k) Política de proteção aplicada; l) Política de resposta aplicada; m) Política de atualização aplicada; n) Versão do sensor/agente instalado.		
5.8	A solução deve prover a capacidade de visibilidade da solução em dispositivos de computação (microcomputadores e servidores) em síntese de ativos, contendo minimamente as seguintes informações: a) Total de hosts vistos nas últimas 24 horas; b) Total de estações vistos nas últimas 24 horas; c) Total de servidores vistos nas últimas 24 horas; d) Hosts comunicando na última hora; e) Hosts off-line; f) Hosts isolados/quarentenados; g) Hosts com sensor sem proteção para desinstalação; h) Total de máquinas em cada política de proteção; i) Total de máquinas em cada política de resposta; j) Total de máquinas em cada política de atualização do sensor; k) Total de máquinas em cada política de controle USB.		
6	**Investigação e detecção de ameaças**		
6.1	A solução deve ser composta de módulo de software com serviço gerenciado de detecção de adversários infiltrados no ambiente e acionamento imediato do cliente via gerência de administração da solução;		
6.2	O Serviço deve analisar campanhas de malwares e de incidentes gerados na gerência de administração da solução;		
6.3	O serviço deve fornecer notas explicativas ou recomendações para remediação baseado nas atividades encontradas;		
6.4	A solução deve notificar os incidentes por e-mail ou gerência de administração da solução;		
6.5	Capacidade de processamento de dados massivos em busca de atividades maliciosas;		

6.6	Capacidade de reportar informações referentes ao incidente na própria gerência de administração da solução;		
7	**Capacidades de inteligência de ameaças**		
7.1	A Ferramenta deverá monitorar ameaças e contextos políticos e globais que possam influenciar na incidência de ataques de cibersegurança;		
7.2	A inteligência de ameaças deve mapear atores maliciosos e dar visibilidade de países e indústrias alvo, pais de origem e última atividade;		
7.3	Para atores maliciosos, o serviço de inteligência deve fornecer, quando aplicável, informações tais como vulnerabilidades utilizadas, métodos de instalação, ações e objetivos, métodos de entrega e breve descrição do grupo;		
7.4	Deve associar, quando pertinente, detecções presentes no ambiente aos atores maliciosos;		
8	**Capacidades de emulação de execução de código**		
8.1	A solução deve prover, integrada à gerência de administração da solução, capacidades de emulação de execução de arquivos, sem instalação de componentes adicionais ou softwares de terceiros;		
8.2	Deve se integrar ao agente instalado em endpoints para permitir que arquivos suspeitos sejam enviados de forma automática ao serviço de emulação de execução;		
8.3	A solução deve emular execução, no mínimo, nos seguintes sistemas operacionais: a) Windows 10, Windows 2012 e superiores; b) LINUX Ubuntu; Hed Rat; CentOS e superiores;		
8.4	A solução deve incluir na análise de execução, no mínimo, as seguintes características: a) Táticas e técnicas de acordo como modelo de ameaças MITRE ATT&CK; b) Características comportamentais suspeitas; c) Imagens de execução, quando aplicável; d) Detalhes do arquivo como nome, hash, tamanho, tipo; e) Atividade de rede incluindo conexões, endereços IP de destino, domínios, portas; f) Leitura e escrita de arquivos em disco; g) Leitura e alteração de chaves de registro; h) Detalhes de processos iniciados durante a execução.		
9	**Capacidades de detecção, visibilidade e investigação**		

9.1	As informações de telemetria dos incidentes e ações ocorridas nos endpoints deverão estar disponíveis na gerência de administração da solução independentemente do status operacional dos endpoints, ou seja, caso o endpoint esteja inoperante, a investigação dos incidentes e eventos deverá ser possível;		
9.2	A solução deve ser capaz de coletar e enviar à gerência de administração da solução os dados de telemetria das ações realizadas nos endpoints incluindo, no mínimo, as seguintes atividades: a) Endereços de rede obtidos; b) Login de usuários; c) Informações de sistema operacional, modelo e última atividade; d) Número de executáveis únicos; e) Processos que foram executados; f) Utilização de ferramentas administrativas; g) Requisições DNS; h) Conexões de rede incluindo portas e processos associados; i) Arquivos compactados escritos; j) Scripts escritos em disco; k) Mapa de geolocalização de conexões de rede.		
9.3	Deve permitir visibilidade sobre parâmetros de execução de um processo;		
9.4	A solução deve permitir busca dos metadados coletados através de sintaxes que filtrem a busca, concatenando critérios;		
9.5	Deve permitir a busca por hashes MD5 e SHA256;		
9.6	Deve permitir buscas por nomes de arquivo;		
9.7	Deve permitir a busca por atividades de usuário;		
9.8	Deve permitir extração de dados em formato CSV e JSON.		
10	**Gerenciamento de vulnerabilidades**		
10.1	A solução deverá identificar vulnerabilidades em hosts Windows, macOS e Linux, incluindo vulnerabilidades do sistema operacional e de aplicações comuns.		
10.2	As vulnerabilidades identificadas deverão mostrar sua severidade usando não apenas conforme definido pelo Common Vulnerability Scoring System (CVSS) v2 e v3, mas também deverá contemplar definição de severidade com base em modelo de inteligência artificial composto de ao menos três componentes:		
10.3	Múltiplas origens de dados, tais como: CVSS, inteligência de ameaças, idade das vulnerabilidades, entre outras;		
10.4	Atualização continua, onde o modelo poderá atualizar as severidades e predizer as ameaças durante atualizações regulares;		
10.5	Transparência do modelo, trazendo assim visibilidade de quais fatores levados em conta, para a avaliação de risco, foram usados;		

10.6	Além de permitir a criação de dashboards personalizados, deverá contemplar ao menos um dashboard inicial contendo as seguintes informações:		
10.6.1	Total de vulnerabilidades presentes no ambiente;		
10.6.2	Principais remediações recomendadas para o ambiente;		
10.6.3	Lista de hosts mais vulneráveis presentes no ambiente;		
10.6.4	Lista de produtos mais vulneráveis presentes no ambiente;		
10.6.5	Quantidade de vulnerabilidades abertas e fechadas por dia;		
10.6.6	Hosts com detecções críticas ou altas nos últimos 90 dias;		
10.7	A solução deverá permitir a criação de regras de supressão, a fim de permitir filtrar vulnerabilidades que ficarão fora do escopo de correção e controle.		
10.8	As regras de supressão deverão permitir ao menos o uso dos seguintes filtros:		
10.8.1	CVE ID: Identificador de Vulnerabilidades e Exposições Comuns (CVE) de uma vulnerabilidade;		
10.8.2	Grupo: nome do grupo de hosts;		
10.8.3	ID do host: identificador exclusivo de um host;		
10.8.4	Nome do host: nome de um host;		
10.8.5	IP/CIDR local: IP do host ou endereço CIDR de um host;		
10.8.6	Produto: Aplicativo ou sistema operacional (SO) instalado em um host;		
10.8.7	Versão do produto: Versão de um produto instalado;		
10.8.8	Tags: Marcações definidas para um host;		
10.8.9	Fabricante e produto: Produto, incluindo o nome do fabricante, instalado em um host;		
10.9	A regra de supressão deverá permitir declarar uma razão para as vulnerabilidades que serão filtradas, permitindo ao menos as seguintes razões:		
10.9.1	Aceite de risco;		
10.9.2	Controle compensatório;		
10.9.3	Falso positivo;		
10.10	Deverá ser possível saber o número de vulnerabilidades suprimidas por uma regra;		
10.11	Deve ser possível a criação de uma regra de supressão a partir dos detalhes de visualização de uma vulnerabilidade;		
10.12	A solução deve permitir a identificação de hosts com patches pendentes que exigem uma reinicialização;		
10.13	A solução deve mostrar patches já instalados nos hosts;		

10.14	A solução deverá monitorar continuamente o host permitindo a detecção de quando um update ou uma aplicação é instalada;		
10.15	Para atualizações de segurança do sistema operacional Windows, a solução deverá permitir via botão na console acionar o Windows Update para que instale o KB em questão;		
10.16	Deverá fornecer o status do exploit de uma vulnerabilidade com ao menos os seguintes status:		
10.16.1	Não provado;		
10.16.2	Disponível;		
10.16.3	Fácil acesso;		
10.16.4	Usado ativamente;		
11	**Inventário de ativos, usuários e aplicações**		
11.1	A solução deverá permitir encontrar ativos potencialmente desatualizados ou suspeitos em sua rede, mesmo que eles não tenham a tecnologia em questão instalada, permitindo assim expandir a cobertura do sensor para ativos corporativos não gerenciados;		
11.2	Deverá permitir o acompanhamento das alterações de senha e a atividade de login junto com o uso de outras contas;		
11.3	A solução deverá obter informações sobre o uso de aplicativos, por exemplo, os aplicativos que estão instalados—incluindo onde e quem os está usando—para orientar decisões sobre quais manter e quais desinstalar.		
11.4	O monitoramento de dispositivos deverá trazer ao menos os seguintes controles:		
11.4.1	Visualizar os ativos que foram adicionados ou removidos;		
11.4.2	Localizar novos ativos sem presença do sensor;		
11.4.3	Mapear relacionamentos entre ativos gerenciados;		
11.4.4	Revisar o status de criptografia de disco;		
11.4.5	Acompanhar o uso de recursos do sistema ao longo do tempo;		
11.5	O monitoramento de credencias deverá trazer ao menos os seguintes controles:		
11.5.1	Monitorar o uso de credenciais e quais ativos eles estão acessando;		
11.5.2	Acompanhe se as credenciais de domínio ou locais são usadas;		
11.5.3	Ver quando as senhas foram alteradas pela última vez;		
11.5.4	Monitorar a atividade de login bem-sucedida e com falha;		
11.6	O monitoramento de aplicações deverá trazer ao menos os seguintes controles:		
11.6.1	Rastrear aplicativos instalados;		
11.6.2	Listar quais máquinas estão;		

11.7	O monitoramento de dispositivos deverá filtrar em ao menos três categorias os dispositivos encontrados, sendo elas:		
11.7.1	Ativo gerenciado: Um ativo que possui a solução instalada;		
11.7.2	Ativo não gerenciado: um ativo que poderia ter a solução instalada;		
11.7.3	Ativo não suportado: um ativo que não pode ter a solução instalada;		
12	**Suporte especializado do fabricante das soluções**		
12.1	Possuir portal de suporte para abertura de chamados, acesso a base de conhecimento;		
12.2	O suporte deverá atender via telefone em escala 24x7x365;		
12.3	O suporte deverá prover minimamente os seguintes canais de comunicação para abertura de chamados: a) Chat; b) Portal web.		

15 PRAZO DE ENTREGA

15.1 O prazo para entrega da CONTRATADA de toda infraestrutura para o módulo de gerenciamento centralizado do EDR deve ocorrer em até 30 dias após a assinatura do contrato;

15.2 O prazo para entrega da CONTRATADA do planejamento de implementação das _____ licenças de EDR é de 25 dias da assinatura do contrato e a CONTRATANTE tem 5 (cinco) dias para dar o aceite no projeto;

15.3 Prazos para implementação das soluções:

15.3.1 Entenda-se como implementação:

15.3.1.1 A instalação da solução de EDR contratada em cada estação de trabalho e Servidores medidos a partir do início do planejamento do projeto, levantamento de requisitos, descrito neste documento;

15.3.1.2 Identificação destas estações de trabalho e Servidores no gerenciamento do EDR contratado;

15.3.1.3 Identificação destes agentes gerenciados com as respectivas atualizações.

15.3.2 Para estações de trabalho e servidores:

15.3.2.1 A CONTRATADA terá 120 (cento e vinte) dias, após a assinatura do contrato, para a implementação de 100% da instalação de todas as estações de trabalho e servidores previstos no planejamento, levantamento de requisitos, descrito neste documento;

15.3.3 Entrega das licenças contratadas em 30 dias após assinatura do contrato;

15.3.4 O prazo para início da Operação Assistida será a partir da primeira data de implementação da solução, imediato a assinatura do contrato;

15.3.5 Treinamento/capacitação, iniciando em até 45 dias após assinatura do contrato, ou negociado a critério da CONTRATANTE.

16 ACEITE

16.1 Após a instalação e configuração, a equipe técnica da PRODAM emitirá o “Termo de Aceite de Instalação e Configuração” em até 5 (cinco) dias úteis após a formalização pela CONTRATADA da finalização do processo da instalação/configuração (operação) da solução e confirmação que todos os quesitos estão sendo cumpridos conforme o Edital.

16.1.1 Entende-se pela instalação e configuração a disponibilização de todas as licenças contratadas, instaladas nos equipamentos descritos no planejamento inicial, devidamente identificadas pela solução de gerenciamento.

16.2 Após a finalização dos ____ treinamentos, a equipe técnica da PRODAM emitirá o “Termo de Aceite de Conclusão de Treinamento” em até 5 (cinco) dias úteis após a formalização pela CONTRATADA da finalização do processo de treinamento e confirmação que todos os quesitos foram cumpridos conforme o Edital.

16.2.1 Caso o treinamento fornecido não esteja de acordo com o que foi especificado nos itens 4 e 5, o Termo de Aceite de Conclusão de Treinamento não será emitido, devendo a CONTRATADA fornecer novo treinamento que contemple todos os requisitos necessários;

16.2.2 Caso o certificado de conclusão do treinamento fornecido não seja emitido de acordo com o que foi especificado nos itens 4 e 5 o Termo de Aceite de Conclusão de Treinamento não será emitido, devendo a CONTRATADA providenciar sua emissão;

São Paulo, 31 de outubro de 2022.

Wagner Kanagusuko

Gerência de Segurança Operacional de Tecnologia – GIT

ANEXO II

MODELO REFERENTE A VISITA TÉCNICA

CERTIFICADO DE REALIZAÇÃO DE VISITA TÉCNICA

(emitido pela Unidade Compradora)

REF.: PE n.º _____/2020

ATESTO que o representante legal do licitante _____, interessado em participar do Pregão Eletrônico nº ___/___, Processo n° ___/___, realizou nesta data visita técnica nas instalações do _____, recebendo assim todas as informações e subsídios necessários para a elaboração da sua proposta.

O licitante está ciente desde já que, em conformidade com o estabelecido no Edital, não poderá pleitear em nenhuma hipótese modificações nos preços, prazos ou condições ajustadas, tampouco alegar quaisquer prejuízos ou reivindicar quaisquer benefícios sob a invocação de insuficiência de dados ou informações sobre os locais em que serão executados os serviços.

(local e data)

_____	_____
(nome completo, assinatura e qualificação do representante da licitante)	(nome completo, assinatura e cargo do servidor responsável por acompanhar a visita)

ANEXO III

DECLARAÇÃO DE RENÚNCIA A VISITA TÉCNICA

(Papel Timbrado do Licitante)

REF.: PE n.º _____/2020

Eu, _____, portador do RG nº _____ e do CPF nº_____, na condição de representante legal de _____ (*nome empresarial*), interessado em participar do Pregão Eletrônico nº ___/___, Processo n° ___/___, **DECLARO** que o licitante não realizou a visita técnica prevista no Edital e que, mesmo ciente da possibilidade de fazê-la e dos riscos e consequências envolvidos, optou por formular a proposta sem realizar a visita técnica que lhe havia sido facultada.

O licitante está ciente desde já que, em conformidade com o estabelecido no Edital, não poderá pleitear em nenhuma hipótese modificações nos preços, prazos ou condições ajustadas, tampouco alegar quaisquer prejuízos ou reivindicar quaisquer benefícios sob a invocação de insuficiência de dados ou informações sobre os locais em que serão executados os serviços.

(Local e data)

_____

(nome completo, assinatura e qualificação do proposto da licitante)

TERMO DE ACEITE DE PAGAMENTO

CONTRATADA: <nome completo da empresa contratada>

CONTRATO: <número do contrato>

OBJETO: <breve definição do objeto de contratação>

ATESTAMOS, para os devidos fins, que a empresa <**nome da empresa**>, procedeu com a prestação dos serviços de <**apontar os serviços prestados**>, discriminados na Nota Fiscal de Serviços n.º <inserir número>, emitida em __ / __ / 20__, referente ao <inserir o número do CO-00.00/000, <**dentro ou fora**> do prazo previsto, não havendo em nossos registros nenhum fato que desabone a conduta da empresa, respeitando as formalidades legais e cautelas de estilo, motivo pelo qual assinamos o presente termo.

São Paulo,..... de..... de 20__.

NOME DO GESTOR DA CONTRATAÇÃO	**NOME DO FISCAL DA CONTRATAÇÃO**
Cargo ou Função	Cargo ou Função
Gerência <detalhar> (XXX)	Gerência <detalhar> (XXX)

TERMO DE ACEITE DE ENTREGA DA SOLUÇÃO

CONTRATADA: <nome completo da empresa contratada>

CONTRATO: <número do contrato>

ORDEM DE SERVIÇO Nº: <número da Ordem de Serviço>

OBJETO: <breve definição do objeto de contratação>

A documentação gerada pela empresa <CONTRATADA> e elencada como produtos entregues do período de __/__/____ até __/__/____ no documento “Confirmação de recebimento de produtos”, parte integrante deste processo, estão disponíveis para consulta e/ou reprodução a qualquer momento no servidor corporativo da PRODAM, identificado no link a seguir:
Todos os produtos foram entregues à equipe de projeto da PRODAM e constam da documentação do sistema atualizada.

Através deste documento, a PRODAM formaliza o recebimento dos itens listados previstos em contrato para o referido período e também atesta que nada consta contra qualidade dos itens apresentados, confirmando-se assim a entrega da versão final e consequente autorização do faturamento do período em questão deste contrato e ordem de serviço.

São Paulo, __ de _____ de 20__.

NOME DO GESTOR DA CONTRATAÇÃO	**NOME DO FISCAL DA CONTRATAÇÃO**
Cargo ou Função	Cargo ou Função
Gerência <detalhar> (XXX)	Gerência <detalhar> (XXX)

TERMO DE ACEITE DE CONCLUSÃO DE TREINAMENTO

CONTRATADA: <nome completo da empresa contratada>

CONTRATO: <número do contrato>

ORDEM DE SERVIÇO Nº: <número da Ordem de Serviço>

OBJETO: <breve definição do objeto de contratação>

ATESTAMOS, para os devidos fins, que a empresa <**nome da empresa**>, procedeu com a prestação dos serviços de TREINAMENTO, discriminados na Nota Fiscal de Serviços n.º <inserir número>, emitida em __ / __ / 20__, referente ao <inserir o número do CO-00.00/000, <**dentro ou fora**> do prazo previsto.

Através deste documento, a PRODAM formaliza o recebimento dos itens listados previstos em contrato para o referido período e também atesta que nada consta contra qualidade dos itens apresentados, confirmando-se assim a entrega final e consequente autorização do faturamento em questão deste contrato e ordem de serviço.

São Paulo, __ de _____ de 20__.

NOME DO GESTOR DA CONTRATAÇÃO	**NOME DO FISCAL DA CONTRATAÇÃO**
Cargo ou Função	Cargo ou Função
Gerência <detalhar> (XXX)	Gerência <detalhar> (XXX)

TERMO DE ACEITE DE INSTALAÇÃO E CONFIGURAÇÃO

CONTRATADA: <nome completo da empresa contratada>

CONTRATO: <número do contrato>

ORDEM DE SERVIÇO Nº: <número da Ordem de Serviço>

OBJETO: <breve definição do objeto de contratação>

Através deste documento, a PRODAM formaliza a conclusão da instalação da solução prevista no objeto do referido contrato e atesta que nada consta contra qualidade dos serviços prestados, confirmando-se assim a entrega final da instalação e configuração, caracterizando assim, o início da validade das licenças fornecidas.

São Paulo, __ de _____ de 20__.

NOME DO GESTOR DA CONTRATAÇÃO	**NOME DO FISCAL DA CONTRATAÇÃO**
Cargo ou Função	Cargo ou Função
Gerência <detalhar> (XXX)	Gerência <detalhar> (XXX)