

Nota Técnica nº 114/2026/Diinf/Ctinf-Inmetro

INMETRO/SEI/NÚMERO DO PROTOCOLO
0052600.010616/2025-90Assunto: **ANEXO I - Especificações Técnicas do item 1 - Proteção de Endpoints (EDR).**

1. REQUISITOS GERAIS DE ARQUITETURA E DO AGENTE, QUANTIDADES E SUPORTE TÉCNICO

1.1. Requisitos Gerais de Arquitetura e do Agente

1.2. O fabricante da solução deverá possuir e operar infraestrutura própria de inteligência de ameaças (Threat Intelligence), com laboratório de pesquisa ativo, publicação documentada de relatórios de ameaças e telemetria global, sem depender exclusivamente de feeds de terceiros.

1.3. A comunicação entre os agentes e o console deverá ser criptografada de ponta a ponta (HTTPS/TLS 1.2 ou superior).

1.4. A solução deverá ser capaz de identificar automaticamente dispositivos pertencentes aos domínios da CONTRATANTE que não estejam sendo gerenciados ou que não possuam o agente de proteção instalado, seja por meio de varredura ativa da rede ou por meio de integração com sensores de descoberta. Deverá ainda verificar a presença do software de proteção nos dispositivos identificados e, caso esteja ausente, realizar sua instalação automática por meio do console de gerenciamento ou de mecanismos de implantação centralizada, tais como GPO (Group Policy Object) ou scripts de login, sem necessidade de intervenção do usuário.

1.5. A solução deverá prover proteção por meio de um agente de proteção único e integrado, responsável por todas as funcionalidades, incluindo as de prevenção, detecção e resposta a ameaças

1.6. O agente de proteção deverá operar com baixo impacto no desempenho dos dispositivos, sem ocasionar degradação significativa no uso normal das estações de trabalho e dos servidores.

1.7. O agente deverá operar nativamente, sem necessidade de mecanismos de emulação ou de camadas adicionais de compatibilidade, suportando ambientes físicos, virtualizados e na nuvem pública (ex.: AWS e Microsoft Azure).

1.8. A solução deverá ser compatível com os sistemas operacionais utilizados em estações de trabalho e servidores de rede, incluindo: Microsoft Windows (*Desktop 7 ou superior e Windows Server 2008 R2 ou superior*), macOS (versões ativamente suportadas pelo fabricante), distribuições Linux corporativas, como Red Hat, SUSE Enterprise Linux, CentOS, Debian e Ubuntu LTS (ou equivalentes). A solução deve ser compatível com a execução nativa nos processadores Apple Silicon (arquitetura ARM), não sendo aceitas soluções que dependam exclusivamente de emulação (ex.: via Rosetta 2).

1.9. A solução deverá permitir a instalação do agente por meio de download seguro na interface de administração, por links enviados por e-mail e por mecanismos automatizados de implantação em massa (tais como políticas de grupo – GPO, integração com diretórios como Active Directory/LDAP e scripts de login). A instalação do software cliente deverá ser realizada de forma silenciosa (sem interação do usuário) e sem necessidade de reinicialização (boot) dos endpoints. Além disso:

1.9.1. O agente deverá possuir um mecanismo de autoproteção contra desinstalação, alteração ou desativação não autorizadas, inclusive por administradores locais do sistema operacional. É vedada a utilização de senhas globais compartilhadas para desinstalação; a autorização deve ocorrer de forma individualizada ou centralizada pelo console.

1.9.2. Não será admitida a necessidade de edição manual de roteiros lógicos ou de arquivos de configuração externos pela CONTRATANTE para a operação e o uso dos recursos da solução.

1.9.3. Quantidades

1.9.4. A solução deverá contemplar a proteção de até 1.905 (mil novecentos e cinco) ativos durante 36 (trinta e seis) meses, distribuídos da seguinte forma: 350 (trezentas e cinquenta) estações de trabalho com sistema operacional Windows 7, 1.450 (mil quatrocentas e cinquenta) estações de trabalho com sistema operacional Windows 10 ou superior, 30 (trinta) servidores com sistema operacional Windows Server 2008 R2 e Windows Server 2012 R2 e 75 (setenta e cinco) servidores com sistema operacional Windows Server 2016 ou superior. Em hipótese alguma, a solução poderá ter seu funcionamento interrompido, limitado ou degradado em razão do atingimento do quantitativo licenciado, devendo manter integralmente suas funcionalidades, mesmo em cenários de variação do parque de ativos.

1.9.5. **Serviço de Suporte Técnico**

1.9.6. As subscrições deverão contemplar, durante o período de validade (36 meses), o serviço de suporte técnico ofertado diretamente pelo fabricante da solução, disponível 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, incluindo feriados, para atendimento a incidentes, dúvidas e problemas relacionados à instalação, configuração, administração e operação da solução. O suporte deverá ser prestado, no mínimo, em língua inglesa, sendo desejável a disponibilidade de atendimento em português (Brasil) ou em espanhol durante o horário comercial. A CONTRATADA deverá assegurar o cumprimento de prazos de resposta e de resolução compatíveis com a criticidade dos chamados, bem como adotar procedimentos de escalonamento e de comunicação periódica do status até a completa resolução dos casos.

1.9.7. O suporte técnico deverá contemplar, no mínimo: esclarecimento de dúvidas não cobertas pela documentação; diagnóstico e resolução de falhas de funcionamento da solução; orientação quanto à detecção e ao tratamento de ameaças; apoio na utilização de funcionalidades de investigação e resposta (incluindo consultas e análise de telemetria); e assistência na configuração da solução para fins operacionais. O atendimento deverá ser realizado por meio de múltiplos canais, incluindo, no mínimo, portal web, e-mail, telefone e chat, devendo todos os chamados serem registrados e rastreáveis.

1.9.8. Os chamados de suporte técnico deverão ser classificados conforme os seguintes níveis de severidade: (a) crítica, quando houver indisponibilidade total da solução ou impacto severo em ambiente de produção, sem solução alternativa disponível; (b) alta, quando houver impacto significativo no funcionamento da solução, com degradação relevante, porém com possibilidade de operação parcial; (c) média, quando houver impacto moderado, sem comprometimento crítico das operações; e (d) baixa, para dúvidas, solicitações de configuração ou impactos mínimos sem prejuízo operacional. O atendimento deverá observar os seguintes prazos: até 4 (quatro) horas *corridas* para severidade crítica; até 8 (oito) horas *corridas* para severidade alta; e até 24 (vinte e quatro) horas *úteis* para severidades médias e baixas.

2. **GERENCIAMENTO CENTRALIZADO, INTERFACE E INTEGRAÇÕES**

2.1. A solução deverá possuir uma interface administrativa mantida na infraestrutura do fabricante, acessível via web, em português (Brasil) e/ou em inglês. Adicionalmente deverá:

2.1.1. Disponibilizar um painel gerencial (Dashboard) com visão consolidada do status de proteção, da classificação de dispositivos (saudáveis, com falha de comunicação, desatualizados), dos alertas ativos e do detalhamento das máquinas. A partir do dashboard, a CONTRATANTE deverá ser capaz de executar ações corretivas remotas, como iniciar varredura, forçar atualização, aplicar políticas, isolar o dispositivo e visualizar eventos. Suportar controle de acesso baseado em perfis, permitindo a criação de grupos de administradores com diferentes níveis de permissão.

2.1.2. Permitir a organização dos dispositivos em grupos hierárquicos, estáticos ou dinâmicos (por sistema operacional, por unidade organizacional, etc.).

2.1.3. A solução deverá possibilitar a integração com o LDAP/AD, sincronizando automaticamente os objetos de computador com os endpoints protegidos e exibindo os dispositivos não gerenciados (sem o agente da solução instalado).

2.1.4. Disponibilizar API baseada em padrões de mercado (ex.: RESTful) e exportação de logs (ex.: JSON/Syslog) para integração nativa com soluções de centralização de eventos de segurança (ex.: SIEM e SOAR).

2.1.5. Monitorar automaticamente a conformidade das configurações de segurança aplicadas, identificando erros de configuração, políticas desativadas, redundâncias ou falhas que possam reduzir o nível de proteção do ambiente, fornecendo alertas e recomendações de correção imediatas.

2.1.6. Exigir autenticação de acesso robusta, com suporte nativo, ou por integração federada, à autenticação de múltiplos fatores (MFA). O acesso a funcionalidades críticas de resposta a incidentes e de execução remota deve ser obrigatoriamente condicionado a esta camada de autenticação, a fim de garantir a integridade da administração do ambiente.

3. PROTEÇÃO ANTIMALWARE E PREVENÇÃO AVANÇADA

3.1. Prover proteção em tempo real (incluindo durante o boot do sistema operacional), com varreduras agendadas e sob demanda, contra vírus, trojans, *worms*, *spywares*, *adwares*, macros maliciosas, *rootkits*, *botnets* e aplicações potencialmente indesejadas (PUA).

3.2. O mecanismo de proteção deverá utilizar múltiplas camadas analíticas, de pré-execução e de tempo de execução: assinaturas atualizadas continuamente, análise heurística, machine learning local, emulação de código e consulta de reputação na nuvem do fabricante.

3.3. Possuir um mecanismo de varredura otimizado, capaz de priorizar arquivos novos ou modificados e de permitir a exclusão de recursos de rede mapeados da varredura, visando otimizar o desempenho do ativo.

3.4. A solução deve possuir capacidade de monitoramento e bloqueio de conexões de rede em nível de host, identificando e interrompendo comunicações associadas a infraestruturas de Comando e Controle (C2), beaconing e exfiltração de dados, com base em inteligência de ameaças em tempo real e na análise de comportamento de processos.

3.5. A solução deve impedir o estabelecimento de pontes de rede (Network Bridging) e de conexões simultâneas entre interfaces distintas (ex.: LAN, Wi-Fi e modems externos), permitindo o bloqueio automático de adaptadores secundários quando a rede corporativa estiver ativa.

3.6. A solução deverá permitir a configuração detalhada de ações (alertar, colocar em quarentena, excluir) e a criação de listas de permissão (*whitelists*) e de bloqueio (*blacklists*), globais ou por grupo, para arquivos, diretórios, identificadores digitais (*hashes*) e processos.

3.7. Detectar e bloquear táticas de ofuscação, identificando inconsistências, como extensões duplas (ex.: arquivo.jpg.exe) e incompatibilidades entre a extensão e o tipo real do arquivo.

3.8. Realizar a remediação profunda e automática de incidentes, incluindo a eliminação de processos ativos, chaves de registro maliciosas, tarefas agendadas e serviços criados por ameaças.

3.9. A solução deverá possuir mecanismos dinâmicos de defesa que, ao detectarem comportamentos anômalos característicos de um adversário ativo no equipamento (ex.: ataques de mãos no teclado - *hands-on-keyboard*), elevem automaticamente a agressividade do bloqueio do agente, impedindo temporariamente a execução de ferramentas administrativas e de comandos que normalmente seriam permitidos, até que a ameaça seja neutralizada.

3.10. A solução deverá garantir a continuidade da proteção avançada em tempo real (incluindo capacidades de análise heurística, aprendizado de máquina local e bloqueio de comportamentos anômalos) mesmo quando o dispositivo protegido estiver temporariamente desconectado da rede corporativa ou da internet, sem depender exclusivamente de consultas à nuvem para bloquear ameaças.

4. PROTEÇÃO ESPECÍFICA CONTRA RANSOMWARE E ANTI-EXPLOIT

4.1. A solução deverá, obrigatoriamente, detectar e bloquear ataques de ransomware com base em análise comportamental, interrompendo o processo malicioso antes do impacto (criptografia dos

dados), independentemente da existência de assinaturas de vírus, hashes conhecidos ou de conexão ativa com a internet.

4.2. A solução deverá possuir capacidades avançadas de remediação que permitam interromper imediatamente os processos de ransomware.

4.2.1. Para as estações de trabalho, a solução também deve permitir a reversão (rollback) automática de alterações maliciosas, seja por meio da restauração de arquivos criptografados ou modificados indevidamente pelo ransomware, seja pela limpeza automatizada de artefatos de persistência e de chaves de registro modificadas. Para servidores, a funcionalidade de reversão deve ser aplicada conforme a compatibilidade com o sistema de arquivos e as recomendações técnicas do fabricante.

4.3. A solução deverá possuir capacidade nativa de proteger servidores de arquivos e pastas compartilhados contra ataques de ransomware iniciados por equipamentos remotos na rede corporativa, inclusive por dispositivos de terceiros que não possuam o agente de segurança instalado ou gerenciado pela Contratante.

4.4. Ao detectar um comportamento de criptografia maliciosa em seus discos locais proveniente de uma conexão de rede externa (ex.: protocolos de compartilhamento de arquivos como SMB/CIFS), o agente instalado no servidor alvo deverá:

- a) Interromper imediatamente o processo de modificação dos arquivos;
- b) Bloquear automaticamente a comunicação de rede (endereço IP) do equipamento atacante, isolando a ameaça;
- c) Reverter os arquivos locais que foram indevidamente alterados pelo equipamento ofensor;
- d) Emitir um alerta detalhado no painel central de gerenciamento, identificando claramente o endereço IP de origem do ataque.

4.5. O HIPS (*Host Intrusion Prevention System*) deverá prover tecnologia *Anti-Exploit* baseada em comportamento, mitigando ataques fileless (em memória) e técnicas de evasão do sistema operacional, incluindo, no mínimo: buffer overflow, *Return-Oriented Programming* (ROP), *Heap Spraying*, manipulação de IAT/VTable, exploração de SEH, injeção de *shellcode* e contorno de DEP/ASLR e WOW64.

4.6. Possuir capacidade nativa de detectar e bloquear táticas de roubo de credenciais em memória, impedindo que ferramentas maliciosas (ex.: Mimikatz ou ataques de dump de memória do processo LSASS) extraiam senhas, hashes ou tíquetes de autenticação dos usuários conectados ao sistema operacional.

4.7. A solução deverá possuir mecanismos que impeçam o reinício ou a inicialização programática do equipamento em "Modo de Segurança" para fins de contorno de proteção. Caso o dispositivo seja iniciado neste modo, a solução deverá manter ativas as capacidades críticas de proteção, incluindo a análise de comportamento e a proteção contra *ransomware*.

5. DETECÇÃO E RESPOSTA A INCIDENTES (EDR)

5.1. O módulo de detecção e resposta (EDR) deverá estar embarcado no mesmo agente único e gerenciado pela mesma interface, com foco na visibilidade e na resposta a táticas, técnicas e procedimentos operacionais utilizados por cibercriminosos.

5.2. A solução deverá mapear e classificar, nativamente, os alertas e detecções de acordo com frameworks globais de segurança, preferencialmente o MITRE ATT&CK, facilitando a compreensão das fases do ataque (ex.: acesso inicial, escalonamento de privilégios, movimentação lateral e exfiltração).

5.3. A solução deverá ser capaz de enviar arquivos suspeitos para ambientes de análise isolados e seguros na nuvem (ex.: *sandbox*) do mesmo fabricante, para verificação avançada de comportamento.

5.4. O EDR deverá fornecer uma visualização gráfica da cadeia de eventos do ataque, demonstrando a origem, as interações no sistema (processos criados, conexões de rede estabelecidas,

arquivos modificados) e a linha do tempo do incidente.

5.5. O relatório detalhado do incidente deverá conter: o *hash* do arquivo, o nome, a data e a hora, a reputação global consultada, o resultado da análise de aprendizado de máquina e as informações do certificado digital, se houver.

5.6. A solução deverá permitir a execução de ações remotas de Resposta a Incidentes diretamente pelo console:

- a) Isolamento lógico do ativo na rede, mantendo apenas a comunicação com o console do EDR;
- b) Encerramento forçado de processos maliciosos ou suspeitos (*kill process*);
- c) Remediação e exclusão da ameaça detectada.

5.7. A solução deverá buscar, proativamente e retrospectivamente, ameaças (Threat Hunting) por meio de indicadores de comprometimento, como hashes, nomes de processos, endereços IP, domínios e linhas de comando.

5.8. A solução deverá possuir um repositório central de telemetria/eventos na nuvem, retendo os dados para investigação por, no mínimo, 30 (trinta) dias, permitindo auditoria forense mesmo que o ativo esteja offline ou formatado, sendo necessário que a telemetria armazenada seja totalmente indexada e pesquisável para fins de busca de ameaças.

5.9. Adicionalmente, a solução deverá suportar a execução de consultas avançadas sobre a telemetria coletada, preferencialmente por meio de linguagem estruturada (ex.: SQL-like) ou mecanismos equivalentes, diretamente sobre a telemetria armazenada, contemplando, no mínimo, as seguintes capacidades:

- a) Disponibilizar consultas pré-elaboradas com possibilidade de customização pelo administrador, contemplando os principais casos de uso de segurança (ex.: processos em portas não padrão, execuções suspeitas de PowerShell, modificações de registro, conexões de rede inesperadas);
- b) Permitir a criação, nomeação e armazenamento de consultas personalizadas pelo administrador, reutilizáveis em buscas futuras;
- c) Executar consultas tanto em tempo real nos endpoints quanto sobre a telemetria histórica armazenada.

5.10. A solução deverá identificar e correlacionar ataques simultâneos em múltiplos dispositivos, emitindo alertas consolidados de surto (*outbreak*). Adicionalmente, deverá possuir mecanismos de resposta que, ao detectarem o uso de ferramentas de *hacking* ou de táticas maliciosas (como o uso indevido de *PowerShell*) em um equipamento, permitam a aplicação, automática ou manual, de bloqueios e restrições preventivas nas demais estações da rede, impedindo a movimentação lateral da ameaça.

5.11. O painel de investigação de incidentes deverá possuir um *recurso integrado de Inteligência Artificial habilitado para interações em linguagem natural*. A ferramenta deverá auxiliar os analistas, traduzindo consultas complexas, resumindo a cadeia do ataque, explicando o comportamento do código malicioso e sugerindo a melhor ação de resposta e de remediação, visando agilizar a tomada de decisão.

5.12. A solução deverá oferecer um *terminal de acesso remoto seguro e interativo (Shell/CLI)* aos endpoints gerenciados, diretamente a partir do painel de controle do EDR, dispensando ferramentas de terceiros, como RDP ou VPN. Esse acesso deverá permitir ao administrador investigar e corrigir problemas em *tempo real*, contemplando, no mínimo, as seguintes capacidades:

- a) Interromper, suspender ou finalizar processos em execução;
- b) Executar comandos e roteiros lógicos (scripts);
- c) Navegar pelo sistema de arquivos;
- d) Instalar, remover ou modificar arquivos e programas para fins de contenção e remediação;

e) Desligar e/ou reinicializar o endpoint;

f) Gerar um registro de auditoria (log) detalhado de todos os comandos executados durante a sessão remota, garantindo o controle rigoroso das ações dos administradores.

5.13. A solução deverá identificar o uso malicioso de ferramentas nativas do sistema operacional (ex.: PowerShell, BITS, Certutil, WMI) por meio de telemetria comportamental, distinguindo atividades administrativas autorizadas de táticas de invasão, garantindo visibilidade sobre a execução de comandos suspeitos, mesmo quando executados por processos legítimos.

6. CONTROLE DE APLICAÇÕES E DISPOSITIVOS PERIFÉRICOS

6.1. Possuir controle de aplicações integrado ao agente para mitigar a execução de ferramentas de hacking, scripts não autorizados e artefatos maliciosos, permitindo o bloqueio de execução com base no nome do arquivo, no hash (ex.: SHA-256) ou na assinatura digital do fabricante.

6.2. Permitir a criação de políticas de bloqueio da execução de aplicações, scripts e utilitários de sistema (ex.: PowerShell, PsExec, WMI) para usuários ou grupos que não necessitem destas ferramentas em suas atividades profissionais, reduzindo a superfície de ataque no endpoint.

6.3. Possuir controle de dispositivos para fechar vetores de entrada físicos de malware, permitindo monitorar e bloquear o uso de mídias de armazenamento removíveis (ex.: pen drives USB e HDs externos).

6.4. O bloqueio de dispositivos USB deverá permitir uma configuração granular básica: bloqueio total, acesso somente leitura (evitando exfiltração) e acesso total.

7. PROTEÇÃO CONTRA EXFILTRAÇÃO E ROUBO DE DADOS

7.1. A solução deverá possuir mecanismos focados na prevenção da exfiltração de dados (roubo de informações), uma tática comumente utilizada em ataques de ransomware de dupla extorsão.

7.2. Monitorar o comportamento de processos e identificar tentativas de cópia em massa de arquivos para dispositivos externos, compartilhamentos de rede suspeitos ou conexões externas não padronizadas.

7.3. Permitir o bloqueio ou o alerta quando processos não autorizados tentarem acessar, modificar ou transferir arquivos críticos do sistema ou de diretórios sensíveis previamente mapeados.

7.4. A proteção contra o vazamento de dados por meio do armazenamento em USB deverá registrar os eventos no console administrativo, incluindo o usuário, o endpoint, a data/hora e o nome do arquivo transferido (quando tecnicamente aplicável), para fins de investigação pelo time de resposta a incidentes.

8. AUDITORIA, RELATÓRIOS E RESPONSABILIDADE TÉCNICA

8.1. A solução deverá manter uma trilha de auditoria inviolável das atividades administrativas no console (registro de quem fez, o que fez e quando fez).

8.2. Permitir a exportação de relatórios em CSV e PDF, com visões gráficas de incidentes, do estado dos agentes, de logs de controle web, de aplicações, de USB e de detecções de roubo de dados.

8.3. Todas as funcionalidades (Sandbox, motores antimalware, Threat Intel) deverão operar de forma nativa e integrada, sob a responsabilidade de um único fabricante. Não será admitida a necessidade de contratações paralelas de terceiros para o pleno funcionamento.

8.4. Os mecanismos de inteligência artificial utilizados deverão ser nativos da solução ofertada ou executados em ambiente controlado pelo fabricante, garantindo que os dados da CONTRATANTE permaneçam sob sua governança e não sejam compartilhados com terceiros.

8.5. A CONTRATADA deverá descrever como os mecanismos de IA são integrados à solução, tanto no processamento quanto no fluxo de dados. A solução não poderá encaminhar, compartilhar ou expor dados da CONTRATANTE a serviços de inteligência artificial de terceiros, incluindo APIs externas, plataformas públicas ou quaisquer subcontratados, para fins de processamento, análise ou inferência, sem autorização prévia e expressa da CONTRATANTE.

9. SERVIÇOS DE IMPLANTAÇÃO, INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO CONTRATADA

9.1. A implantação deverá ser realizada por profissionais devidamente certificados e qualificados na solução ofertada, devendo a CONTRATADA comprovar tais certificações quando solicitadas. As atividades deverão contar com orientação e validação técnicas do fabricante, especialmente nas fases de elaboração do projeto e de validação da configuração.

9.2. A CONTRATADA deverá apresentar um Plano de Implantação detalhado, que será previamente avaliado e aprovado pela equipe técnica da CONTRATANTE, como condição para início dos serviços.

9.3. O Plano de Implantação deverá conter, no mínimo:

- a) Descrição detalhada das atividades, incluindo fases, marcos (milestones), dependências e cronograma de execução;
- b) Estratégia de implantação (ex.: piloto, implantação gradual por grupos, ou big bang), com justificativa técnica;
- c) Políticas de configuração dos elementos da solução;
- d) Topologia lógica e arquitetura da solução;
- e) Plano de comunicação e janelas de execução (incluindo eventuais janelas de manutenção);
- f) Procedimentos de rollback e de contingência, quando aplicáveis.

9.4. O Plano de Implantação deverá contemplar estratégias distintas para os diferentes perfis de ativos da CONTRATANTE, incluindo, no mínimo:

- a) Estações de trabalho, segmentadas por sistema operacional e versão (incluindo ambientes legados);
- b) Servidores, segmentados por criticidade, sistema operacional e função;

9.5. Para cada grupo de ativos, deverão ser definidos: a abordagem de implantação, os pré-requisitos, os riscos, as restrições operacionais e a estratégia de mitigação.

9.6. Todo o trabalho deverá seguir o Plano de Implantação aprovado, sendo quaisquer desvios previamente justificados e aprovados pela CONTRATANTE.

9.7. A CONTRATADA será responsável por realizar a instalação completa da solução, incluindo a configuração, a parametrização, a integração com o ambiente da CONTRATANTE e a execução dos testes necessários, sob supervisão da CONTRATANTE.

9.8. A CONTRATADA será responsável pelo dimensionamento adequado da solução, garantindo o atendimento integral aos requisitos deste Termo, ficando o referido dimensionamento sujeito à validação da equipe técnica da CONTRATANTE.

9.9. A solução implantada não deverá causar impacto negativo no ambiente da CONTRATANTE, incluindo degradação do desempenho em endpoints, servidores ou na rede, devendo operar de forma transparente ao usuário final, respeitando as boas práticas do fabricante.

9.10. Caso o dimensionamento ou a configuração adotada não apresente desempenho satisfatório, a CONTRATADA deverá realizar os ajustes necessários, incluindo eventual redimensionamento da solução, sem ônus adicional para a CONTRATANTE.

9.11. A solução será considerada implantada (entregue) quando atingir, no mínimo, 30% (trinta por cento) dos ativos elegíveis da CONTRATANTE, incluindo as estações de trabalho e os servidores.

10. TRANSFERÊNCIA DE CONHECIMENTO

10.1. A CONTRATADA deverá transferir à equipe técnica da CONTRATANTE o conhecimento da solução implantada.

10.2. A CONTRATADA deverá apresentar um Plano de Transferência de Conhecimento, a ser aprovado pela CONTRATANTE, que contemple o conteúdo programático, a carga horária e a abordagem prática.

10.3. A transferência de conhecimento deverá ser realizada no ambiente já implantado na CONTRATANTE, contemplando atividades práticas (hands-on), de modo a capacitar a equipe para operação autônoma da solução.

10.4. O conteúdo mínimo deverá abranger:

- a) Administração e operação da solução (console);
- b) Criação e ajuste de políticas de segurança;
- c) Monitoramento de alertas e eventos;
- d) Capacitação prática na investigação de incidentes por meio da execução de consultas estruturadas sobre a telemetria, incluindo o uso da biblioteca nativa e a criação de consultas personalizadas para identificar indicadores de comprometimento. Deverá incluir também as instruções sobre como interagir com o assistente de IA em linguagem natural para acelerar a análise da cadeia de ataque e a geração de respostas;
- e) Execução de ações de resposta e remediação, incluindo o uso do terminal de acesso remoto nativo da solução, demonstrando a execução de comandos, coleta de arquivos para perícia, encerramento de processos e limpeza de artefatos em estações isoladas;
- f) Geração de relatórios;
- g) Boas práticas de operação e manutenção;
- h) Elaboração conjunta e simulação de ao menos 03 (três) cenários de ataque (ex.: Ransomware, Movimentação Lateral e Execução de PowerShell Malicioso), exercitando o fluxo completo: detecção -> investigação -> resposta.

10.5. A transferência de conhecimento deverá ser realizada na modalidade remota (EAD) em horários acordados com a CONTRATANTE.

10.6. Todo o material didático deverá ser fornecido pela CONTRATADA, incluindo guias operacionais, manuais e documentação da solução.

10.7. Ao final da transferência de conhecimento, a CONTRATADA deverá disponibilizar documentação complementar, incluindo procedimentos operacionais (playbooks), relativos às principais atividades da solução.

10.8. A transferência de conhecimento será considerada concluída após a validação, pela CONTRATANTE, da capacidade da equipe para operar a solução de forma autônoma.

10.9. Caso a CONTRATANTE identifique insuficiência de capacitação, a CONTRATADA deverá realizar sessões complementares, sem ônus adicional.

11. TESTE DE BANCADA (PROVA DE CONCEITO – POC) DA SOLUÇÃO DE EDR

11.1. A licitante provisoriamente classificada em primeiro lugar deverá submeter a solução ofertada ao Teste de Bancada (PoC), a fim de comprovar, de forma prática, o atendimento aos requisitos técnicos estabelecidos neste Termo de Referência.

11.2. A PoC terá duração de até 6 (seis) horas e deverá ser realizada em ambiente controlado, disponibilizado pela licitante, no prazo máximo de 5 (cinco) dias úteis após a convocação formal, devendo permitir a validação pela CONTRATANTE, inclusive por meio da execução de testes independentes.

11.3. A licitante deverá preparar previamente o ambiente e garantir que todos os cenários de teste estejam aptos à execução no momento da avaliação.

11.4. Durante a PoC, a solução deverá ser implantada em estações de trabalho e/ou servidores definidos pela CONTRATANTE, contemplando cenários reais de uso, incluindo, mas não se limitando a:

- a) Instalação e ativação do agente em endpoint disponibilizado pela CONTRATANTE;
- b) Integração com a interface administrativa e a validação de comunicação;
- c) Aplicação de política de segurança e comprovação de sua efetividade;
- d) Simulação de comportamento malicioso, com respectiva detecção pela solução;
- e) Visualização dos eventos gerados, incluindo telemetria e linha do tempo do incidente, demonstrando ainda a origem, as interações no sistema (processos criados, conexões de rede estabelecidas, arquivos modificados);
- f) Execução de procedimentos de resposta e remediação, incluindo o isolamento do endpoint, o bloqueio de processos e o uso do terminal de acesso remoto nativo para, por exemplo, a criação e a exclusão de arquivos e a execução de scripts de limpeza no host afetado.
- g) Execução de consultas avançadas de investigação sobre a telemetria, demonstrando a criação de uma consulta personalizada (ex.: linguagem estruturada ou mecanismos equivalentes) para localizar um artefato específico (processo, chave de registro ou conexão de rede);
- h) Demonstrar o uso do recurso de inteligência artificial generativa para a explicação de um alerta complexo em linguagem natural e para o auxílio na construção de uma consulta de investigação, comprovando a redução da barreira técnica para o analista
- i) Avaliação do consumo de recursos (CPU, memória e disco) em condições normais e em um cenário de ataque.

11.5. A CONTRATANTE poderá, durante a execução, conduzir ou solicitar a execução direta de testes adicionais ou de variações nos cenários, com o objetivo de verificar a usabilidade, a operação e o atendimento aos requisitos da solução.

11.6. A solução deverá demonstrar capacidade de:

- a) Detectar, registrar e classificar os eventos de segurança;
- b) Correlacionar atividades maliciosas em cadeia de ataque;
- c) Apresentar visibilidade clara da linha do tempo do incidente;
- d) Executar ações de resposta, tais como isolamento de endpoint, bloqueio de processos, quarentena de arquivos e rollback (quando aplicável);
- e) Disponibilizar os logs e as evidências para auditoria.

11.7. A avaliação do Teste de Bancada considerará critérios objetivos, incluindo:

- a) Aderência funcional aos requisitos do edital;
- b) Eficácia na detecção e resposta às ameaças;
- c) Desempenho e impacto nos recursos do endpoint, sem degradação perceptível ao usuário;
- d) Usabilidade da interface administrativa;
- e) Qualidade das informações e dos relatórios apresentados.

- 11.8. A solução será considerada aprovada caso demonstre, de forma satisfatória, o atendimento aos cenários de teste definidos neste Termo de Referência e aos requisitos essenciais estabelecidos.
- 11.9. O descumprimento dos requisitos essenciais implicará a desclassificação da licitante.
- 11.10. Todos os custos relacionados ao Teste de Bancada serão de responsabilidade da licitante.
- 11.11. A CONTRATANTE poderá registrar as evidências e elaborar um relatório técnico com os resultados obtidos na PoC.

Duque de Caxias, na data da assinatura.



DOCUMENTO ASSINADO ELETRONICAMENTE COM FUNDAMENTO NO ART. 6º, § 1º, DO [DECRETO Nº 8.539, DE 8 DE OUTUBRO DE 2015](#) EM 17/07/2026, ÀS 09:52, CONFORME HORÁRIO OFICIAL DE BRASÍLIA, POR

ANDRE GHEVENTER

Integrante Técnico da Equipe de Planejamento da Contratação



DOCUMENTO ASSINADO ELETRONICAMENTE COM FUNDAMENTO NO ART. 6º, § 1º, DO [DECRETO Nº 8.539, DE 8 DE OUTUBRO DE 2015](#) EM 17/07/2026, ÀS 09:53, CONFORME HORÁRIO OFICIAL DE BRASÍLIA, POR

PAULO GUSTAVO DE OLIVEIRA DEL PELOSO

Integrante Requisitante da Equipe de Planejamento da Contratação

A autenticidade deste documento pode ser conferida no site

https://sei.inmetro.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2527142** e o código CRC **E37972EF**.

