

Estudo Técnico Preliminar - EDR MPPI

ESTUDO TÉCNICO PRELIMINAR - ETP

Contratações de Tecnologia da Informação e Comunicação

MODELO OBRIGATÓRIO MP PARA CONTRATAÇÃO/AQUISIÇÃO DE BENS E SERVIÇOS DE TIC: ETP Digital + MOTec CNMP 283/2024

Este Estudo Técnico Preliminar foi elaborado com base na estrutura do modelo institucional de ETP para contratações de TIC do Ministério Público do Estado do Piauí (MPPI), restringindo o escopo à **atualização da subscrição anual de solução corporativa de proteção de dispositivos na modalidade EDR — Endpoint Detection and Response da fabricante CrowdStrike.**

A descrição técnica foi elaborada considerando a manutenção da solução CrowdStrike/Falcon atualmente implantada no MPPI, cuja padronização encontra-se justificada neste Estudo Técnico Preliminar em razão da continuidade operacional, compatibilidade tecnológica, preservação dos investimentos realizados e mitigação dos riscos associados à substituição da plataforma.

INFORMAÇÕES BÁSICAS (ETP Digital)

1. Informações básicas

Número do processo (PGEA): 19.21.0016.0015844/2026-13

Objeto: Registro de preços para contratação da atualização do licenciamento anual de subscrição da solução corporativa CrowdStrike/Falcon, atualmente utilizada pelo MPPI, na modalidade EDR - Endpoint Detection and Response, para proteção de dispositivos, com prevenção, detecção, investigação, resposta a incidentes, caça a ameaças, suporte técnico, atualização, configuração, capacitação e operação assistida, sem ampliação para módulos autônomos de XDR, proteção de identidade ou DLP.

Unidade requisitante: Coordenadoria de Tecnologia da Informação — CTI/MPPI.

2. Histórico de revisões (MOTec)

Data	Versão	Descrição	Autor
29/05/2026	1.0	Elaboração da primeira versão do ETP, com escopo restrito à solução EDR para registro de preços.	Equipe de Planejamento da Contratação

3. Previsão da contratação no PCA/MPPI (Lei 14.133/2021 §1º II; IN 94/2022 art. 6; MOTec) - ITEM OBRIGATÓRIO

- 3.1. O objeto da contratação está previsto no Plano de Contratações Anual 2026 do MPPI, conforme item indicado no ETP de referência:

Código do ITEM	Descrição da solução
36B7	Serviço Anual de Subscrição de Solução de Proteção de Dispositivos - Antivírus

- 3.2. Embora o item do PCA utilize a nomenclatura “Antivírus”, a necessidade institucional atual exige tecnologia compatível com a evolução das soluções de proteção de endpoint, especialmente recursos de **EDR**, capazes de detectar, investigar e responder a ameaças avançadas, incluindo malware, ransomware, exploração de vulnerabilidades, comportamento malicioso, movimentação lateral e uso indevido de processos legítimos.

- 3.3. O Plano de Contratações Anual — PCA 2026 do MPPI está indicado no ETP de referência no seguinte endereço:

https://sei.mppi.mp.br/sei/controlador.php?acao=procedimento_trabalhar&id_procedimento=1553788&id_documento=1602476

NECESSIDADES (ETP Digital)

4. Descrição da necessidade (Lei 14.133/2021 §1º I; IN 94/2022 art. 11º I; MOTec; ETP Digital) - ITEM OBRIGATÓRIO

Motivação/Justificativa

- 4.1. O Ministério Público do Estado do Piauí — MPPI exerce funções institucionais essenciais à defesa da ordem jurídica, do regime democrático e dos interesses sociais e individuais indisponíveis. A continuidade das atividades finalísticas e administrativas depende de ambiente computacional íntegro, disponível, confiável e protegido contra ameaças cibernéticas.
- 4.2. O cenário de ameaças cibernéticas tornou-se progressivamente mais sofisticado, com ataques de ransomware, exploração de

vulnerabilidades, uso de ferramentas legítimas para movimentação lateral, abuso de credenciais e técnicas de evasão capazes de superar mecanismos tradicionais de antivírus. Diante desse contexto, soluções convencionais baseadas apenas em assinatura ou varredura periódica não são suficientes para atender ao nível de proteção exigido pelo MPPI.

- 4.3. À medida que as ameaças cibernéticas se tornam cada vez mais sofisticadas, as organizações enfrentam desafios crescentes para proteger seus ativos. Essas ameaças são frequentemente impulsionadas por criminosos que utilizam inteligência artificial avançada e são financiados por redes criminosas organizadas. Para mitigar esses riscos, é essencial implementar soluções robustas de segurança cibernética. Tais soluções são fundamentais para proteger os ativos digitais e a infraestrutura das organizações contra uma gama de ameaças, incluindo violações de dados, interrupções de serviço, vazamento de informações e danos à reputação.
- 4.4. Entre as várias formas de ataques cibernéticos, os ataques de ransomware destacam-se como os mais prejudiciais e estão em rápido crescimento. Esses ataques podem paralisar operações, causar perdas financeiras significativas e comprometer a confiança dos clientes e parceiros comerciais. Portanto, a adoção de estratégias eficazes de defesa contra ransomware é uma prioridade crucial para qualquer organização que busca manter sua integridade e resiliência no ambiente digital.
- 4.5. Os ataques cibernéticos realizados por Estados-nação, direcionados a instituições governamentais e infraestruturas críticas, estão se tornando cada vez mais frequentes. Essas operações são tipicamente associadas a governos que conduzem atividades cibernéticas ofensivas com diversos objetivos estratégicos. Esses ataques frequentemente envolvem espionagem, sabotagem ou ações disruptivas e destrutivas, visando comprometer a segurança, a economia e a estabilidade dos países-alvo.
- 4.6. O MPPI já utiliza solução corporativa de proteção de dispositivos baseada na plataforma CrowdStrike/Falcon, devidamente implantada e integrada ao ambiente institucional. Considerando os sensores atualmente instalados, as políticas configuradas, a capacitação da equipe técnica, as integrações existentes e os procedimentos operacionais consolidados, a presente contratação objetiva a continuidade da solução padronizada, nos termos da justificativa técnica e econômica constante deste ETP.
- 4.7. A contratação se justifica pela necessidade de manter e/ou contratar subscrição anual de solução EDR corporativa, com console centralizada em nuvem, agente/sensor para dispositivos, monitoramento comportamental, detecção baseada em indicadores de ataque e inteligência de ameaças, resposta remota, isolamento de endpoints e recursos de investigação. A solução deverá permitir ao MPPI aumentar sua resiliência contra ameaças avançadas, reduzir tempo de detecção e resposta, preservar a continuidade

operacional e proteger ativos digitais estratégicos.

- 4.8. Atualmente, o MPPI utiliza solução anual de subscrição de proteção de dispositivos da fabricante CrowdStrike, com cobertura para o parque computacional do órgão. A presente contratação não tem como objetivo a substituição da solução existente nem a ampliação para novos módulos distintos, mas sim a manutenção da subscrição atualmente necessária à continuidade da proteção dos dispositivos, contemplando atualização, suporte, garantia de funcionamento, operação assistida e preservação das capacidades já utilizadas no ambiente do MPPI.
- 4.9. A continuidade da solução se justifica pela necessidade de preservar a proteção já implantada, evitar descontinuidade de cobertura dos dispositivos, manter as políticas de segurança atualmente configuradas, reduzir riscos operacionais decorrentes de troca de tecnologia e preservar o conhecimento técnico já desenvolvido pela equipe do MPPI. A substituição da solução por outro fabricante poderia exigir novo ciclo de implantação, reconfiguração de políticas, reinstalação de agentes, retreinamento da equipe, revalidação de compatibilidades e eventual exposição temporária do ambiente a riscos durante a transição.
- 4.10. Do ponto de vista jurídico, a presente contratação observa os princípios previstos no art. 5º da Lei nº 14.133/2021, especialmente os da eficiência, economicidade, planejamento, segurança jurídica e interesse público. Além disso, nos termos do art. 11 da mesma Lei, o processo licitatório deve assegurar a seleção da proposta apta a gerar o resultado de contratação mais vantajoso para a Administração Pública, inclusive no que se refere ao ciclo de vida do objeto, bem como evitar contratações com sobrepreço, preços manifestamente inexequíveis ou superfaturamento na execução contratual.
- 4.11. Há precedentes na jurisprudência que apontam para a possibilidade de se observar o princípio da padronização, sem conflitar com a vedação da preferência de marca, a exemplo do Acórdão- TCU nº 75681/2022, a definição da divisibilidade ou não por lotes, ou itens na licitação insere-se no âmbito da discricionariedade administrativa, competindo ao gestor público avaliar, na fase de planejamento, qual atende melhor o interesse público, demonstrando a vantajosidade da opção feita, bem como, eventual prejuízo para o conjunto ou complexo ou perda de economia de escala:
- “Em licitações referentes a compras, inclusive de softwares, é possível a indicação da marca, desde que seja estritamente necessária para atender exigências de padronização e que haja prévia justificação.”.*
- 4.12. Importante ressaltar que a padronização não é generalizada, pois está atrelada a manutenção do ambiente de segurança da informação já

existente dentro do órgão e que utiliza a plataforma específica deste fabricante.

- 4.13. A solução a ser mantida deverá permanecer baseada em console única de administração em nuvem, sem dependência de componentes locais para gerenciamento, permitindo administração centralizada, aplicação de políticas, acompanhamento de eventos, geração de relatórios e execução de ações de resposta a incidentes. Essa característica é relevante para o MPPI por reduzir a necessidade de infraestrutura local adicional, simplificar a operação e manter alinhamento com a estratégia de uso eficiente dos recursos tecnológicos.
- 4.14. Também se mostra necessária a manutenção das capacidades de proteção comportamental e de aprendizado de máquina, aptas a detectar e bloquear ameaças conhecidas e desconhecidas, ataques do tipo zero-day, fileless, ransomware, exploits, shell reverso, webshell, técnicas de persistência, execução de scripts suspeitos e demais comportamentos maliciosos. Essas capacidades são essenciais para enfrentar ameaças modernas que não dependem exclusivamente de arquivos maliciosos tradicionais e que, muitas vezes, utilizam ferramentas legítimas do próprio sistema operacional.
- 4.15. A contratação deve preservar, ainda, os recursos de resposta e investigação remota, permitindo que administradores autorizados realizem ações como isolamento de dispositivos comprometidos, coleta de logs e artefatos, execução de scripts, encerramento de processos, consulta a conexões de rede e obtenção de informações relevantes para análise de incidentes. Tais funcionalidades reduzem o tempo de resposta, aumentam a capacidade de contenção e apoiam a equipe técnica na investigação e remediação de eventos de segurança.
- 4.16. A manutenção da solução também contempla recursos de automação de tarefas e fluxos de resposta, permitindo a criação de gatilhos, notificações, playbooks e ações automatizadas a partir de eventos de segurança. Esses mecanismos contribuem para padronizar procedimentos, reduzir atividades manuais repetitivas, acelerar a contenção de ameaças e melhorar a eficiência operacional da equipe de tecnologia da informação.
- 4.17. Além da proteção contra ameaças, permanece necessária a continuidade dos controles complementares já previstos na solução, como gerenciamento de firewall local a partir da console, controle de dispositivos USB, políticas de bloqueio ou permissão por classes de dispositivos, visibilidade sobre atividades de arquivos em mídias removíveis, geração de relatórios e dashboards, bem como uso de inteligência de ameaças para contextualização de campanhas, indicadores de comprometimento, táticas, técnicas e procedimentos observados no ambiente.

- 4.18. A manutenção da padronização tecnológica decorre da necessidade de preservar a continuidade do ambiente de segurança já implantado, reduzir riscos de interoperabilidade, evitar retrabalho operacional e preservar investimentos realizados em configuração, capacitação, políticas de segurança e procedimentos de resposta a incidentes. A eventual substituição imotivada da tecnologia atualmente utilizada poderia exigir novo ciclo de implantação, reconfiguração de políticas, reinstalação de agentes, retreinamento da equipe técnica, revalidação de compatibilidade com os sistemas operacionais do parque computacional e exposição temporária do ambiente a riscos durante a transição.
- 4.19. A adoção de Ata de Registro de Preços é adequada porque a demanda por licenciamento poderá variar conforme crescimento do parque computacional, renovação de estações, inclusão de servidores, expansão de unidades e necessidade de contratação conforme disponibilidade orçamentária e necessidade efetiva.

Necessidades

4.20. As principais necessidades a serem atendidas são:

- Continuidade da proteção corporativa de endpoints do MPPI mediante manutenção da solução EDR CrowdStrike/Falcon atualmente implantada.
- Detecção e resposta em tempo real a ameaças cibernéticas em estações de trabalho e servidores.
- Manutenção da Subscrição Existente - Continuidade da solução corporativa de proteção de dispositivos atualmente utilizada pelo MPPI, garantindo cobertura, atualização, suporte e operação assistida durante a vigência contratual.
- Preservação da Padronização Tecnológica – Continuidade do uso da solução já implantada, evitando substituição desnecessária de tecnologia, retrabalho operacional, reconfiguração de políticas e riscos decorrentes de migração.
- Proteção Contra Ameaças Avançadas – Manutenção das capacidades de detecção e bloqueio de ameaças conhecidas e desconhecidas, ransomware, ataques fileless, exploits, técnicas de Living off the Land, shell reverso, webshell e demais comportamentos maliciosos.
- Resposta a Incidentes e Investigação Remota – Preservação dos recursos de contenção, isolamento de dispositivos, coleta de artefatos, execução de scripts, encerramento de processos e apoio à análise técnica de incidentes de segurança.
- Automação e Eficiência Operacional – Manutenção de fluxos automatizados, notificações, gatilhos e ações de resposta, permitindo maior agilidade e padronização no tratamento de eventos de segurança.
- Controle de Dispositivos e Firewall Local – Continuidade dos mecanismos de controle de dispositivos USB, visibilidade sobre atividades em mídias removíveis e gerenciamento de regras de firewall dos dispositivos protegidos.

- Inteligência de Ameaças, Relatórios e Dashboards – Preservação dos recursos de contextualização de ameaças, extração de indicadores de comprometimento, relatórios operacionais e painéis de acompanhamento para suporte à tomada de decisão.
- Continuidade Operacional e Redução de Riscos – Garantia de que os dispositivos do MPPI permaneçam protegidos sem interrupção de cobertura, minimizando riscos de indisponibilidade, incidentes cibernéticos, perda de visibilidade e enfraquecimento da postura de segurança institucional.
- Prevenção e contenção de malware, ransomware, exploração de vulnerabilidades e técnicas de evasão.
- Gestão centralizada da política de proteção, alertas, investigação, contenção e resposta.
- Operação em nuvem, sem necessidade de implantação de infraestrutura local adicional para console de gerenciamento.
- Redução da superfície de exposição e melhoria da visibilidade sobre eventos de segurança nos dispositivos.
- Preservação dos investimentos já realizados em capacitação, processos operacionais e políticas de segurança.
- Possibilidade de contratação conforme demanda, mediante registro de preços.

5. Área requisitante (ETP DIGITAL; MOTec)

Área requisitante	Responsável
Coordenadoria de Tecnologia da Informação — CTI	Marcos Maciel Martins Brito

6. Necessidades de negócio (IN 94/2022 art.11 I; MOTec; ETP Digital)

6.1. A contratação visa atender às seguintes necessidades de negócio:

- **Garantir a continuidade dos serviços institucionais:** reduzir risco de indisponibilidade causada por incidentes cibernéticos em endpoints e servidores.
- **Fortalecer a segurança cibernética institucional:** elevar a capacidade de prevenção, detecção, investigação e resposta a ameaças avançadas.
- **Proteger dados institucionais sensíveis:** mitigar riscos de comprometimento de informações processuais, administrativas, pessoais e estratégicas.
- **Proteção dos Dispositivos Corporativos:** O MPPI precisa garantir a proteção contínua de estações de trabalho, servidores e demais dispositivos compatíveis, preservando recursos como prevenção comportamental, aprendizado de máquina, proteção contra manipulação do agente, políticas de atualização, quarentena, isolamento de rede e suporte aos sistemas operacionais Windows e Linux.

- **Controle e Redução de Superfície de Ataque:** O Ministério necessita manter recursos de controle de dispositivos USB, gerenciamento de firewall local, bloqueio de comunicações indevidas e visibilidade sobre atividades de arquivos em mídias removíveis, reduzindo riscos de exfiltração de dados, movimentação lateral e uso não autorizado de periféricos no ambiente institucional.
- **Investigação, Automação e Eficiência Operacional:** A solução deve manter capacidades de análise de arquivos em ambiente controlado, extração de indicadores de comprometimento, visualização da cadeia de ataque, execução de ações remotas e automação de fluxos de resposta. Esses recursos apoiam a equipe técnica na padronização de procedimentos, redução de atividades manuais e agilidade no tratamento de eventos de segurança.
- **Reduzir o tempo de detecção e resposta:** permitir atuação rápida da equipe técnica diante de alertas, eventos suspeitos e incidentes confirmados.
- **Manter conformidade com normas e boas práticas:** apoiar o cumprimento da LGPD, da Política de Segurança Institucional do Ministério Público e de normas aplicáveis às contratações de TIC.
- **Preservar investimentos e conhecimento operacional:** aproveitar a experiência da equipe técnica do MPPI com a solução atualmente implantada, preservando a solução CrowdStrike/Falcon atualmente implantada, suas configurações, políticas, integrações e o conhecimento operacional da equipe técnica.
- **Aprimorar a governança da segurança da informação:** disponibilizar relatórios, trilhas de auditoria e indicadores que subsidiem decisões gerenciais e técnicas.

7. Necessidades tecnológicas (IN 94/2022 art.11 I;)

7.1. As necessidades tecnológicas traduzem os requisitos operacionais necessários para viabilizar as necessidades de negócio, considerando o ambiente computacional do MPPI.

7.2. A solução deverá prover, no mínimo:

- Console centralizada, obrigatoriamente em nuvem, com gerenciamento das políticas, sensores/agentes, alertas, eventos, investigações e ações de resposta.
- Agente/sensor de endpoint compatível com estações de trabalho e servidores utilizados pelo MPPI, incluindo sistemas Windows, Windows Server e distribuições Linux corporativas.
- Detecção comportamental e análise baseada em inteligência artificial, aprendizado de máquina, indicadores de ataque, inteligência de ameaças e reputação.
- Prevenção contra malware, ransomware, execução maliciosa de scripts, exploração de vulnerabilidades, técnicas fileless, abuso de ferramentas administrativas e movimentação lateral.
- Recursos de investigação com linha do tempo de eventos, árvore de processos, detalhes de execução, hash, caminho de arquivos, comandos executados, usuário, dispositivo e severidade.

- **Proteção Multiplataforma:** Continuidade da proteção dos dispositivos compatíveis com sistemas operacionais Windows e Linux, garantindo cobertura adequada para estações de trabalho, servidores e demais ativos tecnológicos do ambiente do MPPI.
- **Resistência à Manipulação:** Manutenção de recursos de proteção contra remoção indevida, manipulação do agente, alteração não autorizada de componentes e controle das atualizações dos sensores, preservando a integridade da solução implantada.
- **Visualização da Cadeia de Ataque:** Manutenção de recursos que apresentem a linha do tempo dos eventos, a cadeia de execução associada aos alertas e o contexto necessário para apoiar a análise técnica e a tomada de decisão durante incidentes.
- **Inteligência de Ameaças:** Utilização de inteligência de ameaças para contextualizar campanhas, técnicas, táticas e procedimentos utilizados por agentes maliciosos, contribuindo para melhorar a priorização, a investigação e a resposta a eventos de segurança.
- **Fluxos Automatizados:** Manutenção de recursos para criação de fluxos automatizados de resposta, com gatilhos baseados em novas detecções, eventos de política, alterações em dispositivos e critérios temporais.
- **Ações Automatizadas:** Capacidade de executar ações como contenção de dispositivos, coleta de arquivos, remoção de artefatos, recuperação de conexões de rede, levantamento de processos em execução e envio de notificações por canais como e-mail, Teams e Webhook.
- **Ações remotas de resposta,** incluindo isolamento do dispositivo, contenção de ameaça, quarentena, bloqueio de execução, coleta de artefatos e suporte a investigação.
- **Atualização contínua da inteligência de ameaças** sem necessidade de intervenção manual intensiva.
- **Relatórios executivos, técnicos e operacionais** sobre postura de segurança, incidentes, ameaças detectadas e ações realizadas.
- **Controle de Dispositivos USB:** Manutenção de recursos de controle de dispositivos removíveis, permitindo bloqueio ou liberação conforme classes de dispositivos, como armazenamento em massa, dispositivos móveis, impressoras, adaptadores de rede sem fio e outros periféricos compatíveis.
- **Controle Granular de Acesso:** Capacidade de aplicar permissões específicas para dispositivos de armazenamento, como leitura, escrita, execução ou bloqueio total, reduzindo riscos de exfiltração de dados e uso indevido de mídias removíveis.
- **Gerenciamento de Firewall Local:** Manutenção de recursos de administração de firewall dos dispositivos a partir da console central, permitindo definir regras de tráfego de entrada e saída, protocolos, portas e condições baseadas na localização de rede do dispositivo

- Integração com práticas de operação da CTI/MPPI, permitindo abertura e acompanhamento de chamados, suporte técnico e transferência de conhecimento.

8. Demais requisitos necessários e suficientes à escolha da solução de TIC (Lei 14.133/2021 §1º III; IN 94/2022 art. 16; MOTec)

Requisitos de Negócio (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'a')

8.1. A solução deverá atender aos seguintes requisitos de negócio:

- Proteger, no mínimo, o quantitativo de dispositivos estimado neste ETP, garantindo a proteção contínua de estações de trabalho, servidores e demais dispositivos compatíveis, preservando recursos como prevenção comportamental, aprendizado de máquina, proteção contra manipulação do agente, políticas de atualização, quarentena, isolamento de rede e suporte aos sistemas operacionais Windows e Linux.
- Permitir contratação por subscrição anual, com direito de uso, atualização, suporte e evolução da solução durante a vigência.
- Possuir capacidade de proteção, detecção, investigação e resposta a incidentes em endpoint, mantendo capacidades de análise de arquivos em ambiente controlado, extração de indicadores de comprometimento, visualização da cadeia de ataque, execução de ações remotas e automação de fluxos de resposta. Esses recursos apoiam a equipe técnica na padronização de procedimentos, redução de atividades manuais e agilidade no tratamento de eventos de segurança.
- Permitir gestão centralizada e padronizada das políticas de segurança, utilizando uma abordagem de inteligência cibernética adaptativa para detectar e responder proativamente a novos ataques e comportamentos maliciosos. A solução de proteção dos dispositivos, somada a um trabalho contínuo (24x7) e proativo, é essencial para alcançar níveis mínimos de segurança exigidos pelo órgão.
- Manter as capacidades de proteção atualmente disponibilizadas pela solução CrowdStrike/Falcon implantada no ambiente do MPPI, observados os requisitos técnicos definidos neste ETP e no TR.
- Possuir suporte técnico especializado durante a vigência contratual.
- Disponibilizar documentação técnica e operacional suficiente para operação e auditoria.
- Garantir a proteção dos dados armazenados e Transmitidos em Soluções e Sistemas Governamentais. Com a crescente preocupação em relação à proteção de dados e privacidade, a solução de segurança cibernética desempenha um papel crucial ao assegurar a proteção dos dados armazenados e trafegados em soluções e sistemas governamentais. A implementação dessa solução reduz o risco de violações de segurança, mantendo a conformidade com regulamentações e leis que envolvem o manuseio de informações governamentais.

- Estar alinhada com o Planejamento Estratégico 2022 – 2029 e os valores da Coordenadoria de Tecnologia da Informação do MPPI.

Dos Requisitos de capacitação técnica (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'b' e 'I')

- 8.2. A CONTRATADA deverá promover, quando demandada, capacitação técnica para a equipe do MPPI, com foco na administração da solução, configuração de políticas, análise de alertas, investigação, resposta remota, interpretação de relatórios e boas práticas de operação.
- 8.3. A capacitação poderá ocorrer em formato remoto ou presencial, a critério do MPPI, com carga horária mínima de 04 (quatro) horas, instrutor qualificado na solução ofertada e material de apoio em português ou inglês, podendo ser realizado de segunda a sexta-feira, nos horários de 08:00 às 12:00 ou 14:00 às 18:00, conforme critério do MPPI, garantindo que os alunos absorvam os conhecimentos sobre a implantação da solução fornecida. Todos os custos referentes a deslocamento e/ou softwares de sessão remota necessários serão de responsabilidade da CONTRATADA.
- 8.4. A CONTRATADA deverá realizar, no mínimo, 01 (um) workshop de transferência de conhecimento após a disponibilização da solução, quando solicitado pelo MPPI, e sempre que houver atualização relevante que impacte a operação da plataforma.

Dos Requisitos legais (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'c')

- 8.5. O presente processo de contratação deverá observar, no que couber:
 - 8.5.1. Constituição Federal de 1988.
 - 8.5.2. Lei Complementar nº 123/2006: Institui o Estatuto Nacional da Microempresa e da Empresa de Pequeno Porte, e dá outras providências.
 - 8.5.3. Lei Federal nº 14.133/2021: Estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios.
 - 8.5.4. Lei Federal nº 13.709/2018: Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
 - 8.5.5. Decreto nº 7.845/2012: Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento.
 - 8.5.6. Decreto nº 11.246/2022: Regulamenta o disposto no § 3º do Art. 8º da Lei nº 14.133/2021, para dispor sobre as regras para a atuação do agente de

contratação e da equipe de apoio, o funcionamento da comissão de contratação e a atuação dos gestores e fiscais de contratos.

- 8.5.7. Decreto Estadual nº 21.872/2023: Regulamenta a Lei Federal nº 14.133/2021 no âmbito do Poder Executivo Estadual, para tratar de governança, fase preparatória e procedimental das licitações e contratações diretas para a aquisição de bens, contratações de serviços, obras e serviços de engenharia e sobre bens de luxo.
- 8.5.8. Decreto Estadual nº 21.938/2023: Regulamenta o Sistema de Registro de Preços no âmbito do Estado do Piauí, quando aplicável à contratação.
- 8.5.9. IN SGD/ME nº 94/2022: Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação (TIC) pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Poder Executivo Federal, utilizada como referência para contratações de TIC.
- 8.5.10. IN SEGES/ME nº 65/2021: Dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral.
- 8.5.11. Resolução CNMP nº 283/2024: Disciplina, no âmbito do Ministério Público, os procedimentos relativos à contratação de Soluções de Tecnologia da Informação.
- 8.5.12. Resolução CNMP nº 156/2016: Institui a Política de Segurança Institucional e o Sistema Nacional de Segurança Institucional do Ministério Público, e dá outras providências.
- 8.5.13. CNMP MOTec v1.0, enquanto referência metodológica aplicável à elaboração dos artefatos de planejamento da contratação de TIC no âmbito do Ministério Público.
- 8.5.14. Demais normas, orientações institucionais e atos regulamentares aplicáveis à contratação pública de soluções de Tecnologia da Informação e Comunicação.

Dos Requisitos de manutenção (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'd')

- 8.6. A solução deverá incluir manutenção evolutiva, corretiva e adaptativa durante a vigência da subscrição, contemplando atualizações de versão, correções de falhas, atualização de mecanismos de detecção, atualização de inteligência de ameaças, suporte técnico e adequações necessárias para manutenção da operacionalidade.

- 8.7. A CONTRATADA deverá assegurar que a solução permaneça suportada pelo fabricante durante toda a vigência contratual.

Dos Requisitos temporais (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'e')

- 8.8. A CONTRATADA deverá disponibilizar as subscrições anuais contratadas no prazo máximo de 10 (dez) dias úteis, contado da confirmação do recebimento da Ordem de Serviço, Nota de Empenho ou instrumento equivalente. A confirmação de recebimento, realizada por meio eletrônico ou pelo sistema oficial de comunicação do MPPI, constituirá o marco inicial da contagem do prazo.
- 8.9. A solução CrowdStrike/Falcon já possui console implantada e em funcionamento no MPPI. Por essa razão, não será exigida a implantação de nova console como condição inicial da contratação.
- 8.9.1. Após a disponibilização das subscrições, a CONTRATADA deverá, quando aplicável, validar a continuidade do acesso à console existente, a ativação das licenças, a aplicação das políticas vigentes, a comunicação dos agentes ou sensores e o funcionamento da solução, no prazo máximo de 15 (quinze) dias corridos, contado da comunicação formal da disponibilização das subscrições ao MPPI.
- 8.9.2. A sequência de execução será: a) emissão da Ordem de Serviço, Nota de Empenho ou instrumento equivalente; b) confirmação do recebimento pela CONTRATADA; c) disponibilização das subscrições em até 10 (dez) dias úteis; d) comunicação formal da disponibilização ao MPPI; e) validação, configuração complementar e comprovação do funcionamento em até 15 (quinze) dias corridos.
- 8.10. A vigência contratual terá início na data de assinatura do instrumento e será de 12 (doze) meses acrescida de 90 (noventa) dias corridos, de modo que seu termo final seja objetivamente determinável desde a celebração do contrato. A eficácia do instrumento ficará condicionada à sua divulgação no Portal Nacional de Contratações Públicas – PNCP, não podendo ser exigida qualquer prestação da CONTRATADA antes desse marco. O período de cobertura de cada subscrição será de 12 (doze) meses e deverá permanecer integralmente compreendido na vigência contratual, sem que a data de ativação ou o término da cobertura alterem o termo final previamente estabelecido para o contrato.
- 8.10.1. A adoção de ciclo de cobertura de 12 (doze) meses, inserido em vigência contratual de 12 (doze) meses acrescida de 90 (noventa) dias corridos, em lugar do período ordinário de 24 (vinte e quatro) meses previsto para serviços continuados no art. 5º do Ato PGJ/PI nº 1.415/2024, decorre das peculiaridades da contratação: a unidade de fornecimento corresponde a subscrição anual por dispositivo; os preços de mercado e a pesquisa realizada foram normalizados para ciclos anuais; o Sistema de Registro de Preços pressupõe contratações conforme demanda e disponibilidade orçamentária; e a evolução tecnológica das soluções de segurança recomenda avaliação periódica da necessidade, da vantajosidade e da adequação técnica. A margem adicional de 90 (noventa) dias corridos destina-se a assegurar prazo

contratual suficiente para os atos que antecedem e acompanham a execução, sem ampliar o período anual de cobertura contratado.

8.10.2. A contratação por ciclo anual não prejudica a continuidade da proteção, que será preservada mediante planejamento tempestivo e, quando demonstradas a necessidade, a vantajosidade, a disponibilidade orçamentária e a regularidade da execução, eventuais prorrogações regularmente formalizadas, observadas as condições estabelecidas no Termo de Referência e na legislação aplicável.

8.10.3. A vigência total, incluído o período inicial e todas as prorrogações, não poderá ultrapassar 10 (dez) anos, nos termos dos arts. 106 e 107 da Lei nº 14.133/2021.

Descrição	Início da Execução	Prazo de cobertura do serviço
Início da cobertura do serviço Subscrição anual para solução corporativa EDR de detecção e resposta a incidentes de segurança cibernética em endpoints, com prevenção, investigação, resposta remota, caça de ameaças, inteligência de ameaças, console centralizada em nuvem, agente/sensor e suporte técnico. (Item 1)	Disponibilização em até 10 (dez) dias úteis após a confirmação do recebimento da Ordem de Serviço pela CONTRATADA; ativação/configuração, quando aplicável, em até 15 dias corridos após a comunicação formal da disponibilização.	12 (doze) meses por subscrição anual contratada, devendo o período integral de cobertura permanecer compreendido na vigência do respectivo contrato.

Dos Requisitos de segurança e privacidade (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'f')

- 8.11. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações a que tenha acesso durante a execução contratual, sendo vedada a divulgação, reprodução, compartilhamento ou utilização para finalidade diversa da execução do objeto.
- 8.12. A solução e os serviços deverão observar as normas de Segurança da Informação, Privacidade e Proteção de Dados, especialmente a Lei nº 13.709/2018 — LGPD.
- 8.13. Caso a solução processe dados em nuvem, a CONTRATADA deverá assegurar confidencialidade, integridade, disponibilidade e autenticidade das informações, mantendo controles de acesso, trilhas de auditoria, criptografia em trânsito e em repouso, quando aplicável, e mecanismos de comunicação de incidentes.
- 8.14. A CONTRATADA deverá informar imediatamente ao MPPI qualquer incidente de segurança, vulnerabilidade relevante ou violação de sigilo que possa afetar a solução, os dados, a operação ou o ambiente institucional.
- 8.15. O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

- 8.16. A CONTRATADA será expressamente responsabilizada quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, códigos-fonte e artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venham a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de aplicação de sanção e outras reprimendas previstas em lei, independentemente da classificação de sigilo conferida pelo Ministério Público do Estado do Piauí a tais documentos.
- 8.17. A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, do Ministério Público do Estado do Piauí, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.
- 8.18. Os representantes, empregados e colaboradores da CONTRATADA deverão zelar pela manutenção do sigilo absoluto de dados, informações, documentos e especificações técnicas, que tenham conhecimento em razão dos serviços executados.
- 8.19. Todas as informações, imagens e documentos a serem manuseados e utilizados são de propriedade do Ministério Público do Estado do Piauí e não poderão ser repassados, copiados, alterados ou absorvidos pela CONTRATADA sem expressa autorização do Ministério Público do Estado do Piauí, de acordo com o Termo de Compromisso de Manutenção do Sigilo a ser disponibilizado e firmado entre o Ministério Público do Estado do Piauí e a CONTRATADA.
- 8.20. Cada profissional a serviço da CONTRATADA deverá estar ciente de que a estrutura computacional do órgão não poderá ser utilizada para fins particulares, sendo que quaisquer ações que tramitem em sua rede poderão ser auditadas.
- 8.21. O serviço deve passar por manutenção de acordo com os intervalos e especificações de serviço recomendados pelo fornecedor e acordados com a CONTRATADA.
- 8.22. Devem ser mantidos registros sobre todas as falhas ocorridas ou suspeitadas e sobre todas as manutenções preventivas e corretivas.
- 8.23. Os produtos deverão apresentar política de privacidade oferecida pelo fabricante a fim de garantir o sigilo dos dados consultados através dos softwares licenciados.
- 8.24. A CONTRATADA se compromete a manter sigilo absoluto em relação a todos os dados gerados no processo de prestação dos serviços.
- 8.25. A CONTRATADA deverá respeitar as normas nacionais de proteção de dados e informações vigentes, sobretudo considerando a possibilidade de custódia de conhecimentos, informações e dados

pelo prestador de serviços, observadas as seguintes diretrizes:

- 8.26. Garantia de aplicabilidade da legislação brasileira sobre os princípios, diretrizes e responsabilidades relacionados à segurança da informação e à proteção de dados.
- 8.27. Garantia que, em qualquer hipótese, a Administração tem a tutela absoluta sobre os conhecimentos, informações e dados produzidos pelos serviços.
- 8.28. Vedado o uso corporativo dos conhecimentos, informações e dados pelo prestador de serviço.
- 8.29. Possuir Plano de Continuidade, Recuperação de Desastres e Contingência de Negócio, que possa ser testado regularmente, objetivando a disponibilidade dos dados e serviços em caso de interrupção.
- 8.30. Desenvolver e colocar em prática procedimentos de respostas a incidentes relacionados com os serviços.
- 8.31. A CONTRATADA deverá seguir as normas internas de segurança da informação do Ministério Público do Estado do Piauí, bem como suas atualizações.
- 8.32. A CONTRATADA será expressamente responsabilizada quanto à manutenção de sigilo absoluto sobre quaisquer dados, informações, códigos-fonte e artefatos, contidos em quaisquer documentos e em quaisquer mídias, de que venham a ter conhecimento durante a execução dos trabalhos, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de aplicação de sanção e outras penalidades previstas na legislação vigente, independentemente da classificação de sigilo conferida pelo Ministério Público do Estado do Piauí a tais documentos.
- 8.33. A CONTRATADA não poderá divulgar quaisquer informações a que tenha acesso em virtude dos trabalhos a serem executados ou de que tenha tomado conhecimento em decorrência da execução do objeto, sem autorização, por escrito, do Ministério Público do Estado do Piauí, sob pena de aplicação das sanções cabíveis, além do pagamento de indenização por perdas e danos.
- 8.34. Cada profissional da CONTRATADA deverá assinar termo declarando estar ciente de que a estrutura computacional disponibilizada pelo Ministério Público do Estado do Piauí não poderá ser utilizada para fins particulares, e que a navegação em sítios da Internet e as correspondências em meio eletrônico utilizando o endereço do Ministério Público do Estado do Piauí ou acessadas a partir dos seus equipamentos poderão ser auditadas.
- 8.35. Cada profissional da CONTRATADA deverá assinar termo de compromisso declarando total obediência às normas de segurança vigentes ou que venham a ser implantadas, a qualquer tempo, no Ministério Público do Estado do Piauí.

Dos Requisitos sociais, ambientais, culturais e de sustentabilidade (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'g')

- 8.36. A documentação técnica, relatórios e materiais de capacitação deverão ser entregues preferencialmente em formato digital, reduzindo uso de papel e impressão.
- 8.37. A solução baseada em nuvem deverá evitar a necessidade de aquisição de infraestrutura local adicional, reduzindo consumo de energia, espaço físico, descarte de equipamentos e custos ambientais indiretos.
- 8.38. Quando houver uso de equipamentos ou mídias pela CONTRATADA, deverão ser observadas boas práticas de sustentabilidade, descarte adequado e logística reversa, quando aplicável.

Dos Requisitos da arquitetura tecnológica (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'h')

- 8.39. A solução deverá possuir arquitetura compatível com o ambiente corporativo do MPPI, observando, no mínimo:
 - Console de gerenciamento 100% web ou em nuvem, com acesso seguro por perfis de usuário.
 - Agente/sensor leve, com baixo impacto de desempenho no endpoint.
 - Comunicação segura entre agente e console, preferencialmente com criptografia ponta a ponta ou TLS.
 - Suporte a políticas por grupos, unidades, perfis de dispositivos ou criticidade.
 - Capacidade de operar em endpoints internos, externos ou remotos, mesmo fora da rede corporativa, desde que com conectividade à internet.
 - Integração com mecanismos de autenticação e controle de acesso administrativo, preferencialmente com MFA.
 - Exportação de relatórios e eventos para fins de auditoria e gestão.

Dos Requisitos de projeto e de implementação (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'i')

- 8.40. A contratação não envolve desenvolvimento de software sob encomenda. A implementação consistirá na disponibilização da solução, ativação de licenças, configuração de políticas, validação operacional, instalação ou atualização de agentes/sensores e transferência de conhecimento.
- 8.41. A CONTRATADA deverá apresentar plano de implantação contendo cronograma, etapas, responsabilidades, pré-requisitos, riscos, procedimentos de rollback e critérios de aceite.

Dos Requisitos de implantação (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'j')

- 8.42. A implantação deverá preservar a continuidade operacional do MPPI e minimizar indisponibilidades.

- 8.43. A equipe da CONTRATADA deverá apoiar remotamente a CTI/MPPI na ativação, configuração e validação da solução, inclusive quanto à instalação ou atualização dos agentes/sensores.
- 8.44. Para a implantação, o MPPI não disponibilizará infraestrutura local adicional de hardware para console de gerenciamento, devendo a solução permanecer baseada em arquitetura web ou em nuvem, conforme características do objeto. O MPPI poderá utilizar mecanismos próprios de distribuição de agentes, tais como GPO, ferramentas de gestão de endpoints ou scripts corporativos, cabendo à CONTRATADA orientar a equipe técnica quanto aos pacotes, parâmetros e melhores práticas.
- 8.45. A CONTRATADA deverá orientar a equipe técnica do MPPI quanto aos pacotes de instalação, parâmetros recomendados, melhores práticas de implantação, critérios de validação, eventuais pré-requisitos, procedimentos de rollback e comprovação de funcionamento da solução.
- 8.46. A solução deverá estar funcional e licenciada para o quantitativo contratado, comprovada por relatório, declaração ou console do fabricante/fornecedor.

Dos Requisitos de garantia, manutenção e assistência técnica (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'k')

- 8.47. A CONTRATADA deverá fornecer suporte técnico com operação assistida durante toda a vigência contratual, sem limite de chamados, abrangendo dúvidas, falhas, atualização de versões, apoio em configuração, análise de eventos e orientação de resposta a incidentes.

- 8.48. O suporte deverá observar, no mínimo, os seguintes níveis de atendimento:

Severidade	Descrição	Início do atendimento remoto	Prazo máximo de solução ou encaminhamento qualificado
Crítica	Indisponibilidade e relevante da solução ou incidente crítico com impacto operacional.	Até 2 horas	Até 72 horas
Alta	Impacto relevante em funcionalidade importante, com operação limitada.	Até 4 horas	Até 5 dias

Severidade	Descrição	Início do atendimento remoto	Prazo máximo de solução ou encaminhamento qualificado
Normal	Dúvida ou problema contornável, sem indisponibilidade e relevante.	Até 8 horas	Até 8 dias
Baixa	Consulta técnica, orientação, transferência de conhecimento ou ajuste simples.	Até 24 horas	Até 10 dias

- 8.49. Quando a solução depender de correção do fabricante, a CONTRATADA deverá acompanhar o chamado e manter o MPPI informado, sem alterar o protocolo inicial. Além disso, durante os atendimentos dos chamados, para efeitos de apuração do tempo despendido para solução, serão desconsiderados os períodos em que o Ministério Público do Estado do Piauí estiver responsável por executar alguma ação necessária para a análise e solução da ocorrência ou quando for necessário aguardar alguma correção por parte do fabricante que não impacte no funcionamento e utilização do ambiente, sendo permitido nestes casos pausar ou interromper o chamado, mas sem alterar o número inicial de protocolo/número de abertura do mesmo. O nível de severidade será atribuído pela equipe autorizada da CONTRATANTE no momento da abertura do chamado e poderá ser reclassificado pela equipe da CONTRATADA, caso seja necessário.
- 8.50. A CONTRATADA deverá fornecer suporte da solução durante toda a vigência contratual para atualizações de versão e acionamento em nível de resolução de problemas pelo próprio fabricante, se necessário, conforme previsto neste Termo de Referência e seus Apêndices.
- 8.51. A CONTRATADA deverá prestar, pelo período da vigência contratual, Suporte Técnico com Operação Assistida e Transferência de Conhecimento, que deverão ser do tipo telefônico e/ou internet 24 (vinte e quatro) horas por dia e 07 (sete) dias por semana, sendo realizado por profissionais especializados, e devendo cobrir todo e qualquer defeito ou demanda apresentada.
- 8.52. Os serviços de suporte e manutenção consistem em atendimentos a dúvidas técnicas quanto ao uso do ambiente e atualizações de versões para correções de eventuais problemas identificados.
- 8.53. As atividades de suporte técnico serão realizadas, a critério do MPPI, em seu ambiente, a partir da assinatura do Contrato e

durante toda sua vigência contratual.

- 8.54. O suporte técnico com operação assistida poderá ser utilizado para melhoria das configurações do ambiente, continuidade do processo de implantação e integração dos dispositivos e desenvolvimento de competências técnicas, compreendendo o seguinte escopo mínimo:
 - 8.54.1. Orientação quanto às melhores práticas para implementação e integração da solução no ambiente do MPPI.
 - 8.54.2. Apoio e/ou atuação direta na execução de procedimentos de atualização para novas versões da solução e seu
 - 8.54.3. impacto nos agentes e/ou sensores já instalados no ambiente do MPPI.
 - 8.54.4. Aplicação de melhores práticas para implementação dos produtos de software adquiridos.
 - 8.54.5. Realização de estudos e configuração do ambiente e implementação das integrações necessárias, instáveis ou com comportamento errático, caso aconteçam.
 - 8.54.6. Realização de estudos para melhoria do ambiente atual, políticas, prevenções, análises e aumento da proteção para diminuição e mitigação de vulnerabilidades encontradas.
 - 8.54.7. Implementação de novas integrações que não tenham ainda sido efetivadas ou sejam necessárias novas integrações.
 - 8.54.8. Identificação de melhorias e respectivo tratamento (melhoria de parametrização).
 - 8.54.9. Parametrização da solução, de acordo com as regras e políticas disponíveis em sua console única e definidas pelo MPPI.
 - 8.54.10. Apoio para execução de procedimentos de atualização para novas versões dos agentes e/ou sensores instalados nos dispositivos.
 - 8.54.11. Apoio à elaboração e adequação de relatórios executivos, gerenciais e operacionais quando necessário.
 - 8.54.12. Suporte avançado para estratégia e planejamento de migrações e adequações nos agentes e sensores instalados nos dispositivos protegidos pela solução.
 - 8.54.13. Avaliação e comparação de novas funcionalidades de forma remota e, se necessário, presencial, mediante solicitação prévia da equipe do Ministério Público do Estado do Piauí.
- 8.55. Apoio quanto a obstáculos operacionais e de planejamento, incluindo, sem limitação, a configuração dos componentes da solução, problemas de usabilidade, diagnósticos de problemas técnicos e análises de tendências associadas à solução e seus componentes.
- 8.56. A CONTRATANTE poderá solicitar durante toda a vigência contratual

do serviço, transferência de conhecimento e/ou operação assistida de segunda a sexta-feira em horário comercial como parte integrante do serviço prestado, para isso poderá ser solicitado sessões remotas e/ou presenciais, bem como workshops de transferência de conhecimento para a equipe, para isso serão abertos chamados com severidade “4” classificado como “baixa”.

- 8.57. O treinamento poderá ser de forma remota ou, se for exigido como ação necessária e primordial, deverá ser realizado nas dependências do MPPI, com instrutor certificado na solução e deverá ter carga horária mínima de 04 (quatro) horas, e poderá ser de segunda a sexta-feira, das 08:00 às 12:00 ou das 14:00 às 18:00, à critério do MPPI, de modo que os alunos possam absorver os conhecimentos, acerca da implantação da solução fornecida, sendo todos os custos de deslocamento e/ou softwares de sessão remota necessários por conta e responsabilidade da CONTRATADA, para os casos em que for necessária a forma presencial o prazo de início será estipulado pela equipe do MPPI, podendo ser estendido o prazo máximo do SLA dos chamados de severidade “4” sem prejuízo ou multa ou glosa para a CONTRATADA.
- 8.58. Serão solicitadas no mínimo, 1 (um) workshop de transferência de conhecimento, devendo ser realizado ao final da implantação da solução, para possibilitar a transferência dos conhecimentos para toda a equipe em tempo de execução com a solução funcionando, em produção e devidamente integrada ao ambiente no MPPI.
- 8.59. Para os casos em que houver alguma mudança significativa que reflita na operação da solução ou reflita nos agentes e/ou sensores atualizados nos dispositivos, a CONTRATADA deverá transferir este conhecimento para equipe sempre que ocorrer, para estes casos serão também abertos chamados de severidade “4”.
- 8.60. Os serviços de operação assistida poderão ser de forma remota ou, se for exigido como ação necessária e primordial, deverão ser realizados nas dependências do MPPI, com profissional certificado e devidamente treinado na solução e poderá ser de segunda a sexta-feira, das 08:00 às 12:00 ou das 14:00 às 18:00, à critério do MPPI, de modo que os trabalhos possam ser realizados com qualidade e eficácia, sendo todos os custos de deslocamento e/ou softwares de sessão remota necessários por conta e responsabilidade da CONTRATADA, para os casos em que for necessária a forma presencial o prazo de início será estipulado pela equipe do MPPI, podendo ser estendido o prazo máximo do SLA dos chamados de severidade “4” sem prejuízo ou multa ou glosa para a CONTRATADA.
- 8.61. Será solicitado no mínimo, 1 (uma) sessão de operação assistida por trimestre, e no máximo 2 (duas) sessões por mês, devendo ocorrer logo após a implantação da solução, para possibilitar qualquer nova análise de funcionamento, configuração e/ou modificação necessárias nas implementações e integrações já realizadas, de modo que o funcionamento se mantenha sempre atualizado, em produção e devidamente funcional e integrado aos dispositivos pertencentes ao ambiente do Ministério Público do Estado do Piauí.

- 8.62. O serviço deverá ocorrer durante toda a vigência contratual, e deverá ser disponibilizado pela CONTRATADA um sistema de acompanhamento e controle de chamados onde eles serão registrados com acesso liberado para cada integrante da equipe do Ministério Público do Estado do Piauí e a CONTRATADA, devendo ficar registrado todas as interações sobre o serviço de suporte prestado.
- 8.63. A CONTRATADA deverá disponibilizar sistema de acompanhamento e controle de chamados, com acesso liberado aos integrantes indicados pelo MPPI, permitindo registro, acompanhamento, histórico das interações, classificação de severidade, prazos de atendimento, evidências de tratativas e encerramento formal dos chamados. O sistema deverá permitir abertura de chamados por telefone, e-mail, portal web ou mecanismo equivalente.
- 8.64. Uma vez que a solução estará em produção e funcionando em nuvem, as atividades relacionadas a correções ou atualizações da console, que necessitem indisponibilidade do ambiente, sem prejuízo para o funcionamento dos dispositivos já gerenciados pela solução, deverão ser notificadas ao Ministério Público do Estado do Piauí com antecedência mínima de 1 (um) dia útil.

Dos Requisitos de experiência profissional (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'm')

- 8.65. Documentos de apoio que podem ser apresentados junto com os atestados de capacidade técnica:
- 8.65.1. Declaração do fabricante do produto atestando ao proponente sua condição de representante, distribuidor ou de revendedor.
- 8.65.2. Declaração do fabricante, no caso de produtos de procedência estrangeira, acompanhada de tradução juramentada para o idioma nacional, atestando ao proponente sua condição de importador e, ainda,
se for o caso, do importador para o proponente atestando sua qualidade de distribuidor, representante ou revendedor. e/ou
- 8.65.3. Impressão de página oficial do fabricante do produto na Internet, onde o proponente figure numa das hipóteses acima (distribuidor, representante ou revendedor), devendo ser informado o endereço da página para uma possível confirmação de conteúdo.
- 8.66. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.
- 8.66.1. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.
- 8.66.2. O fornecedor disponibilizará todas as informações necessárias à

comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

- 8.67. Para fins de qualificação técnica, são consideradas parcelas de maior relevância técnica da contratação aquelas cuja execução inadequada possa comprometer diretamente a continuidade da proteção dos dispositivos, a disponibilidade da solução, a capacidade de resposta a incidentes ou a operação segura do ambiente do MPPI:

- 8.67.1. Fornecimento de subscrição/licenciamento de solução corporativa de proteção de endpoints, EDR, EPP ou tecnologia equivalente, destinada a ambientes corporativos, contemplando estações de trabalho e servidores.

Justificativa: esta parcela é essencial por compreender a disponibilização do direito de uso da solução responsável pela proteção contínua dos dispositivos do MPPI. Eventual falha no fornecimento, licenciamento ou manutenção da subscrição poderá ocasionar perda de cobertura, indisponibilidade de funcionalidades de segurança e comprometimento da continuidade da proteção do ambiente.

- 8.67.2. Implantação, ativação, configuração, atualização ou integração de solução corporativa de proteção de endpoints, incluindo configuração de console, políticas de segurança, agentes ou sensores e validação do funcionamento da solução.

Justificativa: trata-se de atividade tecnicamente relevante, pois configurações inadequadas poderão resultar em dispositivos sem proteção, políticas aplicadas incorretamente, falhas na geração de alertas, indisponibilidade de recursos de resposta ou redução da efetividade dos mecanismos de segurança. A experiência prévia da licitante é necessária para reduzir riscos durante a implantação, atualização ou adequação da solução ao ambiente do MPPI.

- 8.67.3. Prestação de suporte técnico especializado e operação assistida para solução corporativa de proteção de endpoints, incluindo tratamento de falhas, apoio à configuração, atualização, análise de eventos e orientação para resposta a incidentes.

Justificativa: o suporte técnico e a operação assistida são essenciais para assegurar a continuidade operacional da solução durante toda a vigência contratual. A ausência de capacidade técnica adequada poderá aumentar o tempo de indisponibilidade, dificultar a resolução de incidentes e comprometer a capacidade do MPPI de manter a solução corretamente configurada e operacional.

- 8.67.4. Transferência de conhecimento relacionada à administração e operação da solução de proteção de endpoints.

Justificativa: esta atividade é relevante para assegurar que a

equipe técnica do MPPI possua conhecimento suficiente para administrar políticas, analisar alertas, executar procedimentos operacionais e acompanhar a execução dos serviços, reduzindo dependência operacional da CONTRATADA.

8.67.5. Para comprovação da capacidade técnico-operacional relativa às parcelas de maior relevância, será exigida experiência anterior em ambiente com, no mínimo, 800 (oitocentos) dispositivos protegidos, correspondente a 50% do quantitativo máximo estimado de 1.600 dispositivos da presente contratação, admitido o somatório de atestados nas condições estabelecidas neste ETP.

8.67.6. A comprovação poderá ser realizada por um ou mais atestados de capacidade técnica, não sendo exigido que todas as parcelas tenham sido executadas em um único contrato, desde que o conjunto da documentação apresentada demonstre experiência compatível com as atividades consideradas de maior relevância técnica.

Dos Requisitos de formação da equipe (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'n')

8.68. A CONTRATADA deverá disponibilizar profissionais capacitados e, quando aplicável, certificados pelo fabricante ou por entidade reconhecida na tecnologia ofertada, especialmente para atividades de implantação, suporte, configuração e capacitação.

8.69. Recomenda-se que a equipe mínima de suporte contenha três profissionais com conhecimento em segurança de endpoints, análise de incidentes, redes, sistemas operacionais Windows/Linux e administração de plataformas em nuvem. Além disso, eles devem ser certificados pela fabricante na solução contratada.

Dos Requisitos de metodologia de trabalho (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'o')

8.70. A execução será condicionada à emissão de Ordem de Serviço, devendo a CONTRATADA acompanhar a execução, registrar ocorrências, comunicar riscos e manter canal formal de atendimento.

8.71. As atividades deverão seguir boas práticas de segurança da informação, gestão de mudanças, documentação técnica, registro de chamados, rastreabilidade e comunicação formal com o MPPI.

Dos Requisitos de segurança dos ativos de TI (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'p')

8.72. A contratação deverá observar a Resolução CNMP nº 156/2016 e demais normas de segurança institucional do Ministério Público.

8.73. A CONTRATADA deverá zelar pela segurança dos ativos de TI do MPPI, abstendo-se de executar qualquer ação não autorizada, coletar dados além do necessário à prestação do serviço ou alterar configurações sem validação da equipe técnica do MPPI.

- 8.74. Todo acesso da CONTRATADA ao ambiente do MPPI dependerá de autorização prévia e deverá observar as políticas de segurança de acesso do órgão.

*Dos Requisitos de previsão da exigência para realização de Prova de Conceito
(Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'q')*

- 8.75. A licitante provisoriamente classificada em primeiro lugar deverá, após o encerramento da fase de lances e quando convocada pelo Pregoeiro, apresentar, juntamente com a proposta ajustada ao último lance, a Planilha de Requisitos Técnicos Obrigatórios constante do Anexo B do Termo de Referência, devidamente preenchida e assinada, acompanhada da documentação técnica comprobatória correspondente.
- 8.75.1. A Planilha de Requisitos Técnicos Obrigatórios - Anexo B do Termo de Referência - deverá relacionar os requisitos técnicos mínimos constantes do Anexo A do Termo de Referência - Descrição dos Requisitos Técnicos Mínimos da Solução EDR -, indicando, para cada requisito, o atendimento, o documento comprobatório e a respectiva página, seção ou referência que permita sua verificação objetiva pela equipe técnica do MPPI.
- 8.75.2. A convocação para apresentação da Planilha, dos documentos técnicos complementares e, quando aplicável, para realização da Prova de Conceito ocorrerá por meio do sistema eletrônico utilizado no certame, nos prazos e condições definidos no edital.
- 8.75.3. O Anexo B reproduz, individualmente, os requisitos técnicos mínimos do Anexo A e destina-se a correlacionar cada requisito ao fabricante, produto ou módulo ofertado e ao documento, página, seção, URL oficial ou outra evidência técnica correspondente.
- 8.75.4. A Planilha de Requisitos Técnicos Obrigatórios e a documentação técnica integram a análise da proposta e não constituem documentos de habilitação.
- 8.76. A Prova de Conceito ou teste de conformidade terá caráter exclusivamente complementar e somente poderá ser exigida se, após a análise da proposta, do Anexo B e da documentação técnica, permanecer dúvida objetiva e relevante sobre requisito técnico mínimo específico.
- 8.76.1. A convocação deverá identificar os requisitos duvidosos, os procedimentos, os critérios objetivos de avaliação, o ambiente, a data, o prazo e os responsáveis pelo acompanhamento. A POC ficará limitada aos requisitos expressamente indicados na convocação, sendo vedada a exigência genérica de teste de todos os requisitos do Anexo A.
- 8.76.2. A licitante será desclassificada somente se deixar de comprovar requisito mínimo obrigatório após a análise documental e, quando cabível, a POC complementar, assegurado o registro motivado do resultado. O Ministério Público do Estado do Piauí realizará diligências objetivando comprovar a veracidade das informações prestadas pela LICITANTE. Caso fique caracterizado o uso inidôneo de documentos probatórios da capacidade jurídica, econômico-

financeira e técnica da LICITANTE, a mesma ficará impedida de licitar e contratar com a União, e será descredenciada do SICAF para prazo previsto em lei, sujeitando-se às penalidades administrativas, cíveis e penais previstas na lei.

- 8.77. O resultado do teste será apresentado no prazo de até 02 (dois) dias úteis, a contar do dia seguinte ao final do Teste de Conformidade.
- 8.78. Prova será pública e todas as Licitantes interessadas e credenciadas no certame poderão assistir. A licitante poderá atender a fase de demonstração com até 03 (três) representantes legais. As demais licitantes interessadas em acompanhar poderão participar com 01 (um) representante legal cada. Todos os participantes serão registrados em ata, durante os dias em que ocorrer a demonstração.
- 8.79. O Ministério Público do Estado do Piauí disponibilizará máquinas virtuais para o caso de solução baseada em software sem sistema operacional, sendo os demais custos relativos à demonstração/teste de conformidade das soluções de responsabilidade da licitante, não tendo direito a qualquer indenização, inclusive no caso de não ser CLASSIFICADA.

DA JUSTIFICATIVA DA EXIGÊNCIA DE PROVA DE CONCEITO (Obrigatório)

- 8.80. A Prova de Conceito justifica-se pela criticidade do objeto e pela necessidade de assegurar que a solução ofertada seja compatível com o padrão técnico atualmente utilizado pelo MPPI. A contratação envolve proteção de ativos institucionais sensíveis, resposta a incidentes e continuidade operacional; portanto, a validação prática reduz riscos de contratação de solução inadequada, mitiga impugnações técnicas posteriores e assegura aderência ao interesse público.

Do Reajuste (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 'r')

- 8.81. Os preços registrados permanecerão fixos e irreajustáveis pelo prazo de 12 (doze) meses, contado da data do orçamento estimado ou da apresentação da proposta, conforme definido no Termo de Referência.
- 8.82. Caso haja contratação com vigência superior a 12 meses, os preços poderão ser reajustados após o interregno mínimo de 12 meses, utilizando-se o ICTI/IPEA para serviços de TIC, quando aplicável, ou outro índice definido justificadamente no instrumento convocatório.

Da aplicação da margem de preferência (Resolução CNMP 283/2024, Art. 17, inciso I, alínea 's')

- 8.83. A aplicação de margem de preferência foi considerada. Entretanto, por se tratar de subscrição de solução de software e serviços de TIC, sem enquadramento identificado como produto manufaturado nacional sujeito à margem de preferência normal ou adicional, a margem de preferência não será aplicada, salvo superveniência normativa ou enquadramento comprovado na fase de planejamento final.

Da modalidade de remuneração a ser adotada (Resolução CNMP 283/2024, Art. 17, inciso II)

- 8.84. A remuneração será por unidade de subscrição anual efetivamente contratada, conforme quantitativo demandado por Ordem de Serviço ou instrumento equivalente, observados os preços registrados na ARP.

Do Parcelamento da solução de TIC (Resolução CNMP 283/2024, Art. 17, inciso III, alínea 'a')

Justificativas para o não parcelamento (Lei 14.133/2021, Art. 18, inciso VIII) - ITEM OBRIGATÓRIO

- 8.85. Não se recomenda o parcelamento da solução EDR em múltiplos itens ou fornecedores, pois a proteção, detecção, investigação, resposta, console de gerenciamento, agente/sensor, suporte e atualizações compõem uma solução única e integrada.
- 8.86. O parcelamento poderia gerar incompatibilidade entre agentes, consoles e mecanismos de resposta, dificuldade de correlação de eventos, múltiplas fontes de logs, aumento de superfície de falha, sobreposição de políticas de segurança e complexidade de suporte. Tais riscos são incompatíveis com o objetivo de proteção contínua do ambiente do MPPI.
- 8.87. A contratação em item/lote único preserva a interoperabilidade, reduz riscos operacionais, simplifica a fiscalização, mantém a rastreabilidade dos eventos e assegura um único ponto de responsabilização técnica.

Da Reserva de cotas para microempresas e empresas de pequeno porte (Lei 14.133/2021, Art. 4; Lei Comp. 123/2006, arts. 42 a 49)

- 8.88. Não será aplicada reserva de cota de 25% para ME/EPP, em razão da natureza indivisível da solução, da necessidade de integração técnica e da criticidade do objeto. Permanecerão assegurados os benefícios legais aplicáveis às ME/EPP, incluindo empate ficto, quando cabível.

Do Desempate ficto em favor de ME/EPP (Lei 123/2006, Art. 44)

- 8.89. Será assegurado o tratamento diferenciado previsto na Lei Complementar nº 123/2006, especialmente quanto ao empate ficto, observadas as condições legais e as regras do edital.

Da Subcontratação, Consórcios e Cooperativas (Resolução CNMP 283/2024, Art. 17, inciso III, alínea 'b'; Lei 14.133/2021, Art. 16)

Justificativa para a não participação de Consórcios e Subcontratação (Resolução CNMP nº 283/2024, Art. 17, inciso I, alínea 's')

- 8.90. A subcontratação do objeto principal não será admitida, a fim de manter controle direto sobre qualidade, prazos, suporte, sigilo, responsabilidade técnica e conformidade contratual.
- 8.91. A participação de empresas em consórcio não será admitida, pois o objeto não apresenta complexidade ou vulto que impeça sua execução por empresa individualmente habilitada no mercado, e a

pluralidade de responsáveis poderia aumentar riscos de gestão e responsabilização.

Justificativa para a não participação de Cooperativas

- 8.92. A participação de cooperativas não é recomendada para a execução do objeto, considerando que a contratação exige fornecimento de subscrição, suporte técnico especializado, garantia de continuidade, relacionamento com fabricante, disponibilidade operacional e responsabilidade empresarial contínua, características típicas de fornecedores regulares do mercado de TIC.

Da Garantia Contratual (Garantia da Contratação) (Modelo TR AGU, abr. 2026; Lei 14.133/2021, Art. 96)

Justificativa para Exigência de Garantia Contratual

- 8.93. Recomenda-se a exigência de garantia contratual no percentual de 5% do valor contratado, conforme autorizado pela Lei nº 14.133/2021, em razão da criticidade do objeto para a segurança da informação do MPPI e dos riscos decorrentes de eventual inadimplemento, interrupção de licenças, falha de suporte ou indisponibilidade da solução.
- 8.94. A garantia visa resguardar o interesse público, proteger o erário e reforçar a segurança jurídica da contratação.

Da indicação e/ou vedação de marcas ou modelos (Modelo TR AGU, abr. 2026; Lei 14.133/2021, Art. 41)

- 8.95. A presente contratação adota a solução CrowdStrike/Falcon como solução padronizada para proteção EDR dos dispositivos do MPPI, em razão da necessidade de manutenção do ambiente atualmente implantado e das justificativas técnicas, operacionais e econômicas apresentadas neste ETP.
- 8.96. A indicação da solução CrowdStrike/Falcon não decorre de preferência imotivada por marca, mas da necessidade de preservação da continuidade operacional, das configurações e políticas existentes, dos investimentos realizados, do conhecimento técnico da equipe e da mitigação dos riscos e custos associados à substituição da plataforma.

Realização de vistoria (Quando necessário)

- 8.97. A vistoria técnica será facultativa. O objetivo é permitir que as licitantes conheçam, quando julgarem necessário, as condições do ambiente computacional físico e lógico do MPPI, especialmente aspectos relacionados à infraestrutura, conectividade, políticas de segurança e formas de implantação.
- 8.98. A não realização da vistoria não poderá fundamentar alegação posterior de desconhecimento das condições de execução do objeto.

Da carta de solidariedade para o fornecimento de bens

- 8.99. Não será exigida carta de solidariedade do fabricante, por se tratar de contratação de subscrição e serviços de TIC. A Administração poderá, contudo, exigir comprovação de que a licitante é autorizada a comercializar, implantar ou prestar suporte à solução ofertada, por meio de documentação hábil, quando necessário para mitigar riscos de execução.

9. Estimativa da demanda - quantidade de bens e serviços (Lei 14.133/2021 §1º IV; IN 94/2022 art. 11 I; MOTec) - ITEM OBRIGATÓRIO

Item	CATSER	Descrição	Unidade	Quantidade estimada
1	27502	Subscrição anual para solução corporativa EDR de detecção e resposta a incidentes de segurança cibernética em endpoints, com prevenção, investigação, resposta remota, caça de ameaças e suporte técnico.	Dispositivo	1.600

- 9.1. Para fins do Sistema de Registro de Preços, estabelece-se como quantitativo máximo estimado passível de contratação durante a vigência da Ata de Registro de Preços o total de 1.600 (mil e seiscentas) subscrições anuais individuais, cada uma destinada à proteção de 1 (um) dispositivo.
- 9.1.1. As contratações decorrentes da Ata poderão ocorrer de forma parcelada, conforme a necessidade efetiva do MPPI, a disponibilidade orçamentária e o saldo registrado, não havendo obrigação de contratação integral do quantitativo máximo estimado.
- 9.1.2. Para fins de padronização dos artefatos, a unidade de fornecimento será “subscrição anual por dispositivo”, correspondendo cada unidade ao direito de uso da solução EDR para proteção de 1 (um) dispositivo pelo período de 12 (doze) meses.
- 9.1.3. O quantitativo de 1.600 unidades não representa consumo inicial ou quantidade mínima obrigatória, constituindo o limite máximo estimado de subscrições passíveis de contratação durante a vigência da ARP.
- 9.1.4. Para fins de classificação no Catálogo de Serviços – CATSER, adota-se o código 27502 – Cessão temporária de direitos sobre programas de computador / locação de software, por ser compatível com a natureza da presente contratação, que consiste em subscrição temporária anual de direito de uso da solução EDR. Não se adota o código 27456, destinado a licenciamento de direitos permanentes de uso de software, uma vez que a contratação não transfere direito de uso perpétuo da solução ao MPPI.

Memória de cálculo:

Componente	Quantidade	Observação
Servidores computacionais inventariados	119	Conforme levantamento da CTI
Estações de trabalho inventariadas	1.781	Conforme levantamento da CTI
Total de equipamentos inventariados	1.900	119 + 1.781
Equipamentos fora do escopo EDR	300	Deverão ser discriminados no inventário e justificados tecnicamente
Quantitativo máximo estimado da ARP	1.600	Subscrições anuais individuais por dispositivo

- 9.2. A estimativa do quantitativo da contratação foi definida a partir da análise do ambiente efetivamente protegido pelo MPPI, do histórico da contratação vigente e da necessidade de manutenção de margem operacional durante a vigência da Ata de Registro de Preços.
- 9.2.1. Na data do levantamento realizado pela Coordenadoria de Tecnologia da Informação – CTI, a console de gerenciamento da solução de proteção de dispositivos atualmente utilizada pelo MPPI registrava 1.462 (mil quatrocentos e sessenta e dois) dispositivos, distribuídos entre 1.390 dispositivos Windows, 71 dispositivos Linux e 1 dispositivo macOS, compreendendo estações de trabalho, servidores e controladores de domínio.
- 9.2.2. A contratação anterior da solução, decorrente do Pregão Eletrônico nº 46/2021 e formalizada pelo Contrato nº 03/2022/PGJ, também foi dimensionada para 1.600 dispositivos, quantitativo que vem sendo utilizado como capacidade contratual de referência para proteção do parque computacional do MPPI.
- 9.2.3. Considerando o quantitativo atual de 1.462 dispositivos efetivamente identificados na console, bem como a necessidade de absorver, durante a vigência da Ata, substituições de equipamentos, inclusão de novos dispositivos, renovação do parque computacional e demais variações ordinárias do ambiente tecnológico, estabelece-se uma margem operacional de 138 dispositivos, equivalente a aproximadamente 9,4% do quantitativo atualmente gerenciado.
- 9.2.4. Dessa forma, define-se como quantitativo máximo estimado passível de contratação durante a vigência da Ata de Registro de Preços o total de 1.600 subscrições anuais, sendo cada subscrição destinada à proteção de um único dispositivo. A definição desse quantitativo não implica obrigação de contratação integral, podendo as subscrições ser contratadas conforme a necessidade efetiva da Administração, disponibilidade orçamentária e condições estabelecidas na Ata de Registro de Preços.

9.3. A memória de cálculo é apresentada a seguir:

Elemento	Quantidade
Dispositivos Windows identificados na console da solução do contrato 03/2022	1.390
Dispositivos Linux identificados na console da solução do contrato 03/2022	71
Dispositivos macOS identificados na console da solução do contrato 03/2022	1
Total atual de dispositivos	1.462
Margem operacional estimada	138
Quantitativo máximo estimado para a ARP	1.600

- 9.4. Memória de cálculo:
 $1.390 + 71 + 1 = 1.462$ dispositivos atualmente identificados
 $1.600 - 1.462 = 138$ dispositivos de margem operacional
 $138 \div 1.462 \times 100 \approx 9,4\%$ de margem operacional
- 9.5. Como documentos de suporte à estimativa, deverão ser considerados o histórico de consumo e o relatório ou evidência extraída da console de gerenciamento da atual solução, demonstrando o quantitativo atual de dispositivos, e o Contrato nº 03/2022/PGJ/Pregão Eletrônico nº 46/2021, que evidencia o histórico de contratação de 1.600 dispositivo
- 9.6. O quantitativo poderá ser demandado de forma parcelada, por meio de Ordens de Serviço, durante a vigência da Ata de Registro de Preços, conforme a necessidade real do MPPI.

SOLUÇÃO

10. Levantamento de soluções (Lei 14.133/2021 §1º V; IN 94/2022 art.11 II; MOTec)

- 10.1. A demanda atual requer a contratação de serviços de atualização e suporte para um pacote de ferramentas já em uso no MPPI.
- 10.2. A substituição completa da plataforma CrowdStrike é uma alternativa inviável no contexto do MPPI. Esse processo demandaria meses de planejamento e estudos detalhados das opções disponíveis, considerando os impactos nas rotinas operacionais da CTI, requisitos modificados, treinamento adicional para os servidores e a complexidade da migração e implantação da nova solução.
- 10.3. Considerando a urgência dos serviços necessários, e a total adaptação dos servidores da CTI ao software atual, a substituição completa da

plataforma não é viável neste momento. Optou-se por buscar soluções que garantam a continuidade dos serviços de forma eficiente e sem interrupções significativas nas operações do MPPI.

10.4. Porém, para o estudo, foram consideradas as seguintes alternativas:

Soluções similares

- 10.5. O mercado possui diversas soluções corporativas de proteção de endpoints com recursos EDR, incluindo plataformas baseadas em nuvem, telemetria contínua, análise comportamental e resposta remota.
- 10.6. Foi realizada análise do mercado de soluções de proteção de endpoints, considerando a relevância desse tipo de tecnologia para a prevenção, detecção, investigação e resposta a ameaças cibernéticas em estações de trabalho, notebooks e servidores. As soluções de Endpoint Protection Platform — EPP representam controles essenciais de segurança para proteção dos dispositivos finais, combinando mecanismos de prevenção contra malware, análise comportamental, redução da superfície de ataque, visibilidade centralizada e, quando aplicável, capacidades de detecção e resposta em endpoints.
- 10.7. Com base na análise do relatório Magic Quadrant for Endpoint Protection, publicado pelo Gartner em 2026, observa-se que o mercado de proteção de endpoints é composto por diversos fabricantes com diferentes níveis de capacidade de execução e completude de visão. Entre os fornecedores avaliados no relatório, destacam-se fabricantes como CrowdStrike, Microsoft, SentinelOne, Sophos, Palo Alto Networks, Trend Micro, Bitdefender, Check Point, ESET, Fortinet, Trellix e Broadcom, entre outros.
- 10.8. O relatório do Gartner posiciona a CrowdStrike no quadrante de líderes em Endpoint Protection, evidenciando sua relevância no mercado e sua capacidade de atender organizações que buscam soluções maduras de proteção de endpoints, com administração baseada em nuvem, recursos de prevenção, detecção e resposta, além de capacidades voltadas à investigação de ameaças em dispositivos corporativos.



Gartner

Figura 1 - Quadrante Mágico do Gartner 2026 — Endpoint Protection Platform.

- 10.9. A análise de mercado demonstra que existem alternativas tecnológicas relevantes no segmento de proteção de endpoints. Entretanto, no caso concreto do MPPI, deve-se considerar que a Ministério já utiliza a plataforma CrowdStrike Falcon em seu ambiente tecnológico, com sensores implantados, políticas configuradas, equipe técnica capacitada e processos operacionais estabelecidos para administração, monitoramento, investigação e resposta a eventos de segurança.
- 10.10. Dessa forma, a análise comparativa não se limita à identificação de fabricantes reconhecidos no mercado, mas também considera a aderência da solução ao ambiente atualmente em produção, a preservação dos investimentos já realizados, a continuidade operacional, a redução de riscos de transição e a manutenção da padronização tecnológica da segurança de endpoints do Ministério.
- 10.11. A substituição da plataforma atualmente utilizada poderia gerar necessidade de nova implantação, reconfiguração de políticas, substituição de sensores, reconstrução de integrações, treinamento adicional da equipe, perda de histórico operacional e eventuais lacunas temporárias de proteção durante o período de transição. Tais fatores representam riscos técnicos e econômicos relevantes, especialmente por se tratar de solução crítica para proteção dos ativos tecnológicos institucionais.
- 10.12. Além disso, a plataforma atualmente utilizada é baseada em arquitetura de nuvem, o que contribui para reduzir a necessidade de infraestrutura local dedicada para gerenciamento da solução, evitando custos adicionais com aquisição, manutenção e sustentação de servidores, bancos de dados, armazenamento, espaço físico, energia elétrica e demais componentes associados a soluções com gerenciamento local.
- 10.13. No que tange à adoção de tecnologia de proteção de endpoints, o MPPI manter a plataforma CrowdStrike Falcon atualmente implantada, de modo a assegurar a continuidade da proteção dos dispositivos institucionais, preservar as configurações e políticas já estabelecidas, manter a eficiência operacional da equipe técnica e garantir a continuidade dos controles de segurança aplicados ao ambiente.
- 10.14. Assim, considerando a posição da CrowdStrike entre os líderes de mercado no relatório Gartner de 2026, a maturidade da plataforma, sua aderência ao modelo de proteção de endpoints e sua implantação prévia no ambiente do MPPI, conclui-se que a manutenção da solução atualmente utilizada se mostra tecnicamente adequada e economicamente vantajosa para atendimento das necessidades do Ministério.
- 10.15. É importante destacar que, em todas as pesquisas de qualificação dos fabricantes mencionados acima, o MPPI está atualmente utilizando a melhor solução disponível no mercado de acordo com o Gartner (solução da CrowdStrike, de acordo com os critérios apontados).

10.16. Desta forma o que tange a adoção de uma tecnologia de Proteção de Endpoints, o MPPI, deseja manter sua atual solução e mantê-la baseada em software, de forma que continue se adaptando ao ambiente atual em produção, aproveitando todo o investimento já realizado em hardware, racks, espaço físico seguro, sistemas de virtualização, sistemas de banco de dados, políticas e softwares de backup e segurança, dentre outros, possibilitando sua expansão de capacidade por meio da infraestrutura já existe no MPPI, não sendo necessário qualquer custo adicional com gerenciamento e manutenção de hardware ou novo custo com consumo de energia elétrica ou espaço físico em seus sites.

10.17. No levantamento de mercado foram avaliadas tanto a manutenção/continuidade da solução atualmente utilizada quanto alternativas tecnológicas disponíveis no mercado. A análise técnica, operacional e econômica realizada demonstrou, contudo, que a substituição da plataforma atualmente implantada implicaria migração, reconfiguração de políticas, reinstalação de agentes, treinamento adicional da equipe, readequação de integrações e risco de descontinuidade temporária da proteção. Por essas razões, para a presente contratação, foi selecionada a alternativa de manutenção da solução CrowdStrike/Falcon, conforme fundamentação constante deste ETP.

Contratações similares em outros órgãos públicos

Nº	Órgão/Entidade	Ano	Referência da contratação	Solução/objeto similar identificado	Aderência ao objeto do MPPI
1	ANTAQ	2026	Pregão Eletrônico nº 90001/2026 – UASG 682010	Solução de proteção gerenciada de endpoints e workloads/servidores, contemplando componentes de Endpoint Security e detecção/correlação de ameaças.	Alta aderência ao núcleo funcional de proteção de endpoints, detecção e resposta a incidentes.
2	COFEN	2024	Pregão Eletrônico nº 90.028/2024 – Processo nº 00196.004611/2024-62 – UASG 389320	Solução integrada de segurança e conectividade, incluindo proteção de estações e servidores e serviços de detecção e resposta 24x7.	Compatível com o objeto quanto à proteção de endpoints, monitoramento, administração e resposta a incidentes.

Nº	Órgão/Entidade	Ano	Referência da contratação	Solução/objeto similar identificado	Aderência ao objeto do MPPI
3	FUNAI	2025	Pregão Eletrônico nº 90001/2025 – Contrato nº 116/2025 – UASG 194035	Solução de segurança cibernética do tipo XDR para endpoints e servidores, contemplando proteção avançada, investigação, análise forense, isolamento e gerenciamento centralizado.	Elevada aderência às funcionalidades de EDR, especialmente prevenção, detecção, investigação e resposta.
4	PRODEB/B A	2024	Pregão Eletrônico nº 23/2024 – Contrato nº 24/126-01	Renovação de solução Trend Micro Vision One – Endpoint Security para proteção de dispositivos, com garantia e atualização de versão.	Aderente à proteção corporativa de endpoints, com licenciamento de solução de segurança e atualização tecnológica.
5	Prefeitura Municipal da Serra/ES	2025	Pregão Eletrônico nº 165/2025	Renovação de Kaspersky Next EDR Optimum para dispositivos e serviços associados de resposta a incidentes.	Aderente ao objeto por contemplar proteção de endpoints com capacidades de EDR e resposta a incidentes.
6	Tribunal de Justiça de Pernambuco – TJPE	2023	Pregão Eletrônico nº 60/2023 – Processo nº 0084.2023.NLCD.PE.0060 .TJPE.FERM-PJ	Ferramentas de segurança cibernética destinadas à proteção de estações de trabalho e sistemas de TI, incluindo proteção de endpoints e workloads.	Possui aderência funcional quanto a antimalware, firewall, machine learning, proteção contra ransomware, detecção e resposta.
7	CREA-SC	2025	Pregão Eletrônico nº 90012/2025 – Contrato nº 025/2025 – UASG 389087	Renovação de soluções de segurança da informação, incluindo FortiEDR para proteção, detecção e resposta em endpoints.	Elevada aderência, por contemplar EDR, resposta a incidentes, gerenciamento e suporte relacionado à proteção dos endpoints.

Nº	Órgão/Entidade	Ano	Referência da contratação	Solução/objeto similar identificado	Aderência ao objeto do MPPI
8	Defensoria Pública do Estado de Mato Grosso do Sul – DPGE/MS	2026	Pregão Eletrônico nº 90001/2026 – Contrato nº 021/DPGE/2026 – UASG 926605	Plataforma de proteção de endpoints XDR integrada a serviços de segurança, com monitoramento, prevenção, detecção e resposta.	Elevada aderência ao objeto, especialmente quanto a proteção de endpoints, análise comportamental, investigação remota, isolamento e gerenciamento centralizado.
9	Tribunal de Contas do Estado do Pará – TCE-PA	2024	Pregão Eletrônico nº 07/2024 – Expediente nº 015278/2024 – Contrato nº 42/2024	Solução de segurança da informação com licenças de Segurança de Endpoints, EDR e XDR para desktops, notebooks, servidores e VDI.	Elevada aderência ao objeto, abrangendo prevenção, detecção, investigação, resposta, proteção contra ransomware e gerenciamento centralizado.
10	Supremo Tribunal Federal – STF	2024	Pregão Eletrônico nº 90005/2024 – Processo nº 002913/2023 – UASG 40001	Solução de detecção e resposta estendida a incidentes – XDR, incluindo proteção de endpoints, prevenção, detecção, investigação, threat hunting e resposta a ameaças.	Elevada aderência funcional, inclusive por contemplar solução CrowdStrike Falcon Enterprise Bundle e funcionalidades correlatas ao objeto do MPPI.
11	Conselho Nacional de Desenvolvimento Científico e Tecnológico – CNPq	2024	Pregão Eletrônico nº 90009/2024 – UASG 364102	Solução Trend Micro Vision One para proteção de endpoints e servidores, com recursos de Endpoint Security.	Aderente ao objeto por contemplar proteção de estações e servidores mediante solução corporativa de segurança de endpoints.
12	Tribunal de Contas do Estado de Alagoas – TCE-AL	2024	Pregão Eletrônico nº 90009/2024 – Contrato nº 5/2025 – UASG 925473	Solução Trend Vision One – Endpoint Security para estações de trabalho e servidores, com recursos de detecção e resposta.	Elevada aderência às funcionalidades exigidas, incluindo antimalware, firewall, Host IPS, controle de aplicações, EDR e gerenciamento centralizado.

As contratações acima foram consideradas como referências de mercado por apresentarem características técnicas compatíveis ou correlatas ao objeto pretendido pelo MPPI, especialmente quanto à proteção de endpoints, prevenção, detecção, investigação e resposta a incidentes de segurança. Os respectivos valores, critérios de normalização, análise estatística e memória de cálculo encontram-se consolidados nos documentos específicos da pesquisa de preços, submetidos ao tratamento de acesso definido para o orçamento estimado da contratação.

Alternativas

- 10.18. Foram avaliadas alternativas como manutenção/continuidade da solução atual ou contratação de solução equivalente de mercado, o que foi descartada para esta contratação. A substituição completa por tecnologia sem equivalência operacional pode exigir migração complexa, treinamento adicional, readequação de políticas, reinstalação massiva de agentes e risco de descontinuidade temporária da proteção.

Software público

- 10.19. Não se identificou solução de software público brasileiro capaz de atender integralmente aos requisitos de proteção EDR corporativa, telemetria contínua, inteligência global de ameaças, resposta remota e suporte especializado exigidos para o ambiente do MPPI.

Adequação de ambiente

- 10.20. A solução deverá ser compatível com o ambiente atual do MPPI e não exigir infraestrutura local adicional para console, banco de dados ou servidores de gerenciamento.

Modelos de prestação

- 10.21. O modelo de subscrição anual é o mais aderente ao mercado de soluções de segurança cibernética, pois inclui direito de uso, atualizações, inteligência de ameaças, evolução tecnológica e suporte durante a vigência.

Aquisição versus serviço

- 10.22. A aquisição perpétua não é recomendada para EDR, pois soluções dessa natureza dependem de atualização contínua, inteligência de ameaças, evolução de mecanismos de detecção e suporte ativo. A subscrição reduz desembolso inicial e evita custos complementares de manutenção e atualização.

Ampliação/substituição

- 10.23. A contratação visa à continuidade e à padronização do nível de proteção atualmente existente mediante manutenção da solução CrowdStrike/Falcon, sem ampliação para módulos autônomos de proteção de identidade, proteção de dados/DLP, indexação de sistemas operacionais ou inventário de rede.

Métricas

- 10.24. A eficácia da solução será acompanhada por indicadores como disponibilidade da console, taxa de atendimento dos chamados, cumprimento de prazos de suporte, quantitativo de dispositivos licenciados, eventos detectados, incidentes tratados e conformidade com requisitos técnicos.

Pesquisa de Mercado

10.25. A pesquisa de mercado deverá considerar contratações públicas similares, painéis oficiais, atas vigentes, banco de preços, propostas formais e referências de fabricantes ou revendedores autorizados, observando a IN SEGES/ME nº 65/2021 e a necessidade de cesta de preços aceitáveis.

11. Análise comparativa de soluções (IN 94/2022 art. 11 II; MOTec)

11.1. A análise técnica demonstra que a solução viável deve ser uma plataforma EDR corporativa, em subscrição anual, com console centralizada, agente/sensor, recursos de prevenção, detecção comportamental, investigação, resposta remota e suporte técnico.

Requisito comparativo	Solução EDR em subscrição	Antivírus tradicional	Licenciamento perpétuo
Detecção comportamental avançada	Sim	Parcial/limitado	Depende do produto
Resposta remota e isolamento de endpoint	Sim	Geralmente não	Depende do produto
Inteligência de ameaças atualizada continuamente	Sim	Parcial	Pode exigir contrato adicional
Operação em nuvem	Sim	Nem sempre	Nem sempre

Requisito comparativo	Solução EDR em subscrição	Antivírus tradicional	Licenciamento perpétuo
Menor desembolso inicial	Sim	Sim	Não
Adequação ao padrão atual do MPPI	Sim	Não	Parcial
Atendimento à necessidade institucional	Sim	Não	Parcial

- 11.2. Com base na análise do relatório Magic Quadrant for Endpoint Protection, publicado pelo Gartner em 2026, observa-se que o mercado de proteção de endpoints é composto por diversos fabricantes com diferentes níveis de capacidade de execução e completude de visão. Entre os fornecedores avaliados no relatório, destacam-se fabricantes como CrowdStrike, Microsoft, SentinelOne, Sophos, Palo Alto Networks, Trend Micro, Bitdefender, Check Point, ESET, Fortinet, Trellix e Broadcom, entre outros.
- 11.3. O relatório do Gartner posiciona a CrowdStrike no quadrante de líderes em Endpoint Protection, evidenciando sua relevância no mercado e sua capacidade de atender organizações que buscam soluções maduras de proteção de endpoints, com administração baseada em nuvem, recursos de prevenção, detecção e resposta, além de capacidades voltadas à investigação de ameaças em dispositivos corporativos.
- 11.4. A análise de mercado demonstra que existem alternativas tecnológicas relevantes no segmento de proteção de endpoints. Entretanto, no caso concreto do MPPI deve-se considerar que o Ministério já utiliza a plataforma CrowdStrike Falcon em seu ambiente tecnológico, com sensores implantados, políticas configuradas, equipe técnica capacitada e processos operacionais estabelecidos para administração, monitoramento, investigação e resposta a eventos de segurança.
- 11.5. Dessa forma, a análise comparativa não se limita à identificação de fabricantes reconhecidos no mercado, mas também considera a aderência da solução ao ambiente atualmente em produção, a preservação dos investimentos já realizados, a continuidade operacional, a redução de riscos de transição e a manutenção da padronização tecnológica da segurança de endpoints do Ministério.
- 11.6. A substituição da plataforma atualmente utilizada poderia gerar necessidade de nova implantação, reconfiguração de políticas, substituição de sensores, reconstrução de integrações, treinamento adicional da equipe, perda de histórico operacional e eventuais lacunas temporárias de proteção durante o período de transição. Tais fatores representam riscos técnicos e econômicos relevantes, especialmente por se tratar de

solução crítica para proteção dos ativos tecnológicos institucionais.

- 11.7. Além disso, a plataforma atualmente utilizada é baseada em arquitetura de nuvem, o que contribui para reduzir a necessidade de infraestrutura local dedicada para gerenciamento da solução, evitando custos adicionais com aquisição, manutenção e sustentação de servidores, bancos de dados, armazenamento, espaço físico, energia elétrica e demais componentes associados a soluções com gerenciamento local.
- 11.8. 13.8. No que tange à adoção de tecnologia de proteção de endpoints, o MPPI busca manter a plataforma CrowdStrike Falcon atualmente implantada, de modo a assegurar a continuidade da proteção dos dispositivos institucionais, preservar as configurações e políticas já estabelecidas, manter a eficiência operacional da equipe técnica e garantir a continuidade dos controles de segurança aplicados ao ambiente.
- 11.9. Assim, considerando a posição da CrowdStrike entre os líderes de mercado no relatório Gartner de 2026, a maturidade da plataforma, sua aderência ao modelo de proteção de endpoints e sua implantação prévia no ambiente do MPPI, conclui-se que a manutenção da solução atualmente utilizada se mostra tecnicamente adequada e economicamente vantajosa para atendimento das necessidades da Agência.
- 11.10. É importante destacar que, em todas as pesquisas de qualificação dos fabricantes mencionados acima, o MPPI está atualmente utilizando a melhor solução disponível no mercado (solução da CrowdStrike, de acordo com os critérios apontados).
- 11.11. Desta forma, o que tange a adoção de uma tecnologia de Proteção de Endpoints, o Ministério Público do Estado do Piauí deseja manter e expandir sua atual solução e mantê-la baseada em software, de forma que continue se adaptando ao ambiente atual em produção, aproveitando todo o investimento já realizado em hardware, racks, espaço físico seguro, sistemas de virtualização, sistemas de banco de dados, políticas e softwares de backup e segurança, dentre outros, possibilitando sua expansão de capacidade por meio da infraestrutura já existente no Ministério Público do Estado do Piauí, não sendo necessário qualquer custo adicional com gerenciamento e manutenção de hardware ou novo custo com consumo de energia elétrica ou espaço físico em seus sites.

Pesquisa inicial de preços (MOTec)

- 11.12. A pesquisa de preços deverá ser consolidada em mapa próprio.

Metodologia e Justificativa da Pesquisa de Preços

- 11.13. A pesquisa deverá priorizar fontes públicas, contratações similares, atas de registro de preços e bases oficiais. Na ausência de fontes suficientes, poderão ser utilizadas cotações com fornecedores, desde que acompanhadas de justificativa, análise crítica, identificação de

preços destoantes e comprovação de compatibilidade técnica.

Conclusão da Análise Comparativa das Soluções

- 11.14. A solução EDR em subscrição anual é a alternativa tecnicamente mais adequada, pois atende à necessidade de proteção avançada, reduz riscos de obsolescência, preserva a capacidade de resposta a incidentes e mantém aderência ao modelo operacional atualmente utilizado pelo MPPI.

12. Registro de soluções consideradas inviáveis (IN 94/2022 art. 11 §1º; MOTec)

- 12.1. Foram consideradas inviáveis:

Solução considerada	Justificativa de inviabilidade
Antivírus tradicional sem EDR	Não atende à necessidade de investigação, resposta remota, isolamento, telemetria avançada e caça de ameaças.
Licenciamento perpétuo	Incompatível com a dinâmica de atualização contínua, inteligência de ameaças e suporte exigidos por soluções EDR modernas.
Solução sem console em nuvem ou que exija infraestrutura local relevante	Aumenta custos, complexidade operacional, consumo de recursos e risco de indisponibilidade.
Contratação parcelada por componentes independentes	Gera risco de incompatibilidade, múltiplas consoles, falhas de correlação e dificuldade de responsabilização.
Soluções sem equivalência funcional ao padrão Falcon atualmente utilizado	Podem reduzir o nível de proteção e exigir readequação operacional significativa.

13. Análise comparativa de custos (TCO) (Lei 14.133/2021 §1º VI; IN 94/2022 art.11 III; MOTec) - ITEM OBRIGATÓRIO

- 13.1. A análise de TCO demonstra que a subscrição anual tende a ser mais adequada que o licenciamento perpétuo, pois reduz desembolso inicial, inclui atualizações, suporte, evolução da inteligência de ameaças e evita contratação adicional de manutenção.
- 13.2. O modelo de EDR em nuvem também reduz custos indiretos com servidores, bancos de dados, armazenamento local, energia, climatização, manutenção e administração de infraestrutura.
- 13.3. Além disso, o modelo de subscrição proporciona maior flexibilidade na substituição da solução, possibilitando a adoção de novas tecnologias sem comprometer investimentos já realizados. A redução do risco de descontinuidade também é um fator relevante, pois o fornecedor é responsável por manter o software sempre atualizado, corrigindo bugs e falhas de segurança e disponibilizando upgrades para novas versões, sem custos extras.

- 13.4. Considerando a convergência do mercado para o licenciamento por subscrição e a decisão da equipe de planejamento em contratar os serviços conforme a demanda, fica evidente que essa abordagem desonera o Ministério Público do Estado do Piauí da necessidade de aquisição de software com licenciamento perpétuo e de contratos adicionais de manutenção e suporte.
- 13.5. Dessa forma, a análise de TCO demonstra que a opção de subscrição anual é a alternativa mais eficiente e sustentável, alinhada às boas práticas de mercado e garantindo melhor custo-benefício ao longo do tempo.

MODELO	SOLUÇÃO
Subscrição	1. Pagamentos anuais, desembolso fracionado
	2. Possibilidade de substituição da ferramenta a qualquer momento
	3. Dispensa a necessidade de contratação de serviços complementares
	4. Redução de riscos de interrupção

Justificativa para dispensa do TCO

- 13.6. Considerando que as alternativas de antivírus tradicional, licenciamento perpétuo e soluções sem equivalência funcional foram consideradas inviáveis, fica dispensado o cálculo comparativo detalhado de TCO para tais alternativas. A análise econômica deverá concentrar-se na solução viável: subscrição anual de EDR por dispositivo.

Definição da Solução a ser adotada

- 13.7. A solução definida é a contratação, por Ata de Registro de Preços, de subscrição anual da solução corporativa CrowdStrike/Falcon, na modalidade EDR, para proteção dos dispositivos do MPPI, conforme requisitos técnicos estabelecidos neste ETP e no Termo de Referência.

14. Descrição da solução de TIC a ser contratada (Lei 14.133/2021 §1º VII; MOTec)

- 14.1. A solução a ser contratada consiste em subscrição anual de plataforma EDR para endpoints, incluindo:

Item	Descrição	Unidade
1	Subscrição anual para solução corporativa EDR de detecção e resposta a incidentes de segurança cibernética em endpoints, com prevenção, investigação, resposta remota, caça de ameaças, inteligência de ameaças, console centralizada em nuvem, agente/sensor e suporte técnico.	Dispositivo

- 14.2. A solução CrowdStrike/Falcon objeto da presente contratação

deverá preservar as capacidades atualmente utilizadas no ambiente do MPPI e contemplar, no mínimo, os seguintes requisitos técnicos:

- Plataforma baseada em nuvem para gerenciamento centralizado.
- Agente/sensor único ou conjunto de componentes integrados para proteção de endpoint.
- Detecção comportamental em tempo real.
- Prevenção contra malware, ransomware, exploits e técnicas fileless.
- Correlação de eventos por dispositivo, usuário, processo e artefato.
- Investigação com linha do tempo e árvore de processos.
- Resposta remota, incluindo isolamento de host.
- Inteligência global de ameaças e atualização contínua.
- Caça de ameaças e consultas sobre telemetria do endpoint, quando disponível no módulo EDR ofertado.
- Relatórios técnicos e executivos.
- Suporte técnico especializado.

Declaração de conformidade

- 14.3. A contratação configura uma solução única de TIC, composta por subscrição EDR e serviços acessórios indispensáveis à sua operação. O objeto é aderente à Lei nº 14.133/2021, à Resolução CNMP nº 283/2024, à IN SGD/ME nº 94/2022 e às demais normas aplicáveis às contratações de TIC.

15. Estimativa de custo total da contratação (Lei 14.133/2021 §1º VI; IN 94/2022 art. 11 IV; MOTec) - ITEM OBRIGATÓRIO

- 15.1. *[Conteúdo Sigiloso | Justificativa: O orçamento estimado da contratação não será divulgado antes do encerramento da fase de julgamento das propostas, conforme o disposto no art.24 da Lei nº 14.133/2021, combinado com o § 1º do art. 91 do Decreto Estadual nº 21.872/2023. A adoção do orçamento sigiloso tem como objetivo estimular a competitividade entre os licitantes e buscar a obtenção da proposta mais vantajosa para o MPPI. A divulgação prévia do valor estimado pode fazer com que as propostas apresentadas sejam estabelecidas próximas a esse valor, reduzindo a possibilidade de obtenção de preços mais competitivos. Com a não divulgação prévia do orçamento, os licitantes deverão formular suas propostas com base em seus próprios custos, condições de mercado e margem de lucro, evitando que o orçamento da Administração seja utilizado como referência para a formação dos preços. Dessa forma, busca-se favorecer uma disputa mais efetiva e a obtenção de preços mais vantajosos para a Administração, sem prejuízo da transparência do procedimento, uma vez que o orçamento será disponibilizado no momento legalmente adequado].*

16. Justificativa técnica da escolha da solução

- 16.1. A escolha da solução EDR justifica-se tecnicamente pelos seguintes fatores:
- Proporciona detecção e resposta em tempo real contra ameaças conhecidas e desconhecidas.

- Permite resposta remota, incluindo isolamento de endpoints comprometidos.
- Melhora a investigação de incidentes por meio de telemetria, linha do tempo e árvore de processos.
- Permite manter a proteção contínua de estações de trabalho, servidores e demais dispositivos compatíveis, com recursos de prevenção, detecção, quarentena, isolamento de rede, atualização de sensores e proteção contra manipulação indevida do agente.
- Possibilita a análise de arquivos em ambiente controlado, com observação de comportamento, atividades de rede, processos iniciados, alterações em arquivos e demais características relevantes para identificação de artefatos maliciosos
- Aumenta a proteção contra ransomware, malware e técnicas de evasão.
- Preserva o padrão técnico, as capacidades de proteção e o ambiente CrowdStrike/Falcon atualmente implantado no MPPI.
- As plataformas automatizam respostas a incidentes para conter e mitigar rapidamente as ameaças detectadas.
- Disponibiliza recursos para investigação e remediação remota, permitindo coleta de logs e artefatos, execução de scripts, encerramento de processos, análise de conexões de rede e outras ações necessárias ao tratamento de incidentes.
- Permite controlar o uso de dispositivos removíveis, com aplicação de políticas por classe de dispositivo e permissões granulares, reduzindo riscos de uso indevido de periféricos e exfiltração de informações
- Reduz a curva de aprendizado da equipe técnica ao preservar a plataforma, os processos operacionais, as políticas e os procedimentos já adotados no ambiente CrowdStrike/Falcon do MPPI.
- Possibilita administrar regras de firewall dos dispositivos protegidos a partir da console central, permitindo controlar comunicações de entrada e saída, portas, protocolos e condições baseadas na localização de rede.
- Fornece acompanhamento contínuo de eventos, alertas, comportamentos suspeitos e atividades relevantes nos dispositivos protegidos, permitindo atuação rápida da equipe técnica diante de possíveis incidentes.
- Adiciona camadas extras de segurança além da senha, tornando mais difícil o acesso de invasores ao ambiente computacional.
- Permite gestão centralizada em nuvem e operação sobre dispositivos internos e remotos.
- Evita adoção de solução inferior ao padrão atualmente existente.

17. Justificativa econômica da escolha da solução

- 17.1. A solução por subscrição anual permite previsibilidade orçamentária, atualização contínua, suporte incluso, menor desembolso inicial e redução de custos indiretos com infraestrutura local.
- 17.2. A adoção de registro de preços permite contratação conforme a necessidade real do MPPI, evitando aquisição imediata de todo o quantitativo quando não houver demanda ou disponibilidade orçamentária.

- 17.3. A manutenção da solução CrowdStrike/Falcon atualmente implantada reduz custos associados à transição tecnológica, treinamento, reconfiguração de políticas, reinstalação de agentes, reconstrução de integrações, retrabalho operacional e riscos decorrentes de eventual migração.

PLANEJAMENTO

18. Benefícios a serem alcançados com a contratação (Lei 14.133/2021 §1º IX)

18.1. Os benefícios esperados são:

- Continuidade da proteção de dispositivos do MPPI.
- Manter a solução de proteção de dispositivos já implantada, preservando a padronização tecnológica, as configurações existentes, os investimentos realizados e o conhecimento técnico adquirido pela equipe.
- Garantir maior capacidade de detecção, prevenção e resposta a ameaças cibernéticas em estações de trabalho, servidores e demais dispositivos compatíveis.
- Reduzir riscos associados a malware, ransomware, exploits, ataques sem arquivo, shell reverso, webshell, scripts maliciosos e comportamentos suspeitos nos dispositivos protegidos.

- Proporcionar visão detalhada das atividades nos dispositivos, permitindo investigações aprofundadas sobre incidentes de segurança, incluindo rastreamento de processos, arquivos, conexões de rede, eventos e alterações relevantes no sistema.
- Permitir ações de resposta remota a incidentes, como isolamento de dispositivos, coleta de logs e artefatos, execução de scripts, encerramento de processos e apoio à remediação de ameaças.
- Melhorar a eficiência operacional por meio de automações de segurança, agilizando o tratamento, a contenção e a resposta a incidentes.
- Manter recursos de análise de arquivos suspeitos em ambiente controlado, apoiando a identificação de comportamentos maliciosos, indicadores de comprometimento e evidências técnicas para investigação.
- Reduzir a superfície de ataque por meio de recursos de controle de dispositivos USB, gerenciamento de firewall local e aplicação centralizada de políticas de segurança.
- Preservar a gestão centralizada da segurança dos dispositivos por meio de console em nuvem, reduzindo a necessidade de infraestrutura local adicional e simplificando a administração da solução.
- Apoiar a conformidade com normas, políticas e diretrizes de segurança da informação e proteção de dados, por meio de registros, relatórios, trilhas de auditoria e evidências técnicas.
- Fortalecer a postura de segurança cibernética do MPPI, aumentando a confiabilidade, a resiliência e a continuidade operacional do ambiente computacional que sustenta as atividades institucionais.

19. Providências a serem adotadas pela administração (Lei 14.133/2021 §1º X; Res. CNMP283/2024)

19.1. O MPPI deverá adotar as seguintes providências:

- Designar Equipe de Gestão e Fiscalização do contrato.
- Validar o quantitativo de dispositivos a serem licenciados.
- Atualizar a pesquisa de preços e o mapa comparativo.
- Definir critérios de aceite técnico e recebimento provisório/definitivo.
- Disponibilizar equipe técnica para acompanhar a implantação.
- Validar políticas de segurança a serem aplicadas na solução.
- Definir canais oficiais de comunicação com a CONTRATADA.
- Assegurar cláusulas de confidencialidade, segurança e proteção de dados.

20. Papéis e responsabilidades

Papéis do contratante

- 20.1. A Equipe de Gestão e Fiscalização Contratual será responsável por acompanhar, fiscalizar, avaliar, receber e atestar a execução do objeto, nos termos da Resolução CNMP nº 283/2024 e normativos internos do MPPI.

Papéis da contratada

- 20.2. A CONTRATADA deverá indicar representante legal e preposto, quando necessário, responsáveis por representar a empresa perante o MPPI e coordenar a execução contratual.

Obrigações do Contratante

- 20.3. São obrigações do CONTRATANTE:

- Emitir Ordens de Serviço.
- Acompanhar a execução contratual.
- Validar entregas e relatórios.
- Efetuar pagamentos conforme condições contratuais.
- Comunicar falhas, incidentes e inconformidades.
- Garantir acesso autorizado às informações estritamente necessárias.

Obrigações da Contratada

- 20.4. São obrigações da CONTRATADA:

- Fornecer licenças válidas e funcionais.
- Prestar suporte técnico durante toda a vigência.
- Realizar implantação, configuração e orientação técnica quando demandada.
- Manter sigilo e cumprir normas de segurança e LGPD.
- Corrigir falhas e inconformidades nos prazos pactuados.
- Fornecer relatórios e documentos de comprovação.
- Manter condições de habilitação durante a vigência contratual.

Obrigações do Gestor da Ata de Registro de Preços (Quando aplicável)

- 20.5. O órgão gerenciador da ARP deverá controlar quantitativos, autorizar contratações, acompanhar saldos, gerir solicitações de adesão, conduzir renegociações quando cabíveis e aplicar as providências previstas na legislação e no edital.

21. Modelo de Execução do Contrato (MOTec; IN 94/2022 arts. 18-22)

Rotinas de execução

- 21.1. A execução será iniciada mediante Ordem de Serviço, contendo quantidade de licenças, localidade/unidade beneficiária, prazo, responsáveis e demais condições.
- 21.2. A CONTRATADA deverá disponibilizar as licenças, orientar a ativação e apoiar a validação operacional da solução.

Prazos, horários de fornecimento de bens ou prestação dos serviços e locais de entrega

- 21.3. As licenças e autorizações de acesso deverão ser disponibilizadas eletronicamente e encaminhadas ao e-mail institucional definido pelo MPPI no prazo de até 10 (dez) dias úteis após recebimento da Ordem de Serviço.

Local da entrega dos bens

- 21.4. Os serviços serão prestados preferencialmente de forma remota, tendo como referência administrativa:
 - Ministério Público do Estado do Piauí — Sede Centro
 - Rua Álvaro Mendes, 2294 — Centro — Teresina/PI — CEP 64000-060
 - E-mail de referência: cti@mppi.mp.br

Dos horários de execução contratual

- 21.5. As atividades ordinárias ocorrerão de segunda a sexta-feira, das 08h às 15h, exceto feriados, salvo suporte emergencial ou necessidade previamente acordada.

Documentação mínima exigida

- 21.6. A CONTRATADA deverá apresentar:
 - Comprovação de licenciamento e quantitativo disponibilizado.
 - Documentação técnica da solução.
 - Canais de suporte e procedimentos de abertura de chamados.
 - Relatório de implantação/configuração, quando aplicável.
 - Certificações, declarações ou documentos que comprovem atendimento aos requisitos técnicos.

Quantidade mínima de bens e serviços para comparação e controle

- 21.7. Para fins de comparação, controle e gestão do saldo da Ata de Registro de Preços, fica estabelecido o quantitativo máximo estimado de 1.600 (mil e seiscentas) subscrições anuais individuais, cada uma destinada à proteção de 1 (um) dispositivo, passíveis de contratação durante a vigência da Ata.
 - 21.7.1. As contratações serão realizadas conforme demanda formalizada pelo MPPI, disponibilidade orçamentária e saldo remanescente da ARP, não havendo obrigação de contratação da totalidade registrada.

21.7.2. O órgão gerenciador deverá atualizar o saldo da Ata a cada contratação, de modo a impedir que a soma das subscrições contratadas ultrapasse o quantitativo máximo registrado

Mecanismos formais de comunicação

21.8. Serão utilizados como mecanismos formais:

- Ordem de Serviço.
- Ata de reunião.
- Sistema de chamados.
- E-mail institucional.
- Ofício.
- Termos de Recebimento Provisório e Definitivo.
- Relatórios técnicos.

Forma e prazo de pagamento

21.9. O pagamento será realizado após disponibilização das licenças, validação técnica, emissão do Termo de Recebimento Definitivo e apresentação da Nota Fiscal/Fatura, conforme regras do contrato.

Vigência e alterações contratuais

Da vigência contratual

21.10. Os contratos decorrentes da Ata de Registro de Preços terão vigência inicial de 12 (doze) meses acrescida de 90 (noventa) dias corridos, contada da data de assinatura do instrumento contratual, sendo o termo final objetivamente determinável a partir desse marco. O período de cobertura de cada subscrição permanecerá limitado a 12 (doze) meses e deverá estar integralmente inserido na vigência contratual. Eventual prorrogação observará os arts. 106 e 107 da Lei nº 14.133/2021, a regulamentação institucional vigente e a demonstração formal da vantajosidade.

Da Vigência da ata de Registro de Preços

21.11. A Ata de Registro de Preços terá vigência de 12 (doze) meses, prorrogável por igual período, desde que comprovado o preço vantajoso.

Das prorrogações

21.12. As prorrogações observarão a legislação aplicável, a vantajosidade, a disponibilidade orçamentária e a avaliação da execução contratual.

Das alterações contratuais

21.13. Alterações contratuais observarão os limites e hipóteses da Lei nº 14.133/2021.

Termo de ciência de manutenção de sigilo (Art. 24, inciso VI, da Resolução CNMP nº 283/2024)

21.14. A CONTRATADA e seus profissionais deverão firmar termo de ciência e compromisso de sigilo, quando houver acesso a informações sensíveis do MPPI.

Direitos de propriedade intelectual e autorais (Quando necessário, principalmente em serviços que envolvam desenvolvimento de alguma solução)

- 21.15. A solução ofertada é software proprietário do fabricante/fornecedor. O MPPI terá direito de uso durante a vigência da subscrição. Documentos, relatórios e artefatos produzidos especificamente para o MPPI no âmbito da contratação não poderão ser comercializados ou divulgados pela CONTRATADA.

22. Modelo de Gestão do Contrato

Reunião inicial

- 22.1. Após a assinatura do contrato e designação da equipe de fiscalização, será realizada reunião inicial em até 5 (cinco) dias úteis, para alinhamento operacional, apresentação de preposto, canais de suporte, cronograma e procedimentos.

Principais marcos da gestão contratual (Opcional)

- 22.2. Marcos sugeridos:

- Assinatura do contrato.
- Reunião inicial.
- Emissão da Ordem de Serviço.
- Disponibilização das licenças.
- Validação técnica.
- Recebimento provisório.
- Recebimento definitivo.
- Acompanhamento mensal de suporte e indicadores.

Equipe de Fiscalização

Fiscal requisitante (Art. 36, Resolução CNMP 283/2024)

- 22.3. O fiscal requisitante acompanhará a aderência da solução às necessidades funcionais e institucionais.

Fiscal técnico

- 22.4. O fiscal técnico verificará conformidade técnica, licenças, funcionamento, suporte, atendimento dos requisitos e relatórios.

Fiscal administrativo

- 22.5. O fiscal administrativo acompanhará aspectos documentais, fiscais, trabalhistas, garantias, pagamentos e regularidade da CONTRATADA.

Gestor do contrato

- 22.6. O gestor coordenará a fiscalização, registrará ocorrências, tomará decisões administrativas, acompanhará riscos e proporá providências.

Critérios de aceitação (MOTec)

- 22.7. A solução será aceita quando:

- As licenças estiverem disponíveis e vigentes.
- O quantitativo contratado estiver comprovado.
- A console estiver acessível e funcional.
- A solução atender aos requisitos técnicos mínimos.
- Os canais de suporte estiverem ativos.
- A documentação mínima tiver sido entregue.

Da aplicação dos critérios de aceitação

- 22.8. O não atendimento aos critérios de aceitação implicará notificação da CONTRATADA para saneamento, sem ônus adicional ao MPPI.

Procedimento de teste e inspeção

- 22.9. Poderão ser realizados testes de acesso à console, validação de licença, instalação de agente/sensor em amostra, aplicação de política, geração de alerta simulado e execução de ação de resposta remota.

Níveis mínimos de serviço exigidos (Acordo de Nível de serviço exigidos (ANS))

- 22.10. Será utilizado o indicador IAP — Índice de Atendimento no Prazo, com meta mínima de 90%.

IAP apurado	Efeito
$\geq 90\%$	Sem desconto
$\geq 80\%$ e $< 90\%$	Desconto de 10% sobre parcela afetada
$\geq 70\%$ e $< 80\%$	Desconto de 20% sobre parcela afetada
$< 70\%$	Desconto de 30% sobre parcela afetada, sem prejuízo de sanções

23. Sanções administrativas e procedimentos para retenção ou glosa no pagamento

- 23.1. A CONTRATADA estará sujeita às sanções da Lei nº 14.133/2021 e do instrumento contratual em caso de inexecução parcial ou total, atraso injustificado, falha de suporte, descumprimento de sigilo, documentação falsa, fraude ou conduta inidônea.

- 23.2. Poderão ser aplicadas advertência, multa, impedimento de licitar e contratar, declaração de inidoneidade, retenção ou glosa proporcional ao descumprimento verificado, assegurados contraditório e ampla defesa.

24. Critérios de medição e pagamento

Lista de verificação e roteiro de testes aplicáveis (MOTec)

- 24.1. A lista de verificação deverá contemplar: licenciamento, console, agentes/sensores, políticas, alertas, resposta remota, suporte, relatórios e documentação.

Inspeções e diligências aplicáveis (MOTec)

- 24.2. O MPPI poderá realizar diligências para verificar autenticidade de documentos, comprovação de autorização comercial, aderência técnica e funcionamento da solução.

Procedimentos para recebimento provisório e definitivo

- 24.3. O recebimento provisório ocorrerá após disponibilização das licenças e acesso inicial à solução. O recebimento definitivo ocorrerá após verificação técnica do quantitativo, funcionalidades essenciais, suporte e documentação.

Procedimento para pagamento

Liquidação

- 24.4. A liquidação ocorrerá após validação da Nota Fiscal/Fatura, documentação fiscal, atesto do fiscal e comprovação do atendimento ao objeto.

Prazo de Pagamento

- 24.5. O prazo de pagamento seguirá o contrato e a legislação aplicável, contado da liquidação regular da despesa.

Forma de Pagamento

- 24.6. O pagamento será efetuado mediante ordem bancária, em conta indicada pela CONTRATADA, após cumprimento das condições contratuais.

25. Plano de sustentação e transição contratual

Recursos necessários à continuidade do negócio durante e após a execução do contrato

- 25.1. 25.1. A continuidade dependerá da manutenção das licenças ativas, do suporte técnico, da documentação de políticas, da transferência de conhecimento e do planejamento prévio de eventual transição para nova solução.

Recursos materiais e Humanos

Recurso	Quantidade	Responsável
Gestor do contrato	1	MPPI/CTI
Fiscal técnico	1	MPPI/CTI
Fiscal administrativo	1	MPPI
Equipe técnica de segurança/infraestrutura	Conforme designação	MPPI/CTI
Profissionais de suporte da CONTRATADA	Conforme necessidade	CONTRATADA

Estratégia e ações de transição contratual

- 25.2. Em caso de encerramento ou substituição da solução, a CONTRATADA deverá apoiar a exportação de relatórios, documentação de políticas, histórico de chamados e orientações necessárias para continuidade da proteção, observados os limites técnicos e contratuais.

26. 26. Extinção contratual

- 26.1. A extinção contratual observará as hipóteses da Lei nº 14.133/2021, o contrato e as regras da ARP. A CONTRATADA deverá cooperar para transição segura, evitando descontinuidade abrupta da proteção dos endpoints.

27. 27. Estratégia de independência (MOTec)

- 27.1. Para reduzir dependência tecnológica, o MPPI deverá manter documentação atualizada de políticas, grupos, procedimentos, relatórios, fluxos de atendimento, configurações relevantes e histórico de incidentes.

Formas de transferência de conhecimento

- 27.2. A transferência de conhecimento poderá ocorrer por workshops, reuniões técnicas, base de conhecimento, documentação, relatórios, registros de lições aprendidas e sessões remotas de operação assistida.

28. 28. Contratações correlatas/interdependentes (Lei 14.133/2021 §1º XI)

- 28.1. Não foram identificadas contratações correlatas ou interdependentes obrigatórias para viabilizar a solução EDR, considerando que a solução deverá ser ofertada de forma completa e funcional.

29. . Possíveis Impactos ambientais e medidas mitigadoras (Lei 14.133/2021 §1º XII)

Impactos ambientais

- 29.1. Os impactos ambientais são indiretos, relacionados ao consumo energético dos dispositivos protegidos, uso de infraestrutura em nuvem e eventual necessidade de equipamentos de apoio.

Medidas mitigadoras

- 29.2. Serão adotadas as seguintes medidas:

- Preferência por documentação digital.
- Solução em nuvem, evitando infraestrutura local adicional.
- Uso racional de recursos computacionais.
- Aproveitamento do parque tecnológico existente.
- Observância de práticas de TI Verde e sustentabilidade.

30. Adequação orçamentária e cronograma (IN 94/2022 art.21)

- 30.1. A contratação deverá observar disponibilidade orçamentária própria e dotação a ser indicada pela área competente.

Marco	Prazo estimado
Conclusão do ETP	Após validação da equipe de planejamento
Pesquisa de preços	Antes da elaboração final do TR
Publicação do edital	Após aprovação jurídica e administrativa
Assinatura da ARP	Após homologação
Contratação por OS/Contrato	Conforme demanda
Disponibilização das licenças	Até 10 dias úteis após OS

31. Forma e Critério de seleção do fornecedor (IN 94/2022 arts. 28-29)

Forma de seleção e Critério de julgamento da proposta

- 31.1. O fornecedor será selecionado por licitação, na modalidade Pregão, em forma eletrônica, com critério de julgamento pelo menor preço, observadas as especificações técnicas mínimas.

Justificativa da escolha da modalidade

- 31.2. O objeto possui padrões de desempenho e qualidade objetivamente definidos no ETP e no Termo de Referência, havendo oferta no mercado por diversos fornecedores, caracterizando serviço comum de TIC.

Regime de execução/fornecimento (IN 94/2022 art. 22; Lei 14.133/2021 art.92)

- 31.3. O regime de execução será por empreitada por preço unitário, com fornecimento conforme demanda formalizada por Ordem de Serviço.

Justificativa pela adoção do Sistema de Registro de Preços (Decreto Estadual nº 21.938/2023, Art. 4)

- 31.4. A adoção do Sistema de Registro de Preços — SRP é adequada à presente contratação, considerando o disposto no Decreto Estadual nº 21.938/2023, especialmente diante das seguintes características:
- 31.4.1. possibilidade de contratações permanentes ou frequentes, conforme evolução do parque computacional do MPPI;
- 31.4.2. conveniência de contratação conforme demanda, com fornecimento remunerado por unidade de medida, correspondente ao dispositivo licenciado;
- 31.4.3. impossibilidade de definir com absoluta precisão, no momento do planejamento, o quantitativo total a ser demandado durante toda a vigência da Ata.
- 31.5. O SRP permite maior flexibilidade administrativa, contratação conforme disponibilidade orçamentária e necessidade efetiva, além de evitar a realização de novos procedimentos licitatórios para objeto de mesma natureza, promovendo economicidade, celeridade e racionalização dos esforços administrativos.

Justificativa para Permissão ou não de Adesão de Órgãos Não Participantes à Ata de Registro de Preços

- 31.6. Não será admitida a adesão à Ata de Registro de Preços por órgãos ou entidades que não tenham participado do procedimento de Intenção de Registro de Preços e do planejamento da presente contratação.
- 31.7. A vedação decorre das características específicas do objeto, estruturado para assegurar a continuidade e a padronização da solução de proteção de endpoints já implantada no ambiente do MPPI, cujos requisitos técnicos, operacionais, de suporte, implantação e gestão foram definidos a partir das necessidades, políticas de segurança, infraestrutura e processos internos do órgão gerenciador.
- 31.7.1. A eventual adesão de órgãos externos exigiria análise individualizada de compatibilidade técnica, operacional e de segurança de ambientes distintos, podendo demandar requisitos, integrações, quantitativos, níveis de serviço e condições de execução não considerados no planejamento desta contratação.
- 31.7.2. A não previsão de adesão por órgãos não participantes também

visa preservar a capacidade administrativa do MPPI para gerir a Ata, controlar seus saldos, acompanhar as contratações decorrentes e priorizar o atendimento às necessidades institucionais que fundamentaram o procedimento.

- 31.7.3. Considerando a especificidade do objeto e a ausência de vantagem administrativa concreta e individualizada para o MPPI decorrente da gestão de solicitações de adesão de terceiros, não se mostra adequada a manutenção de cláusula genérica de “carona” baseada apenas em economia de escala, racionalização administrativa ou ampliação da utilidade da Ata.

Apresentação das propostas

- 31.8. As propostas deverão conter descrição técnica detalhada das subscrições CrowdStrike/Falcon ofertadas, comprovação do atendimento aos requisitos técnicos aplicáveis, documentos técnicos do fabricante, quantitativos, valores unitários e totais, prazo de validade da proposta e declaração de atendimento integral às especificações deste ETP e do Termo de Referência.

Exigências para a habilitação

Habilitação jurídica

- 31.9. Serão exigidos documentos de habilitação jurídica compatíveis com a natureza da licitante, conforme Lei nº 14.133/2021 e edital.

Habilitação fiscal, social e trabalhista

- 31.10. Serão exigidas comprovações de regularidade fiscal, social e trabalhista, incluindo CNPJ, Fazenda Nacional, FGTS, Justiça do Trabalho e demais certidões cabíveis.

Qualificação econômico-financeira

- 31.11. A qualificação econômico-financeira deverá comprovar capacidade compatível com a execução do objeto, podendo incluir balanço patrimonial, índices contábeis, certidão negativa de falência e capital mínimo, conforme edital.

Qualificação técnica

- 31.12. A licitante deverá comprovar aptidão para fornecimento de solução de proteção corporativa de endpoints/EDR de complexidade equivalente ou superior, por meio de atestados emitidos por pessoa jurídica de direito público ou privado, em nome da LICITANTE.
Enterprise Linux 6,7 e 8.

- 31.12.1. Documentos de apoio que podem ser apresentados junto com os atestados de capacidade técnica:
- 31.12.1.1. Declaração do fabricante do produto atestando ao proponente sua condição de representante, distribuidor ou de revendedor.
- 31.12.1.2. Declaração do fabricante, no caso de produtos de procedência estrangeira, acompanhada de tradução juramentada para o idioma nacional, atestando ao proponente sua condição de importador e, ainda, se for o caso, do importador para o proponente atestando sua qualidade de distribuidor, representante ou revendedor. e/ou
- 31.12.1.3. Impressão de página oficial do fabricante do produto na Internet, onde o proponente figure numa das hipóteses acima (distribuidor, representante ou revendedor), devendo ser informado o endereço da página para uma possível confirmação de conteúdo.
- 31.13. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.
- 31.14. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.
- 31.15. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da contratante e local em que foi executado o objeto contratado, dentre outros documentos.

32. Mapa de Gerenciamento de Riscos (Res. CNMP 283/2024 art. 45; IN 94/2022 art. 38; MOTec) - ITEM OBRIGATÓRIO

- 32.1. A matriz de riscos deverá ser juntada ao processo. Com base na matriz de gerenciamento de riscos de referência, destacam-se riscos relevantes para esta contratação:

Risco	Fase	Nível	Medidas preventivas/mitigadoras
Definição inadequada do objeto	Planejamento	Médio	Especificar requisitos técnicos objetivos e validar com a CTI.
Estimativa de custos incorreta	Planejamento	Alto	Realizar pesquisa de mercado ampla e análise crítica de preços.
Risco	Fase	Nível	Medidas preventivas/mitigadoras

Risco	Fase	Nível	Medidas preventivas/mitigadoras
Justificar tecnicamente a padronização da solução CrowdStrike/Falcon, realizar pesquisa de mercado abrangente e assegurar participação competitiva dos fornecedores, distribuidores e revendedores aptos a comercializar e prestar suporte à solução padronizada.	Seleção do fornecedor	Alto	Justificação da padronização e ampliação da competitividade entre revendedores/fornecedores autorizados da solução padronizada.
Impugnação ou recursos	Seleção do fornecedor	Alto	Revisar edital, justificar requisitos e responder questionamentos.
Não cumprimento dos prazos de entrega	Gestão contratual	Médio	Prever SLAs, penalidades e acompanhamento da execução.
Falta de suporte adequado	Gestão contratual	Médio	Exigir suporte durante toda a vigência, níveis mínimos e canais formais.
Problemas no gerenciamento de licenças	Gestão contratual	Baixo	Realizar inventário periódico e controlar quantitativos contratados.

VIABILIDADE

33. Declaração de Viabilidade (Lei 14.133/2021 §1º XIII; IN 94/2022 art.11 V; MOTec) - ITENS OBRIGATÓRIOS

- 33.1. A Equipe de Planejamento declara **viável** a contratação por registro de preços de subscrição anual de solução corporativa EDR para proteção de dispositivos do MPPI, observadas as especificações técnicas, a pesquisa de preços atualizada, a disponibilidade orçamentária e as condições previstas neste ETP.

Justificativa da Viabilidade/Inviabilidade

- 33.2. A viabilidade decorre da necessidade institucional de continuidade da proteção cibernética, da existência de soluções disponíveis no

mercado, da adequação do modelo de subscrição anual, da possibilidade de contratação por demanda via SRP e da compatibilidade da solução EDR com as necessidades do MPPI.

- 33.3. A solução proposta é tecnicamente adequada, economicamente justificável e alinhada às normas aplicáveis às contratações de TIC, estando a adoção da solução CrowdStrike/Falcon fundamentada na necessidade de manutenção da padronização tecnológica, continuidade operacional, compatibilidade com o ambiente existente, preservação dos investimentos realizados e mitigação dos riscos e custos associados à substituição da plataforma.

34. Responsáveis (IN 94/2022 art. 11 §2-3; MOTec)

- 34.1. O presente documento deverá ser assinado eletronicamente pelos integrantes da Equipe de Planejamento da Contratação designados por ato competente.

Papel	Responsável
Integrante Requisitante	Ítalo Garcia Araújo Nogueira
Integrante Administrativo	Breno Reis do Nascimento
Integrante Técnico	Marcos Maciel Martins Brito

ANEXO A — DESCRIÇÃO DOS REQUISITOS TÉCNICOS MÍNIMOS DA SOLUÇÃO EDR

- 1.1. 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.
- 1.2. A solução de gerenciamento em nuvem deve ser certificada nos programas FedRAMP (Federal Risk and Authorization Management Program) e ISO 27001.
- 1.3. A solução em nuvem deverá cumprir com as exigências da acreditação NSA-CIRA (certificando que foi avaliada e certificada em áreas de foco críticas derivadas das práticas recomendadas da indústria e do governo para investigação de segurança cibernética).
- 1.4. A plataforma em nuvem deverá cumprir com os requisitos exigidos no item 5 da certificação PCI-DSS V4 (Padrão de segurança de dados do setor de cartões de pagamento para organizações que lidam com cartões de crédito de marca das principais bandeiras de cartões).
- 1.5. Deverá possuir console única de administração, independentemente da versão ou arquitetura do Sistema Operacional suportado, obrigatoriamente baseada em nuvem (Cloud). Portanto, não deve possuir quaisquer dependências de componentes na rede local (on-premise) para gerenciamento da solução.
- 1.6. A solução deverá proteger os dispositivos de ameaças avançadas, persistentes e direcionadas que utilizam técnicas inovadoras de modificação de código

(polimorfismo, criptografia, codificação, entre outras) que não são detectadas por sistemas tradicionais de antivírus baseados em assinaturas, heurísticas e reputações globais.

- 1.7. Serão aceitas apenas soluções que possuam detecção de ameaças exclusivamente por meio de técnicas comportamentais, que se utilizam de motores baseados em aprendizado de máquina (Machine Learning) para averiguação de arquivos, não sendo aceitas soluções que utilizem modelos de assinaturas (vacinas) no agente ou sensor, independentemente se esses motores de assinaturas possam ser desligados e ou desativados.
- 1.8. A solução deve ser capaz de detectar e bloquear em tempo real ameaças conhecidas e desconhecidas (zero-day), ataques do tipo *fileless*, ameaças avançadas (APTs), Ransomware, exploits e outros comportamentos maliciosos, sem depender de bases de assinaturas.
- 1.9. A solução deve possuir prevenção de explorações baseada em kernel.
- 1.10. Identificação e prevenção de tentativas de escalonamento de privilégios ao nível de Kernel. Essa proteção deve poder ser usada em agentes instalados em endpoints com Sistemas Operacionais Windows, Mac e Linux;
- 1.11. Possuir capacidade de proteção contra shell reverso (reverse shell) e Webshell.
- 1.12. Deve manter suas funcionalidades de proteção do dispositivo, independente de conexão com a console de gerenciamento.
- 1.13. Deve possuir recursos para identificar ataques cibernéticos do tipo Live off the Land ou conhecidos como LOTL, técnicas que utilizam recursos, ferramentas ou utilitários legítimos, disponíveis no próprio sistema operacional.
- 1.14. A solução deve possuir acesso baseado em funções (RBAC) para permissões granulares.
- 1.15. A solução deve possibilitar o logon único (SSO) e deve possuir autenticação multifator (MFA) para gerenciamento da console
- 1.16. Possuir capacidade de executar detecção em tempo real (real-time) contra-ataques direcionados às vulnerabilidades de navegadores de internet (browsers).
- 1.17. A solução deverá possuir um único agente no dispositivo, evitando degradação de desempenho e ou componentes duplicados que dificultem a distribuição, manutenção e atualização dos equipamentos.
- 1.18. A proteção deve estar disponível para os sistemas operacionais Microsoft Windows e Linux, para as versões suportadas pelos seus respectivos fabricantes, incluindo versões posteriores ao lançamento

deste edital.

- 1.19. A solução não deverá exigir a reinicialização do Sistema Operacional. Todos os seus componentes de detecção e prevenção devem estar ativos e funcionais contra-ataques cibernéticos, tanto durante a instalação inicial quanto nas atualizações do agente ou sensor, visando vantajosidade para ambientes críticos e ininterruptos, livres de descontinuidade.
- 1.20. Deverá garantir que funções básicas como exclusões, ajustes finos de falsos-positivos e exceções também não deverão exigir a reinicialização do dispositivo para que sejam efetivadas ou entrem em vigor.
- 1.21. A plataforma deve possibilitar a proteção de desinstalação do agente por meio de uma senha ou de um token para cada dispositivo gerenciado
- 1.22. A solução deverá possuir métodos de proteção contra a remoção do agente ou sensor, através de aprovação na console de gerenciamento, por uma senha, chave ou equivalente.
- 1.23. A atualização dos sensores ou agentes deverá ser feita de forma automática seguindo uma política de atualização definida na console de gerenciamento considerando as seguintes opções no mínimo:
 - 1.23.1. Versão específica
 - 1.23.2. Versão de teste de recursos novos
 - 1.23.3. Versão mais recente
 - 1.23.4. Uma versão anterior a mais recente (N-1)
 - 1.23.5. Duas versões anteriores a mais recente (N-2)
 - 1.23.6. A atualização dos sensores ou agentes deverá permitir bloqueio de atualizações em horários e datas pré configurados.
- 1.24. A solução deve ter a capacidade de detectar tentativas de manipulação indevida dos componentes do agente (*Tamper Protection*).
- 1.25. A solução deve ser compatível com máquinas físicas ou virtuais, ainda com suporte a ambientes do tipo VDI (*Virtual Desktop Infrastructure*).
- 1.26. No gerenciador as detecções devem ser contextualizadas pela matriz do MITRE ATT&CK, mostrando as táticas, técnicas e procedimentos (TTPs – Tactics, Techniques, and Procedures) que foram observadas na cadeia de ataque (Kill chain).
- 1.27. A comunicação entre o agente a console deverá utilizar um túnel de segurança TLS criptografado utilizando certificate pinning
- 1.28. A capacidade de certificate pinning implementada no agente não deverá permitir a relação de confiança com o armazenamento de chaves local do sistema operacional, ou seja, mesmo se um certificado raiz for adicionado na keystore local o agente não deverá herdar essa relação de confiança.
- 1.29. A solução deverá prover a capacidade de emular a execução de

arquivos (Sandbox), integrada a um único agente.

- 1.30. A capacidade de emulação de arquivos (Sandbox) deve permitir controles da conectividade de rede, permitindo identificar comportamentos suspeitos em artefatos maliciosos inteligentes (artefatos que possuem capacidade de identificar quando estão sendo executados em ambientes controlados e apresentam comportamento diferente com e sem conectividade com a internet).
- 1.31. Deve permitir a interação diretamente com a amostra enviada para a análise podendo ser executada no mínimo 2 dos seguintes sistemas operacionais:
 - 1.31.1. Windows;
 - 1.31.2. Linux
 - 1.31.3. MacOS
- 1.32. A solução deve emular execução, no mínimo, nos seguintes sistemas operacionais:
 - 1.32.1. Windows 7 (32 e 64 bits);
 - 1.32.2. Windows 10;
 - 1.32.3. Windows 11
 - 1.32.4. Linux Ubuntu 16;
 - 1.32.5. macOS Catalina
- 1.33. A solução deverá possuir procedimento documentado e suportado para implantação em ambientes baseados em imagem mestre, clone, golden image ou VDI, prevenindo duplicidade de identificadores e garantindo inventário correto dos dispositivos provisionado
- 1.34. A solução deve incluir na análise de execução, no mínimo, as seguintes características:
 - 1.34.1. Táticas e técnicas de acordo com o framework do MITRE ATT&CK;
 - 1.34.2. Características comportamentais suspeitas;
 - 1.34.3. Imagens de execução, quando aplicável;
 - 1.34.4. Detalhes do arquivo como nome, hash, tamanho, tipo;
 - 1.34.5. Atividade de rede incluindo conexões, endereços IP de destino, domínios, portas;
 - 1.34.6. Atividades de arquivos;
 - 1.34.7. Detalhes de processos iniciados durante a execução.
- 1.35. Deve disponibilizar ferramenta de remediação remota para os administradores. Nesta ferramenta de remediação remota, a solução deve permitir a interação de, no mínimo, as seguintes ações:
 - 1.35.1. Listar processos em execução e permitir que sejam encerrados pelo administrador;
 - 1.35.2. Coletar logs de diagnóstico e artefatos maliciosos no sistema de arquivos do dispositivo remoto;

- 1.35.3. Reiniciar ou desligar o dispositivo;
- 1.35.4. Coletar despejos de memória (memory dumps);
- 1.35.5. Mostrar conexões de rede, configurações e testes de conectividade;
- 1.35.6. Executar scripts compatíveis com as linguagens PowerShell e Bash;
- 1.35.7. Listar componentes básicos do sistema operacional, devendo estes serem compatíveis para extrair dados do registro para Sistemas Operacionais Windows (Registry), tarefas agendadas, coletar ou disponibilizar arquivos no dispositivo;
- 1.36. Deve possibilitar que o administrador da solução faça o isolamento do tráfego de rede de dispositivos classificados como comprometidos, restringindo a comunicação somente com a console de gerenciamento e/ou com uma faixa de rede específica configurada em uma política.
- 1.37. A solução deve mostrar a visualização das cadeias de execução que levam a um alerta, incluindo a linha de tempo dos eventos.
- 1.38. A solução deverá apresentar na console de gerenciamento, informações referentes às ameaças identificadas, fornecendo informações referentes a primeira vez que uma ameaça foi vista no ambiente e quantos dispositivos tiveram essa mesma ameaça:
- 1.39. Deve permitir extrair Indicadores de Comprometimento (IOC), como por exemplo, hashes MD5, SHA1, SHA256, domínios, endereços IP, endereços de e-mail, nomes de arquivos associados às atividades maliciosas;
- 1.40. A solução deve oferecer suporte a administração via módulos utilizando o PowerShell ou equivalente, fornecida pelo próprio fabricante. Minimamente contendo as seguintes funcionalidades:
 - 1.41.1.1. Gerenciamento de políticas, incidentes, detecções;
 - 1.41.1.2. Gerenciamento de Regras e configurações da solução;
 - 1.41.1.3. Gestão de dispositivos via conexão remota, para resposta a incidentes, execução de scripts e coleta de artefatos e atividades forenses;
 - 1.41.1.4. Permitir a instalação de aplicativos nos dispositivos;
 - 1.41.1.5. Permitir a gestão de usuários e funções administrativas do gerenciador da solução.
- 1.41. A solução deve possuir capacidade integrada para utilização de fluxos automatizados para automação de tarefas, permitindo criação de notificação, critérios e ou gatilhos para que os fluxos sejam executados, possibilidade de personalização das condições de execução dos fluxos e associação de rotinas e ações a serem disparadas pelos (scripts, comandos, notificações).
 - 1.42.1.1. A solução deve possibilitar de workflows de automação a partir de playbooks pré-configurados para cenários específicos.
 - 1.42.1.2. A solução deve possuir no mínimo os seguintes gatilhos:

- 1.42.1.2.1. Nova
detecção
- 1.42.1.2.2. Eventos de política
- 1.42.1.2.3. Alteração em um dispositivo
- 1.42.1.2.4. Gatilho temporal (horas, dia, semana e mês)
- 1.42.1.3. A solução deve possuir no mínimo as seguintes ações:
 - 1.42.1.3.1. Conter a rede do dispositivo, fazendo que ele só se comunique com a console da solução
 - 1.42.1.3.2. Pegar o arquivo associado a uma detecção da endpoint e faça o upload para a console
 - 1.42.1.3.3. Remover o arquivo associado a uma detecção do endpoint
 - 1.42.1.3.4. Notificar um usuário, no mínimo e-mail, Teams e Webhook
 - 1.42.1.3.5. Recuperar conexões de rede ativas durante uma detecção
 - 1.42.1.3.6. Recuperar os processos em andamento durante a detecção
- 1.42.2. A solução deverá disponibilizar biblioteca de playbooks ou modelos de automação pré-configurados para cenários comuns de segurança, tais como nova detecção crítica, contenção de dispositivo, coleta de artefatos, coleta de diagnóstico, notificação de incidente, análise de malware, resposta a phishing, vulnerabilidade crítica e criação de ticket.
- 1.42.3. A solução deverá permitir integração nativa ou por conectores/API com ferramentas de colaboração e gestão de chamados, permitindo criação, atualização ou encerramento de tickets, envio de notificações, atribuição de responsáveis e registro de evidências relacionadas ao incidente.
- 1.42.4. A solução deve permitir controle de dispositivos USB, minimamente para os sistemas Windows
- 1.42.5. A solução deve permitir bloqueio de dispositivos USB baseado em, no mínimo, as seguintes classes de dispositivos:
 - 1.42.5.1. Dispositivos de imagem;
 - 1.42.5.2. Dispositivos de áudio e vídeo;
 - 1.42.5.3. Dispositivos de armazenamento em massa;
 - 1.42.5.4. Dispositivos móveis (MTP/PTP)
 - 1.42.5.5. Impressoras;
 - 1.42.5.6. Adaptadores de rede wireless;
 - 1.42.5.7. Para os dispositivos de armazenamento em massa, deve atribuir, no mínimo, as seguintes permissões granulares:
 - 1.42.5.7.1. Leitura somente;
 - 1.42.5.7.2. Escrita e leitura;

1.42.5.7.3. Escrita leitura e
execução; 1.42.5.7.4. Bloqueio
total;

- 1.42.5.8. O controle de dispositivos USB deve fornecer informações detalhadas sobre as atividades dos arquivos no contexto de metadados habilitando investigação de potenciais eventos de exfiltração de dados.
- 1.42.5.9. A solução deve apresentar dashboard dedicada a prover visibilidade dos arquivos específicos escritos pelo host em um dispositivo USB removível.
- 1.42.5.10. O controle de dispositivos oferecer visibilidade das extensões de arquivos. Documentos, design, multimídia, código fonte, executável, máquinas virtuais, e-mail e logs.

1.42. Características específicas para sistemas operacionais Windows

- 1.42.1. A solução deve ser participante do Microsoft Active Protections Program (MAPP) para provedores de software de segurança.
- 1.42.2. Deverá ser capaz de impedir ataques que sobrescrevem a SEH (Structured Exception Handling).
- 1.42.3. Deverá impedir ataques que utilizem a técnica Heap Spray Preallocation.
- 1.42.4. Deverá proteger contra vulnerabilidades associadas ao ASLR (Address Space Layout Randomization).
- 1.42.5. Deverá forçar Data Execution Prevention (DEP) para impedir ameaças que utilizem memória para execução de códigos em região de memória não executável
- 1.42.6. Deve possuir a capacidade de detectar e prevenir processos que tentem realizar extração de credenciais (Credential Dumping).
- 1.42.7. A solução deve ser capaz de oferecer visibilidade de potenciais ataques não provenientes de arquivos e executáveis, mas sim por meio de varreduras na memória e CPU, evitando ataques sem arquivos (Fileless).
- 1.42.8. O ML (Machine Learning) deve ser capaz de 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.
 - 1.42.8.1. Caso seja configurado para bloqueio o arquivo deverá ser quarentenado.
- 1.42.9. A solução deverá ter a capacidade de detecção e prevenção das seguintes ameaças cibernéticas:
 - 1.42.9.1. Adwares, Spywares, Graywares e PUP (Potentially Unwanted Programs);

- 1.42.9.2. Operações no Registro (Registry) consideradas suspeitas ou técnicas de persistência;
- 1.42.9.3. Scripts e linhas de comando consideradas suspeitas;
- 1.42.9.4. Macros suspeitas e ou maliciosas em documentos do Microsoft Office;
- 1.42.9.5. Bloquear o carregamento de drivers suspeitos;
- 1.42.9.6. Encerrar processos que utilizam técnicas de injetar códigos em processos (Code Injection).
- 1.42.10. A solução deverá oferecer suporte a detectar e bloquear ameaças do tipo Ransomware, com base nas seguintes capacidades:
 - 1.42.10.1. Detectar e prevenir deleção de snapshots baseados em cópias de sombra (VSS – Volume Shadow Copies);
 - 1.42.10.2. Bloquear processos que criem arquivos com extensões conhecidas por ataques de Ransomware ou comportamentos relacionados.
- 1.42.11. A solução deve possuir módulo ou a capacidade de gerenciamento de Firewall para os dispositivos a partir da console de administração, permitindo a filtragem do tráfego de entrada e saída, capacidade de especificar portas de comunicação, protocolos e capacidade de bloquear ou permitir a comunicação.
 - 1.42.11.1. 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
 - 1.42.11.2. A Solução deve possibilitar a aplicação de regras de firewall personalizadas dependendo da localização de rede do dispositivo, utilizando como critério: tipo de conexão, IP do gateway, DHCP, DNS e IP do dispositivo.

1.43. Características específicas para sistemas operacionais Linux

- 1.43.1. Deverá possuir proteção Anti-malware.
- 1.43.2. A solução deverá permitir detecção e prevenção de atividades maliciosas sobre o sistema de arquivos (filesystem).
- 1.43.3. Deve monitorar o tráfego de rede do dispositivo buscando atividades ou padrões de comportamento maliciosos ou proteção equivalente.
- 1.43.4. A solução deve incorporar técnicas de aprendizado de máquina (Machine Learning) para detecção e prevenção de ataques.
- 1.43.5. Deve possuir recursos para que a solução opere em modo de detecção ou em conjunto com o modo de prevenção de ameaças, oferecendo diferentes níveis de sensibilidade nos ajustes de configurações.

- 1.43.6. Deve oferecer suporte a quarentena de arquivos classificados como maliciosos (isolamento do arquivo).
- 1.43.7. A solução deve oferecer suporte a bloquear e permitir indicadores de comprometimento (IOCs).
- 1.43.8. Deve ser capaz de detectar e bloquear execução de scripts suspeitos.
- 1.43.9. Deve permitir monitorar as atividades e eventos relacionadas a tráfego não encriptado FTP.
- 1.43.10. Deve permitir monitorar as atividades e eventos relacionadas a tráfego não encriptado TLS.
- 1.43.11. Deve permitir bloqueio personalizado através da inclusão de assinaturas digitais (hashes) de arquivos;
- 1.43.12. Deve permitir bloqueio de processos com comportamento malicioso de acordo com a inteligência da fabricante.

1.44. Capacidades de inteligência de ameaças

- 1.44.1. A inteligência de ameaças deve mapear campanhas de ataque e dar visibilidade de países e indústrias alvo, país de origem da campanha e última atividade;
- 1.44.2. Para campanhas de ameaça, a inteligência de ameaças deve fornecer, quando aplicável, informações tais como vulnerabilidades utilizadas, métodos de entrega, breve descrição da campanha, forma de monetização, métodos de ataque e motivação da campanha.
- 1.44.3. Deve associar, quando pertinente, detecções presentes no ambiente à campanha de ataque;
- 1.44.4. 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;

1.45. Relatórios e dashboard

- 1.45.1. A solução deverá prover Dashboard trazendo as detecções mais recentes, número de novas detecções e detecções por táticas nos últimos 30 dias.
- 1.45.2. Deve gerar relatórios em PDF e CSV.
- 1.45.3. A solução deve permitir a configuração de uma frequência dos relatórios gerados para serem enviados por e-mail
- 1.45.4. A plataforma deverá ter a capacidade de reportar as detecções de forma agrupada das seguintes formas:
 - 1.45.4.1. Por dispositivo afetado;

- 1.45.4.2. Por técnica;
- 1.45.4.3. Por tática;
- 1.45.4.4. Por arquivo detectado;
- 1.45.4.5. Por linha de comando;
- 1.45.4.6. Por severidade.
- 1.45.4.7. A plataforma deverá ter a capacidade de reportar as detecções, permitindo organizar com a mais recente no topo, ou a mais antiga no topo.
- 1.45.5. A plataforma deverá ter a capacidade de reportar as detecções, permitindo filtrar minimamente com base aos seguintes filtros:
 - 1.45.5.1. Detectadas na última hora;
 - 1.45.5.2. Detectadas na última semana;
 - 1.45.5.3. Detectadas no último dia;
 - 1.45.5.4. Detectadas nos últimos 30 dias;
 - 1.45.5.5. Hash;
 - 1.45.5.6. Host;
 - 1.45.5.7. Nome de arquivo;
 - 1.45.5.8. Severidade;
 - 1.45.5.9. Linha de comando;
 - 1.45.5.10. Tática;
 - 1.45.5.11. Técnica;
 - 1.45.5.12. Tipo de sistema operacional;
 - 1.45.5.13. Usuário;
 - 1.45.5.14. Versão do sistema operacional.

