



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

TERMO DE REFERÊNCIA COMPRAS DE TIC – LEI 14.133/2021

Referência: RESOLUÇÃO Nº 283, DE 5 DE FEVEREIRO DE 2024

1. OBJETO

1.1. Formação de Registro de Preços para aquisição de software antivírus KASPERSKY NEXT EDR OPTIMUM, para fins de proteção da rede lógica, equipamentos de TI e informações, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses.

1.2. A solução é composta pelos itens constantes na tabela abaixo:

Item	Especificação	CATMAT / CATSER	Quantidade
1	Licença de software antivírus KASPERSKY NEXT EDR OPTIMUM , por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses, e demais detalhamentos descritos no termo de referência.	27456 CATSER	5000

2. JUSTIFICATIVA DA AQUISIÇÃO

2.1. Considerando a necessidade de garantir o controle e prevenção de ataques informatizados, oriundos de vírus e software maliciosos, ou demais mecanismos informatizados que violem a segurança das informações eletrônicas;

2.2. Considerando a necessidade de dotar a Instituição de software licenciado e original que contemple uma base de dados constantemente atualizada, além do mapeamento de novos vírus que surgem diariamente e suas respectivas proteções (vacinas), a fim de evitar prejuízos aos equipamentos de tecnologia da informação (TI) e informações eletrônicas da Instituição;

2.3. A solução de segurança e proteção antivírus atua na defesa contra vírus, *ransomwares* e outras ameaças que surgem a cada segundo na rede mundial de computadores (Internet), além de nos permitir a utilização de software para controle de acesso, identificação, contingência e eliminação de códigos e limpeza



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

de mensagens maliciosas via servidores de e-mail, controle de detecção de intrusão, geração e emissão de relatórios e gerenciamento centralizado, além de nos proporcionar o bom funcionamento e proteção dos dados e informações sigilosas;

2.4. Atualmente, a Instituição possui ferramentas de defesa (antivírus), tendo reduzido a praticamente zero o número de incidentes devido a vírus e outras ameaças virtuais nas estações de trabalho e equipamentos servidores. Com isso, faz-se necessário dar continuidade ao uso destas licenças de forma a padronizar as configurações e uniformizar o gerenciamento da solução, haja vista que o licenciamento finda em fevereiro ;

2.5. Considerando que a ferramenta de gerenciamento e a base de dados de antivírus, já utilizada para realizar essa proteção na Instituição, está com seu licenciamento em vias de expirar e desatualizar-se;

2.6. Considerando que a solução atual de antivírus encontra-se implantada em todos os computadores distribuídos nas unidades da Capital e Interior do Estado;

2.7. Considerando que, com a implantação do sistema de antivírus na rede da Instituição, com gerenciamento centralizado, reduziu-se os casos de infecção por vírus no ambiente computacional e eliminou-se a perda de produtividade causada pelas interrupções nos trabalhos administrativos e finalísticos, bem como otimizou a utilização dos recursos humanos ligados à manutenção da infraestrutura de tecnologia da informação;

2.8. Tendo em vista a impossibilidade de se definir, de forma prévia e precisa, o quantitativo de materiais e serviços a serem demandados, sugere-se a realização de licitação na modalidade de pregão, ata de registro de preços do tipo menor preço ou maior desconto, nos termos do inciso XLI, artigo 6º, da lei 14.133/2021;

2.9. *Com relação ao Art. 15, inc. I, do Decreto 11.462/2023, por se tratar de um registro de preços, o quantitativo definido não significa necessariamente, que serão adquiridos na sua totalidade, porém é importante que se tenha esse quantitativo para atendimento da demanda atual e reserva técnica, caso necessário;*

2.10. A contratação desta solução de TI está alinhada ao Planejamento Estratégico Institucional (PEI) do Ministério Público do Estado do Maranhão (MPMA), bem como prevista no Plano de Contratações Anual (PCA) 2027, contribuindo para a prestação de serviços, a otimização dos recursos de Tecnologia da Informação e a garantia da continuidade das atividades finalísticas da instituição.

3. JUSTIFICATIVAS PARA MANUTENÇÃO DA MARCA

3.1. Em 2024 o MPMA prosseguiu com o processo de atualização da proteção de rede que compõe sua infraestrutura (Antivírus), juntamente com um software para gerenciamento centralizado dos mesmos.

3.2. Com intuito de garantir o melhor desempenho, disponibilidade e estabilidade da Rede Corporativa que cada vez mais está sendo utilizada para tráfego sigiloso e sensível do GESP, SEI, ATHENAS e SIMP.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

Assim faz-se necessário o uso de políticas, protocolos e tecnologias que visam principalmente garantir a segurança das informações e o melhor desempenho dos serviços e aplicações.

3.3. A criação de políticas de segurança, perfis de acesso do tráfego, está estreitamente ligado às características próprias de cada componente e ao conjunto da solução adotada..

3.4. Consequentemente à aquisição de soluções de Antivírus, de fabricantes diferentes (heterogeneidade), obriga uma reconfiguração dos equipamentos, reconstrução das políticas, reinstalação de todos os clientes, além da curva de aprendizado da própria equipe de Administração de rede.

3.5. Disto, justifica-se a manutenção da marca, devido à:

3.5.1. Manutenção de experiência e know-how tecnológico : O MPMA utiliza, há cerca de seis anos, soluções de antivírus Kaspersky. Nesse período, a instituição consolidou, de forma satisfatória, elevado grau de maturidade na administração de políticas de segurança, perfis, objetos, inspeção de rede, mecanismos avançados de proteção, automação e integração com os serviços corporativos internos de monitoramento.

3.5.2. Risco na alteração da solução: A eventual substituição por uma solução de outro fabricante resultaria no desperdício imediato de todo conhecimento acumulado na plataforma atual, impondo uma nova curva de aprendizado à uma equipe reduzida, além de elevar o risco de erro humano, reduzir a eficiência operacional durante toda a fase inicial de transição e enquanto a maturidade da nova solução for inferior à já alcançada na solução atual; Considerando tratar-se de uma solução de Segurança da informação e com o crescimento cada vez maior do número e da complexidade de ataques, a redução da maturidade, mesmo que temporária, implicaria em um aumento proporcional na vulnerabilidade do ambiente do MPMA.

3.5.3. Migração de Regras e funções de segurança para outra plataforma : A transição para uma plataforma de outro fabricante exigiria a revisão minuciosa das políticas vigentes, a conversão extensiva de objetos, a validação da equivalência funcional de recursos nativos, o reajuste de integrações críticas e a realização de testes abrangentes. Esse processo aumentaria significativamente o risco de instabilidades, incompatibilidades temporárias, degradação do desempenho dos serviços, inconsistências na aplicação de regras, vulnerabilidades transitórias de segurança durante a implantação;

3.5.4. Gerenciamento: todas as configurações do software de gerenciamento centralizado da solução atual poderão ser aproveitadas com menor janela de migração possível, bem como todos os equipamentos que atualmente são gerenciados irão manter as informações de conexão, gerenciamento e sincronização podem ser configurados e administrados por uma única console, proporcionando gerenciamento sem interrupções;

3.5.5. Competitividade:

3.5.6. Conforme Acordo Corporativo N°24/2026 do Ministério da Gestão e da Inovação em Serviços Públicos, a Kaspersky declara que não se utiliza do “registro de oportunidade” no seu item



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

2.8:

“ 2.8. Por este instrumento, a KASPERSKY declara que não se utiliza do “registro de oportunidade” (conforme definido pelo Tribunal de Contas da União no Acórdão TC 030.236/2016-9, é o oferecimento de registro a um revendedor para que este obtenha privilégios para manter o relacionamento, fazendo com que outras vendas ligadas ao mesmo fabricante não se envolvam em negociações com a mesma organização, para praticar descontos ou preços diferenciados) e outras práticas junto a seus revendedores que possam frustrar o caráter competitivo das licitações, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública.”

3.5.7. A fabricante Kaspersky possui uma ampla rede de fornecedores habilitados à participar de processos de contratação, conforme pode ser observado em licitações com objetos semelhantes(Kaspersky Next Edr Optimum). As informações podem ser confirmadas no Portal Nacional de Contratações Públicas - PNCP :

3.5.7.1. Edital nº 90052/2025 -

Órgão/Entidade: ESTADO DO MARANHÃO - TRIBUNAL DE JUSTIÇA DO MARANHÃO.

Objeto: Registro de preços para Contratação de empresa especializada para o fornecimento de licenças de software antivírus com suporte técnico para 36 meses, observadas as condições estabelecidas nos Termo de Referência e ETP.

Propostas e Fornecedores:

<https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra/item/1?compra=92512505900522025>

3.5.7.2. Edital nº 90028/2025:

Órgão/Entidade: 08.539.710/0001-04 - MINISTÉRIO PÚBLICO DO ESTADO DO RIO GRANDE DO NORTE.

Objeto: Registro de preços para eventual prestação de serviço de licenciamento do antivírus Kaspersky Next Edr Optimum, por um período de 24 (vinte e quatro) meses para os dispositivos do parque tecnológico do MPRN.

Propostas e Fornecedores:



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

<https://cnetmobile.estaleiro.serpro.gov.br/comprasnet-web/public/compras/acompanhamento-compra/item/1?compra=9256030590028202>

5

4. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

4.1. RESULTADOS ESPERADOS

4.1.1. Proteger os dispositivos e dados da instituição, contra ameaças conhecidas e avançadas, como ransomware, malware e ataques de dia zero;

4.1.2. Detectar, entender e responder a ataques sofisticados, realizando análise de causa raiz e remediação;

4.1.3. Economizar recursos e simplificar o gerenciamento de soluções de Segurança da Informação;

4.1.4. Garantir a conformidade com as normas e regulamentos de segurança cibernética do setor público.

4.2. Parcelamento da solução de TI:

4.2.1. Pela natureza da contratação, que envolve o licenciamento de uso de software como um pacote integrado de funcionalidades e agentes, não há enquadramento nos critérios de parcelamento do objeto. O parcelamento seria técnica e economicamente inviável, pois descaracterizaria a solução, comprometeria a interoperabilidade e a segurança, além de gerar custos adicionais de gerenciamento e licenciamento fragmentado, em desacordo com o art. 40, inciso V, alínea 'b', da Lei nº 14.133/2021.

4.2.2. A centralização da responsabilização em uma única empresa CONTRATADA, por tratar-se de uma solução de alta disponibilidade e desempenho, além da abrangência de distribuição dos equipamentos, se mostra mais adequada, não apenas sob o prisma dos requisitos de interoperabilidade e do acompanhamento de problemas e soluções, mas sobremaneira para facilitar a verificação das causas e atribuição de responsabilidade, de modo a aumentar o controle sobre a execução do objeto licitado e para minimizar reposições em caso de defeitos durante a garantia técnica, por exemplo.

4.2.3.

5. REQUISITOS DA CONTRATAÇÃO

5.1. Requisitos de Negócio



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 5.1.1. Proteger os dispositivos e dados da instituição, contra ameaças conhecidas e avançadas, como ransomware, malware e ataques de dia zero;
- 5.1.2. Detectar, entender e responder a ataques sofisticados, realizando análise de causa raiz e remediação;
- 5.1.3. Economizar recursos e simplificar o gerenciamento de soluções de Segurança da Informação;
- 5.1.4. Garantir a conformidade com as normas e regulamentos de segurança cibernética do setor público.
- 5.1.5.

5.2. Requisitos de Capacitação

- 5.2.1. Não faz parte do escopo da contratação a realização de capacitação técnica.

5.3. Requisitos Legais

- 5.3.1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Resolução nº 238, de 5 de fevereiro de 2024, do Conselho Nacional do Ministério Público (CNMP), à Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, à Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) e a outras legislações aplicáveis.

5.4. Requisitos de Manutenção

- 5.4.1. A CONTRATADA deverá possuir Central de Atendimento (contato telefônico, sítio na Internet e e-mail) para consultas, aberturas de chamados técnicos e envio de arquivos para análise, durante 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana;
- 5.4.2. Atualizações durante o período de assinatura do software, de 36 (trinta e seis) meses, para a versão fornecida e para eventuais *releases* da versão adquirida;
- 5.4.3. Serviço de suporte técnico pelo período mínimo de 36 (trinta e seis) meses, através de consultas por e-mail e telefone ilimitado durante a vigência da licença.
- 5.4.4.** Os incidentes, situações inesperadas e não programadas, deverão ser atendidas pelos serviços de suporte da CONTRATADA. Os incidentes têm a seguinte classificação:
 - 5.4.4.1. Severidade 1 ou Crítica: Ambiente/Sistema está indisponível ou usuário sem acesso;
 - 5.4.4.2. Severidade 2 ou Alta: Uma função do Ambiente/Sistema está indisponível;
 - 5.4.4.3. Severidade 3 ou Média: O Ambiente/Sistema está disponível, porém apresentando lentidão, erros que forçam o reinício de operações no mesmo, e/ou alguma intermitência em seu funcionamento.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

5.4.5. A CONTRATADA deverá prestar, durante a vigência deste contrato, serviços de suporte a produção e manutenção corretiva abrangendo no mínimo:

5.4.6. Investigação e resolução de problemas no ambiente, mesmo que para isso seja necessário acionar o suporte do fabricante;

5.4.7. Nível de serviço (SLA), para chamados abertos entre o horário compreendido entre as 08 horas e 18 horas em dias úteis, conforme tabela a seguir:

Severidade	Descrição	Prazo máximo para início do atendimento remoto	Prazo máximo para a solução remota	Prazo máximo de Solução
1 - Crítica	Situação emergencial ou problema crítico que cause a indisponibilidade de sistema.	Até 2 horas	Até 10 horas	Até 30 horas após abertura do chamado remoto
2 - Alta	Impacto de alta significância relacionado à utilização da solução: ocorrência de indisponibilidade de funcionalidade.	Até 4 horas	Até 20 horas	Até 80 horas após abertura do chamado remoto
3 - Média	Impacto de baixa significância relacionado à utilização da solução. Não há ocorrência de indisponibilidade de funcionalidade, sendo contornável por solução paliativa sem grandes esforços ou retrabalho.	Até 8 horas	Até 40 horas	Até 120 horas após abertura do chamado remoto

5.4.8. Caso seja necessário o complemento de informações para atendimento do chamado, que impossibilitem a resolução do chamado pela CONTRATADA, a CONTRATANTE será solicitada para fornecer a informação, e os prazos serão suspensos ou prorrogados até o recebimento das informações.

5.4.9. O tempo em horas, previsto no SLA, será computado a partir da abertura do chamado até a sua regularização, nesse caso, uma solução de contorno poderá ser utilizada, caso a solução definitiva não seja possível de ser executada imediatamente.

5.4.10. A CONTRATADA deverá atender no mínimo 90% (noventa por cento) dos chamados dentro do SLA estabelecido na tabela.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

5.4.11. É garantido à Contratada o direito de contestação dos resultados da apuração do Acordo de Nível de Serviço, bem como de apresentar as justificativas que se fizerem necessárias.

5.4.12. A contestação, desde que devidamente justificada, com a apresentação de documentos comprobatórios dos fatos alegados, poderá anular a incidência de glosas.

5.4.13. As glosas previstas neste Termo de Referência não excluem, nem alteram as penalidades também previstas.

5.5. Requisitos Temporais

5.5.1. O prazo de disponibilidade da assinatura do software se dará em até **10 (dez) dias úteis**, a partir da emissão da nota de empenho e/ou assinatura do CONTRATO.

5.6. Requisitos de Segurança da Informação e Privacidade:

5.6.1. A solução deverá atender aos princípios e procedimentos elencados na Política de Segurança da Informação da Contratante;

5.6.2. Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;

5.6.3. Não compartilhar, sob qualquer forma, informações sigilosas com outros que não tenham necessidade de conhecer.

5.6.4. O Contratado deverá observar integralmente os requisitos da Lei Geral de Proteção de Dados-LGPD.

5.7. Requisitos Sociais, Ambientais e Culturais

5.7.1. Por se tratar exclusivamente de licenciamento de uso de software, não há requisitos desses tipos a serem considerados.

5.8. Requisitos da Arquitetura Tecnológica

5.8.1. O objeto deverá corresponder, integralmente, aos requisitos de arquitetura tecnológica descritos no **Anexo I - Especificações Técnicas do Objeto**

5.8.2.

5.9. Requisitos de Projeto e de Implementação

5.9.1. O objeto deverá observar integralmente os requisitos de projeto e de implementação constantes no **ITEM 7 - Modelo de execução do contrato**.

5.10. Requisitos de Garantia, Manutenção e Assistência Técnica

5.10.1. A CONTRATADA deverá garantir à CONTRATANTE que os softwares licenciados não infrinjam quaisquer patentes, direitos autorais ou “*trade-secrets*”;



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

5.10.2. A garantia deverá ser prestada pelo período de, no mínimo, 36 (trinta e seis) meses, a contar do recebimento definitivo do objeto do CONTRATO, sem nenhum custo adicional para a CONTRATANTE, abrangendo a manutenção corretiva com a cobertura de todo e qualquer defeito apresentado, incluindo substituição de softwares, componentes e acessórios, correções de defeitos que afetem o desempenho, funcionalidade e/ou configuração dos produtos e atualização da versão de novos “*releases*” das licenças de software que incorporem melhorias tecnológicas de desempenho e/ou funcionais (suporte técnico e manutenção), além de eventuais *patches* de segurança e vacinas que surjam durante a vigência da garantia da solução ofertada;

5.10.3. A CONTRATADA deverá garantir que os programas licenciados para o CONTRATANTE operarão, em todos os aspectos essenciais, da forma descrita na respectiva documentação, desempenhando as funções devidamente contratadas;

5.10.3.1. A garantia a que se refere o Caput desta Cláusula inclui todas as ações, sejam elas de manutenção ou outras necessárias, com vistas a garantir o perfeito funcionamento da plataforma licitada, assim como o atendimento às necessidades do CONTRATANTE;

5.10.4. Todas as despesas envolvidas no processo de suporte correrão por conta da CONTRATADA, inclusive as despesas com frete de envio e retorno de profissionais técnicos ou componentes da Solução, sem ônus adicional à CONTRATANTE;

5.10.5. A CONTRATADA deverá possuir Central de Atendimento (contato telefônico, sítio na Internet e e-mail) para consultas, aberturas de chamados técnicos e envio de arquivos para análise, durante 24 (vinte e quatro) horas por dia, 07 (sete) dias por semana

5.10.5.1. Entende-se por hora da solicitação a hora de envio do e-mail, web ou da chamada telefônica;

5.10.5.2. Entende-se por início do atendimento a hora de chegada do técnico ao local determinado no chamado ou a sua atuação de forma remota;

5.10.5.3. Poderá ser solicitado o atendimento *on-site*, restrito ao município-sede do CONTRATANTE, visando à resolução de problemas que não forem solucionados através do atendimento telefônico ou remoto;

5.10.5.4. A CONTRATADA deve possuir pessoal certificado pelo FABRICANTE para a integral execução e manutenção dos serviços;

5.10.5.5. A garantia “*on-site*” deverá observar os prazos estabelecidos neste TERMO DE REFERÊNCIA, contados a partir da data e hora do chamado, com tempo de resposta e solução indicados na proposta, de acordo com item 12;



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

5.10.6. Deverá ser informado link (URL) de site na Internet do FABRICANTE da solução ofertada com disponibilidade de informações para suporte, tais como: guias de instalação, informações técnicas, atualização.

5.10.7. Os técnicos, ou pessoas autorizadas pela CONTRATADA, deverão apresentar, no ato do atendimento, credenciamento (crachá da CONTRATADA) e documento de identidade pessoal (RG), para efetuarem qualquer serviço nas dependências da CONTRATANTE;

5.10.8. Após cada atendimento técnico, a CONTRATADA deverá emitir, no ato, relatório técnico do atendimento onde deverão constar, obrigatoriamente, os seguintes dados: data e horário da abertura do chamado, horário de início e término do atendimento, número do chamado, nome do técnico responsável pelo atendimento, descrição do problema relatado pela CONTRATANTE, descrição do problema realmente encontrado com a solução dada ao problema e local para atesto dos servidores da CONTRATANTE.

5.10.8.1. A CONTRATADA deverá deixar cópia do relatório com servidor da CONTRATANTE responsável pelo acompanhamento do atendimento técnico;

5.10.9. A CONTRATADA compromete-se a manter registros escritos dos referidos chamados constando o nome do técnico da CONTRATADA e uma descrição resumida do problema.

5.10.10.

5.11. Requisitos de capacitação técnica

5.12. A LICITANTE deverá comprovar que já forneceu, para pessoa jurídica de direito público ou privado, solução compatível com o objeto desta licitação, demonstrando a experiência no fornecimento, instalação, configuração, ativação e suporte técnico da solução ofertada;

5.12.1. Não serão considerados atestados emitidos por distribuidor ou FABRICANTE das soluções cotadas, em favor da licitante. Em qualquer caso o atestado deverá ser emitido pela empresa que contratou os produtos/serviços (cliente final) em favor da licitante;

5.12.2. Os atestados devem conter identificação clara e informação de contato da pessoa que assinou o mesmo;

5.12.3. Tal exigência se faz necessária por se tratar de fornecimentos e serviços que devem ser executados por profissionais que detenham conhecimento específico dos produtos, que são desenvolvidos pelo FABRICANTE das soluções e softwares, no sentido de respaldar a garantia fornecida pelo FABRICANTE e, ainda, garantir maior segurança para a CONTRATANTE.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

5.13. A LICITANTE deverá apresentar junto à proposta, sob pena de desclassificação, Declaração de que ela mesma é responsável pelos serviços de garantia e manutenção remota e *on-site* ou indicando a Rede de Assistência Técnica Autorizada;

5.14. A CONTRATADA deverá comprovar na data da Assinatura do CONTRATO que a equipe técnica que realizará a instalação será composta por profissionais que possuam, no mínimo, as certificações a seguir:

5.14.1. Certificação emitida pelo FABRICANTE, que fornece ao profissional a validação da proficiência necessária para a instalação, configuração e administração da solução;

5.15. A comprovação da capacitação técnica dar-se-á mediante a apresentação de certificado(s) de cada instituição/FABRICANTE. As certificações deverão ser obrigatoriamente técnicas e do mesmo FABRICANTE dos produtos cotados. Não serão aceitas certificações comerciais;

5.16. Requisitos de Experiência Profissional

5.16.1. Visando a garantir a qualidade dos serviços ofertados, a CONTRATADA deverá, até 05 (cinco) dias após a **data de assinatura do Contrato**, comprovar que possui em seu corpo técnico permanente, pelo menos 01 (um) técnico com certificação oficial fornecida pelo(s) FABRICANTE(s) dos produtos (soluções e licenças). A comprovação de possuir profissional no quadro permanente far-se-á mediante a apresentação de um dos seguintes documentos:

5.16.1.1. Cópia da Carteira de Trabalho e Previdência Social – CTPS;

5.16.1.2. Cópia do ato de investidura do cargo ou cópia do Contrato social, quando se tratar de diretor ou sócio;

5.16.1.3. Contrato de prestação de serviços, regido pela legislação comum.

5.17. Requisitos de Formação da Equipe

5.17.1. Não serão exigidos requisitos de formação da equipe para a presente contratação.

5.18. Requisitos de Metodologia de Trabalho

5.18.1. O licenciamento deverá ser entregue no formato eletrônico, encaminhado para o e-mail **cmti_rede@mpma.mp.br**.

5.18.2. Após o recebimento e aplicação das subscrições adquiridas, a interface web de gerência da plataforma, deve permitir verificar o novo período de vigência do serviço.

5.18.3. Constatada a ocorrência de divergência na especificação do objeto entregue, fica a CONTRATADA obrigada a providenciar a substituição em até 05 (cinco) dias úteis, contados a partir do recebimento da notificação da ocorrência por parte da CONTRATANTE.

5.19. Sustentabilidade:



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

5.20.1 Por se tratar exclusivamente de licenciamento de uso de software, e considerando a natureza do objeto que não envolve consumo de materiais físicos, deslocamento de equipes ou impacto ambiental direto na sua execução, não se aplicam requisitos sociais, ambientais e culturais específicos diretamente vinculados à entrega do produto. Contudo, a Contratante valoriza e incentiva a adoção de práticas de sustentabilidade por parte das empresas fornecedoras em suas operações gerais.

5.20. Informações relevantes para o dimensionamento E/OU apresentação da proposta

5.21.1 Todos os itens necessários para a correta e eficiente implantação e operacionalização da solução ofertada deverão ser dispostos, quantificados e precificados.

5.21.2 A CONTRATANTE realizará a análise de conformidade da proposta técnica de cada LICITANTE confrontando os requisitos especificados no TERMO DE REFERÊNCIA com as características da solução ofertada.

6. PAPÉIS E RESPONSABILIDADES

6.1. São obrigações da CONTRATANTE (conforme art. 117 da Lei nº 14.133/2021):

- 6.1.1. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
- 6.1.2. encaminhar formalmente a demanda por meio de Nota de Empenho, Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;
- 6.1.3. receber o objeto fornecido pelo Contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- 6.1.4. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;
- 6.1.5. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
- 6.1.6. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;
- 6.1.7. definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte do Contratado, com base em pesquisas de mercado, quando aplicável;
- 6.1.8. prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer.

6.2. São obrigações do CONTRATADO (conforme art. 118 da Lei nº 14.133/2021):



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 6.2.1. indicar formalmente preposto apto a representá-la junto à Contratante, que deverá responder pela fiel execução do contrato;
- 6.2.2. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
- 6.2.3. reparar quaisquer danos diretamente causados à Contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução do contrato pela Contratante;
- 6.2.4. propiciar todos os meios necessários à fiscalização do contrato pela Contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;
- 6.2.5. manter, durante toda a execução do contrato, as mesmas condições da habilitação;
- 6.2.6. quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;
- 6.2.7. quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do contrato;
- 6.2.8. ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;
- 6.2.9. fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos do contratante ou da nova empresa que continuará a execução do contrato, quando for o caso.

7. MODELO DE EXECUÇÃO DO CONTRATO

7.1. Rotinas de Execução

7.1.1. Do Encaminhamento Formal de Demandas

7.1.1.1. O gestor do contrato ou fiscal administrativo enviará a nota de empenho, por meio eletrônico, para a CONTRATADA, visando as devidas providências para a entrega do objeto;

7.1.1.2. O recebimento provisório e definitivo dos bens é disciplinado no tópico 9. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO deste Termo de Referência .

7.2. Forma de execução e acompanhamento do contrato



**ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO**

7.2.1. Condições de Entrega

7.2.1.1. O prazo de disponibilidade da assinatura do software se dará em até **10 (dez) dias úteis**, a partir da emissão da nota de empenho e/ou assinatura do CONTRATO.

7.2.1.2. Eventual pedido de prorrogação de prazo de entrega deverá ser encaminhado para o endereço de e-mail cmti_rede@mpma.mp.br.

7.2.1.3. Serão injustificados os atrasos não comunicados tempestivamente ou indevidamente fundamentados, e a aceitação da justificativa ficará a critério da CONTRATANTE.

7.3. Formas de transferência de conhecimento

7.3.1. Não será necessária transferência de conhecimento devido às características do objeto.

7.4. Procedimentos de transição e finalização do contrato

7.4.1 Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

7.5. Quantidade mínima de bens ou serviços para comparação e controle

7.5.1. Conforme definições deste Termo de Referência.

7.6. Mecanismos formais de comunicação

7.6.1. A comunicação formal entre as partes se dará preferencialmente por escrito, por meio dos endereços de e-mail institucionais da Contratante (cmti_rede@mpma.mp.br para assuntos técnicos e cmti@mpma.mp.br para assuntos administrativos), exceto para a abertura de chamados de suporte do software, que poderá ser realizada também por telefone ou aplicativo web/site do fabricante, conforme orientações da Contratada.

7.7. Formas de Pagamento

7.7.1. Os critérios de medição e pagamento serão tratados em tópico próprio do Modelo de Gestão do Contrato.

8. MODELO DE GESTÃO DO CONTRATO



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

8.1. O contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

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

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

8.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

Formalização da contratação

8.5. A contratação será formalizada mediante a emissão da nota de empenho e/ou assinatura de contrato, cujo envio se dará por meio eletrônico.

8.5.1. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

Fiscalização

8.6. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos ([Lei nº 14.133, de 2021, art. 117, caput](#)).

Fiscalização Técnica

8.7. O fiscal técnico do contrato acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração;

8.7.1. O fiscal técnico do contrato anotar no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. ([Lei nº 14.133, de 2021, art. 117, §1º](#));

8.7.2. Identificada qualquer inexecução ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção;

8.7.3. O fiscal técnico do contrato informará ao gestor do contrato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso.

8.7.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprezadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

8.7.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual.

Fiscalização Administrativa

8.8. O fiscal administrativo do contrato verificará a manutenção das condições de habilitação da contratada, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário.

8.8.1. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência.

Gestor do Contrato

8.9. O gestor do contrato coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração..

8.10. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência.

8.11. O gestor do contrato acompanhará a manutenção das condições de habilitação da contratada, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais.

8.12. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações.

8.13. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso.

8.14. O gestor do contrato deverá elaborar relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração.

8.15. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.



**ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO**

Critérios de Aceitação

8.16. A avaliação da qualidade do objeto entregue, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

8.17. Todas as licenças, referentes ao software solicitado, devem estar registradas para utilização do Contratante, legalizado, não sendo admitidas versões “shareware” ou “trial”.

8.18. Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao Contratante o direito de não receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no CONTRATO. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

Procedimentos de Teste e Inspeção

8.19. Não se aplica

Níveis Mínimos de Serviço Exigidos

8.20. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pela Contratante para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

IAP – INDICADOR DE ATENDIMENTO NO PRAZO		
Tópico	Descrição	
Finalidade	Medir o tempo de atraso na entrega do objeto	
Meta a cumprir	10 dias úteis	A meta definida visa garantir a entrega do objeto dentro do prazo previsto.
Instrumento de medição	Envio de nota de empenho e/ou data de assinatura do contrato, Termo de Recebimento Provisório (TRP) e Termo de Recebimento Definitivo (TRD)	
Forma de acompanhamento	A avaliação será feita conforme linha de base da data de envio da Nota de Empenho e/ou da data de assinatura de contrato. Será subtraída a data de entrega do objeto (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início	



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

	da contagem de prazos, com o envio de nota de empenho e/ou assinatura de contrato.
Periodicidade	Uma única vez com a assinatura do Termo de Recebimento Definitivo
Mecanismo de Cálculo (métrica)	IAP = <u>DEO – DENE</u>C Onde: IAP – Indicador de Atendimento no Prazo; DEO – Data de Entrega do Objeto. A data de entrega deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução continua a correr, findando-se apenas quanto o Contratado entregar objeto e houver aceitação por parte do fiscal técnico. DENEC – Data de Envio da Nota de Empenho e/ou data de assinatura do Contrato. A data de início será aquela do envio da nota de empenho (por meio eletrônico) e/ou da assinatura do contrato.
Observações	Obs1: Serão utilizados dias úteis na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias úteis no cômputo do indicador.
Início de Vigência	A partir do envio da nota de empenho e/ou da assinatura do contrato.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador IAP: Menor ou igual a 0 – Pagamento integral; De 1 a 60 – aplicar-se-á glosa de 0,1666% por dia de atraso sobre o valor da nota fiscal; Acima de 60 – aplicar-se-á glosa de 10% bem como multa de 2% sobre o valor da nota fiscal.
Exemplo de Aplicação das Sanções do IAP	- Se o prazo de entrega for de 10 dias úteis e o objeto for entregue no 15º dia útil (5 dias de atraso), o IAP será 5. A glosa aplicada será de 0,1666% por dia de atraso sobre o valor da nota fiscal, totalizando $0,1666\% \times 5 = 0,833\%$ do valor da NF. - Se o prazo de entrega for de 10 dias úteis e o objeto for entregue no 75º dia útil (65 dias de atraso), o IAP será 65. Neste caso, aplicar-se-á glosa de 10%



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

	bem como multa de 2% sobre o valor da nota fiscal, conforme a faixa 'Acima de 60'.
--	--

Procedimentos para retenção ou glosa no pagamento

8.21. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme a tabxela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Não prestar os esclarecimentos imediatamente, referente à execução do contrato, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 72 (setenta e duas) horas.	Multa de 5% sobre o valor total do Contrato/Nota Fiscal-NF por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela Contratante, até o limite de 3 (três) dias.
		Após o limite de 15 (quinze) dias, aplicar-se-á multa de 10% do valor total do Contrato/NF.
2	Não atender ao indicador de nível de serviço IAP (Indicador de Atendimento no Prazo)	Glosa de 1% sobre o valor da NF para valores do indicador IAP de 0,11 a 0,20.
		Glosa de 2% sobre o valor da NF para valores do indicador IAP de 0,21 a 0,30.
		Glosa de 5% sobre o valor da NF para valores do indicador IAP de 0,31 a 0,50.
		Glosa de 7% sobre o valor da NF para valores do indicador IAP de 0,51 a 1,00.
		Multa de 10% sobre o valor do Contrato/NF, para valores do indicador IAP maiores que 1,00.
N	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 15% do valor total do Contrato.

8.22. Nos termos do Inciso II, do art. 25 da Resolução do CNMP nº 238, de 5 de fevereiro de 2024, será fixado os valores e procedimentos para retenção ou glosa no pagamento, sem prejuízo das sanções cabíveis, quando a contratada:

8.22.1. Não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

8.22.2. Deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TI, ou utilizá-los com qualidade ou quantidade inferior à demandada.

9. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento

9.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável do acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

9.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 5 (cinco) dias úteis, a contar da notificação da contratada, às suas custas, sem prejuízo da aplicação das penalidades.

9.3. O recebimento definitivo ocorrerá no prazo de 10 (dez) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação pela Contratante, com a solicitação de autorização de liquidação e pagamento da nota fiscal recebida.

9.4. Para as contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o [inciso II do art. 75 da Lei nº 14.133, de 2021](#), o prazo será reduzido à metade, mantendo-se a possibilidade de prorrogação.

9.5. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

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

9.7. O prazo para a solução, pelo contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

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

Liquidação

9.9. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

9.9.1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o [inciso II do art. 75 da Lei nº 14.133, de 2021](#).

9.10. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

9.10.1. O prazo de validade;

9.10.2. A data da emissão;

9.10.3. Os dados do contrato e do órgão contratante;

9.10.4. O período respectivo de execução do contrato;

9.10.5. O valor a pagar; e

9.10.6. Eventual destaque do valor de retenções tributárias cabíveis.

9.11. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

9.12. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta *on-line* ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no [art. 68 da Lei nº 14.133, de 2021](#).

9.13. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

9.14. Constatando-se, junto ao SICAF, a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante.

9.15. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

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



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

9.17. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

9.18. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior

9.19. No caso de atraso de pagamento, desde que o CONTRATADO não tenha concorrido de alguma forma para tanto, serão devidos, pela CONTRATANTE, encargos moratórios à taxa nominal de 6% a.a. (seis por cento ao ano), capitalizados diariamente em regime de juros simples:

9.19.1. O valor dos encargos será calculado pela fórmula: $EM = I \times N \times VP$, onde: EM = Encargos moratórios devidos; N = Número de dias entre a data prevista para o pagamento e a do efetivo pagamento; I = Índice de compensação financeira = 0,00016438; e VP = Valor da prestação em atraso. Antes de cada pagamento à contratada, será realizada consulta ao SICAF para verificar a manutenção das condições de habilitação exigidas no edital.

9.20.

Forma de pagamento

9.21. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta correntes indicadas pelo contratado.

9.22. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

9.23. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

9.23.1. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

9.24. O contratado regularmente optante pelo Simples Nacional, nos termos da [Lei Complementar nº 123, de 2006](#), não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

10. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

10.1. Comete infração administrativa nos termos da Lei nº 14.133/2021, a Contratada que:

10.1.1. Der causa à inexecução parcial do contrato;

10.1.2. Der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 10.1.3. Der causa à inexecução total do contrato;
- 10.1.4. Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- 10.1.5. Apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- 10.1.6. Praticar ato fraudulento na execução do contrato;
- 10.1.7. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- 10.1.8. Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.
- 10.2.** Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:
- 10.2.1. **Advertência**, quando o contratado der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);
- 10.2.2. **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nos subitens 10.1.2 a 10.1.4 desta cláusula, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);
- 10.2.3. **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nos subitens 10.1.5 a 10.1.8 do subitem acima do Contrato, bem como nos subitens 10.1.2 a 10.1.4, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).
- 10.2.4. **Multa:**
- 10.2.4.1. **Moratória** de 1% (um por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;
- 10.2.4.2. Moratória de 0,07% (sete centésimos por cento) do valor total do contrato por dia de atraso injustificado, até o máximo de 2% (dois por cento), pela inobservância do prazo fixado para apresentação, suplementação ou reposição da garantia.
- 10.2.4.3. O atraso superior a 30 (trinta) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.
- 10.2.4.4. **Compensatória**, para as infrações previstas nos subitens 10.1.5 a 10.1.8 de 5% a 15% do valor do contrato;
- 10.2.4.5. **Compensatória**, para a inexecução total do contrato prevista no subitem



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO
10.1.3 de 20% a 30% do valor do contrato;

10.2.4.6. Para as infrações descritas nos subitens 10.1.1, 10.1.2 e 10.1.4, a multa será de 15% a 20% do valor do Contrato.

10.3. A aplicação das sanções previstas neste contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021).

10.4. Todas as sanções previstas neste contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

10.4.1. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021)

10.5. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

10.5.1. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

10.6. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

10.7. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

10.7.1. A natureza e a gravidade da infração cometida;

10.7.2. As peculiaridades do caso concreto;

10.7.3. As circunstâncias agravantes ou atenuantes;

10.7.4. Os danos que dela provierem para o Contratante;

10.7.5. A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

10.8. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

10.9. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Projeto Básico ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021)

10.10. O Contratante deverá, no prazo máximo 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021)

10.11. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

10.12. Os débitos do contratado para com a Procuradoria Geral de Justiça, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

11. FORMA E CRITÉRIO DE SELEÇÃO DO FORNECEDOR E FORMA DE FORNECIMENTO

11.1. Forma de seleção e critério de julgamento da proposta

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

11.2. Da aplicação da Margem de Preferência

11.2.1. DO NÃO PARCELAMENTO E DA NÃO APLICAÇÃO DO TRATAMENTO FAVORECIDO ÀS ME/EPP

11.2.2. Da Inviabilidade Técnica de Parcelamento

11.2.2.1. Pela natureza da contratação, que envolve o licenciamento de uso de solução integrada de tecnologia da informação, o parcelamento do objeto não será



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO
adotado, em estrita conformidade com o Art. 40, § 3º, inciso II, da Lei nº 14.133/2021.

11.2.2.2. A solução pretendida configura sistema único e integrado, em que as ferramentas guardam estreita relação de interdependência técnica. A divisão ou fracionamento do fornecimento em lotes ou itens distintos geraria os seguintes prejuízos e riscos inaceitáveis à Administração:

- **Perda de Interoperabilidade e Interrupção:** Riscos à comunicação fluida entre os usuários e à aplicação homogênea de políticas de segurança na rede corporativa;
- **Perda da Responsabilidade Técnica Unificada:** Multiplicidade de fornecedores prestando suporte sobre a mesma plataforma, o que dificulta a responsabilização em caso de falhas críticas ou incidentes de segurança;
- **Incompatibilidade de Gestão (Console Único):** A administração das contas, licenças e segurança de dados exige gestão centralizada em um único console administrativo, sendo inviável segmentar a operação;
- **Elevação do TCO (Custo Total de Propriedade):** O parcelamento acarretaria severo aumento dos custos indiretos de gestão de múltiplos contratos e de eventuais integrações complexas.

11.2.3. Do Afastamento do Tratamento Favorecido da LC nº 123/2006

11.2.3.1. Diante da robusta inviabilidade técnica de parcelamento acima demonstrada, afasta-se a aplicação das regras de exclusividade, cota reservada ou exigência de subcontratação em favor de Microempresas (ME) e Empresas de Pequeno Porte (EPP) estabelecidas na Lei Complementar nº 123/2006.

11.2.3.2. Portanto, o certame será processado em lote global único sob ampla concorrência, exigindo-se dos licitantes o cumprimento integral dos requisitos de qualificação técnica e operacional mínimos definidos neste Termo de Referência, como garantia da segurança operacional e da eficiência dos serviços no Ministério Público do Estado do Maranhão.

11.3. Exigências de habilitação



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

11.4. A LICITANTE deverá comprovar que já forneceu, para pessoa jurídica de direito público ou privado, solução compatível com o objeto desta licitação, demonstrando a experiência no fornecimento, instalação, configuração, ativação e suporte técnico da solução ofertada;

11.4.1. Não serão considerados atestados emitidos por distribuidor ou FABRICANTE das soluções cotadas, em favor da licitante. Em qualquer caso o atestado deverá ser emitido pela empresa que contratou os produtos/serviços (cliente final) em favor da licitante;

11.4.2. Os atestados devem conter identificação clara e informação de contato da pessoa que assinou o mesmo;

11.4.3. Tal exigência se faz necessária por se tratar de fornecimentos e serviços que devem ser executados por profissionais que detenham conhecimento específico dos produtos, que são desenvolvidos pelo FABRICANTE da solução, no sentido de respaldar a garantia fornecida pelo FABRICANTE e, ainda, garantir maior segurança para a CONTRATANTE.

11.5. A LICITANTE deverá apresentar junto à proposta, sob pena de desclassificação, Declaração de que ela mesma é responsável pelos serviços de garantia e manutenção remota e *on-site* ou indicando a Rede de Assistência Técnica Autorizada;

11.6. A CONTRATADA deverá comprovar na data da Assinatura do CONTRATO que a equipe técnica que realizará a instalação será composta por profissionais que possuam, no mínimo, as certificações a seguir:

11.6.1. Certificação emitida pelo FABRICANTE, que fornece ao profissional a validação da proficiência necessária para a instalação, configuração e administração da solução;

11.6.2. A comprovação da capacitação técnica dar-se-á mediante a apresentação de certificado(s) de cada instituição/FABRICANTE. As certificações deverão ser obrigatoriamente técnicas e do mesmo FABRICANTE dos produtos cotados. Não serão aceitas certificações comerciais;

11.7. Visando a garantir a qualidade dos serviços ofertados, a CONTRATADA deverá, até 05 (cinco) dias após a **data de assinatura do Contrato**, comprovar que possui em seu corpo técnico permanente, pelo menos 01 (um) técnico com certificação oficial fornecida pelo(s) FABRICANTE(s) dos produtos (software e licenças). A comprovação de possuir profissional no quadro permanente far-se-á mediante a apresentação de um dos seguintes documentos:

11.7.1. Cópia da Carteira de Trabalho e Previdência Social – CTPS;

11.7.2. Cópia do ato de investidura do cargo ou cópia do Contrato social, quando se tratar de diretor ou sócio;

11.8. Contrato de prestação de serviços, regido pela legislação comum.

12. DA VIGÊNCIA CONTRATUAL



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

12.1. O prazo de vigência terá seu início com a assinatura do contrato e término ao final do período de 36 (trinta e seis) meses previsto para atualização, suporte e assistência técnica da assinatura do software.

12.2. Para início do prazo de 36 (trinta e seis) meses de atualização, suporte e assistência técnica, será considerada a data do recebimento definitivo da assinatura do software, na forma prevista neste termo de referência.

12.3. As obrigações recíprocas, decorrentes da presente contratação, correspondem ao estabelecido neste Termo de Referência, na proposta comercial da contratada e ainda no disposto na Lei 14.133, de 2021 e demais normas pertinentes;

12.4. O encerramento da vigência contratual não prejudica a manutenção das obrigações das partes, no que se refere aos bens/serviços em garantia, além de estar conciliado com as datas de execução, entrega, observação e recebimento definitivo do objeto contratual e pagamento, de acordo com os termos já descritos neste TERMO DE REFERÊNCIA;

13. REAJUSTE DO CONTRATO

13.1. Os preços inicialmente contratados são fixos e irredutíveis no prazo de um ano contado da data do orçamento estimado (data da pesquisa de mercado), em 18/06/2026;

13.2. Dentro do prazo de vigência do contrato e mediante solicitação da contratada, os preços contratados poderão sofrer reajuste após o interregno de um ano, contado da data do orçamento estimado, aplicando-se o índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada – IPEA, exclusivamente, para as obrigações iniciadas e concluídas após a ocorrência da anualidade;

13.3. Nos reajustes subsequentes ao primeiro, o intervalo mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste;

13.4. No caso de atraso ou não divulgação do índice de reajustamento, o CONTRATANTE pagará à CONTRATADA a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo. Fica a CONTRATADA obrigada a apresentar memória de cálculo referente ao reajustamento de preços do valor remanescente, sempre que este ocorrer;

13.5. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo;



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

13.6. Caso o índice estabelecido para reajustamento venha a ser extinto ou de qualquer forma não possa mais ser utilizado, será adotado, em substituição, o que vier a ser determinado pela legislação então em vigor;

13.7. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo;

13.8. O reajuste será realizado por apostilamento;

13.9. Caso a CONTRATADA não requeira tempestivamente o reajuste e prorrogue o contrato sem pleiteá-lo, ocorrerá a preclusão do direito;

13.10. Também ocorrerá a preclusão do direito ao reajuste se o pedido for formulado depois de extinto o contrato.

14. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

14.1. O custo total para aquisição do objeto é de **R\$1.228.750,00 (um milhão, duzentos e vinte oito mil, setecentos e cinquenta reais)**, baseado na pesquisa de mercado realizada (anexo mapa de preços), conforme demonstrado no quadro a seguir:

Item	Especificação	CATMAT	Quantidade	Valor Unitário	Valor Total
1	Atualização de licença de software antivírus Kaspersky Endpoint Security for Advanced Brazilian Edition com upgrade para KASPERSKY NEXT EDR OPTIMUM, por um período de atualização, suporte e assistência técnica de 36 (trinta e seis) meses, e demais detalhamentos descritos no termo de referência.	27456 CATSER	5000	R\$ 245,75	R\$1.228.750,00

15. DO REGISTRO DE PREÇOS

Justificativa para formação



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

15.1. Tendo em vista a impossibilidade de se definir, de forma prévia e precisa, o quantitativo de materiais e serviços a serem demandados, sugere-se a realização de licitação na modalidade de pregão, ata de registro de preços do tipo menor preço ou maior desconto, nos termos do inciso XLI, artigo 6º, da lei 14.133/2021;

15.2. A adoção do SRP justifica-se com base no art. 82, inciso II, da Lei nº 14.133/2021, pela conveniência da contratação de serviços com previsão de demandas futuras e parceladas.

Do Gerenciamento da Ata de Registro de Preços e das Adesões (Caronas)

15.3. O Ministério Público do Maranhão atuará como **Órgão Gerenciador** da Ata de Registro de Preços, sendo responsável pela condução dos procedimentos de renegociação, controle de saldos e autorização de adesões.

15.4. Da Admissibilidade de Adesão (Carona):

15.4.1. Nos termos do art. 86, § 2º, da Lei nº 14.133/2021, **será admitida a adesão** à Ata de Registro de Preços decorrente desta licitação por órgãos e entidades da Administração Pública que não participaram do procedimento licitatório (órgãos não participantes), desde que devidamente justificada a vantagem e mediante prévia consulta e anuência do Órgão Gerenciador e do Fornecedor.

15.4.2. A permissão para adesão justifica-se pelo potencial ganho de escala, atratividade econômica para o mercado fornecedor e racionalização administrativa, alinhando-se aos princípios da eficiência e economicidade.

15.5. Dos Limites de Quantitativos para Adesão:

15.5.1. As adesões por órgãos não participantes ficam condicionadas aos seguintes limites, conforme regulamentação vigente (Decreto Federal nº 11.462/2023, arts. 31 e 32):

15.5.1.1. Limite Individual: Cada órgão ou entidade não participante poderá aderir a até **50% (cinquenta por cento)** dos quantitativos dos itens registrados na Ata;

15.5.1.2. Limite Global: O quantitativo total decorrente das adesões (soma de todos os caronas) não poderá exceder, na totalidade, ao **dobro (2x)** do quantitativo de cada item registrado na Ata.

15.6. Do Procedimento de Adesão:

15.6.1. Caberá ao órgão não participante interessado solicitar formalmente a adesão ao Órgão Gerenciador (MPMA), instruindo o pedido com a demonstração da vantajosidade e a aceitação do Fornecedor.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

15.6.2. O Órgão Gerenciador somente autorizará a adesão após verificar se o saldo de "carona" disponível (limite do dobro) comporta a demanda, e se a adesão não prejudicará as obrigações assumidas com o MPMA.

15.7. Da Faculdade do Fornecedor:

15.7.1. O fornecedor beneficiário da Ata de Registro de Preços, desde que observadas as obrigações com o Órgão Gerenciador, poderá aceitar ou recusar o fornecimento aos órgãos não participantes, sem prejuízo das penalidades, caso a execução do carona comprometa a capacidade operativa de atendimento ao MPMA.

15.8. As aquisições ou contratações adicionais decorrentes de adesões não poderão exceder, por órgão ou entidade, a **50% (cinquenta por cento)** dos quantitativos dos itens do instrumento convocatório e registrados na ata de registro de preços para o órgão gerenciador e para os órgãos participantes.

Da Vigência

15.9. A validade da Ata de Registro de Preços será de 1 (um) ano, contado a partir do primeiro dia útil subsequente à data de divulgação no PNCP, podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso.

16. ADEQUAÇÃO ORÇAMENTÁRIA

16.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento da Procuradoria Geral de Justiça do Maranhão.

16.2. A contratação será atendida pela seguinte dotação:

Ação: Plano de Contratações Anual 2027;

Subação;;

Natureza de despesa: Investimento;

Nível de prioridade: Alta.

Cronograma Físico-Financeiro

Evento	Prazo estimado	Valor
Entrega do Objeto	Até 10 dias úteis a partir da emissão da nota de empenho e/ou assinatura do CONTRATO	



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

Recebimento total do Objeto	10 dias úteis após a entrega do objeto, podendo ser prorrogável por igual período, em caso de inconformidades	
Pagamento	10 dias úteis após a liquidação de despesa	R\$1.228.750,00

Equipe de Planejamento da Contratação			
Gestor do Contrato	Fiscal Requisitante	Fiscal Técnico	Fiscal Administrativa
THIAGO NUNES DE SOUSA:02743842300 Assinado de forma digital por THIAGO NUNES DE SOUSA:02743842300 Dados: 2026.10.21 10:57:47 -03'00'	DIEGO WALISSON PEREIRA CAMARA SANTOS:00678931399 Assinado de forma digital por DIEGO WALISSON PEREIRA CAMARA SANTOS:00678931399 Dados: 2026.10.21 10:51:40 -03'00'	LEONARDO DORNELES FIGUEIREDO SILVA:02490915347 Assinado de forma digital por LEONARDO DORNELES FIGUEIREDO SILVA:02490915347 Dados: 2026.10.21 10:33:11 -03'00'	
Thiago Nunes de Sousa	Diego Walisson Pereira Camara Santos	Leonardo Dorneles Figueiredo Silva	Daniela Nascimento Montelo
Matrícula: 1071452	Matrícula: 1070278	Matrícula: 1071397	Matrícula: 1071575

Anexo I - Especificações Técnicas do Objeto



**ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO**

1 ESPECIFICAÇÕES TÉCNICAS DO OBJETO

1.1 Constitui objeto desta LICITAÇÃO a aquisição e atualização de licenças de uso de software antivírus, para fins de proteção da rede lógica, equipamentos de TI e informações, por um período de atualização, suporte e assistência técnica de, no mínimo, 36 (trinta e seis) meses, aplicação das novas licenças e versões do software, configuração e suporte técnico remoto e on-site, todos necessários para manter atualizada a solução de segurança contra códigos maliciosos, minimizando, assim, os riscos de segurança da informação. O objeto deverá ser entregue de acordo com as especificações técnicas a seguir:

1.2 Do módulo de proteção de endpoint

1.2.1 A solução proposta deverá proteger os sistemas operacionais abaixo:

1.2.1.1 Windows 7

1.2.1.2 Windows 8

1.2.1.3 Windows 8.1

1.2.1.4 Windows 10

1.2.1.5 Windows 11

1.3 Servidores

1.3.1 Windows Small Business Server 2011

1.3.2 Windows MultiPoint Server 2011

1.3.3 Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

1.4 Servidores de terminal Microsoft

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

1.5 Sistemas operacionais Linux de 32 bits:

1.5.1 CentOS 6.7 e posterior

1.5.2 Debian GNU/Linux 11.0 e posterior

1.5.3 Debian GNU/Linux 12.0 e posterior

1.5.4 Red Hat Enterprise Linux 6.7 e posterior

1.6 Sistemas operacionais Linux de 64 bits:

1.6.1.1 Amazon Linux 2.

1.6.1.2 CentOS 6.7 e mais tarde



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

1.6.1.3 CentOS 7.2 e posterior.

1.6.1.4 CentOS Stream 8.

1.6.1.5 CentOS Stream 9.

1.6.1.6 Debian GNU/Linux 11.0 e posterior.

1.6.1.7 Debian GNU/Linux 12.0 e posterior.

1.6.1.8 Linux Mint 20.3 e superior.

1.6.1.9 Linux Mint 21.1 e posterior.

1.6.1.10 openSUSE Leap 15.0 e posterior.

1.6.1.11 Oracle Linux 7.3 e posterior.

1.6.1.12 Oracle Linux 8.0 e posterior.

1.6.1.13 Oracle Linux 9.0 e posterior.

1.6.1.14 Red Hat Enterprise Linux 6.7 e posterior

1.6.1.15 Red Hat Enterprise Linux 7.2 e posterior.

1.6.1.16 Red Hat Enterprise Linux 8.0 e posterior.

1.6.1.17 Red Hat Enterprise Linux 9.0 e posterior.

1.6.1.18 Rocky Linux 8.5 e posterior.

1.6.1.19 Rocky Linux 9.1.

1.6.1.20 SUSE Linux Enterprise Server 12.5 ou posterior.

1.6.1.21 SUSE Linux Enterprise Server 15 ou posterior.

1.6.1.22 Ubuntu 20.04 LTS.

1.6.1.23 Ubuntu 22.04 LTS.

1.6.2 Sistemas operacionais Arm de 64 bits:

1.6.2.1 CentOS Stream 9.

1.6.2.2 SUSE Linux Enterprise Server 15.

1.6.2.3 Ubuntu 22.04 LTS.

1.7 Sistemas operacionais MAC OS:

1.7.1.1 macOS 12 – 14

1.8 Ferramentas de virtualização MAC OS:

1.8.1 Parallels Desktop 16 para Mac Business Edition



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

1.8.2 VMware Fusion 11.5 Profissional

1.8.3 VMware Fusion 12 Profissional

1.9 A solução proposta deverá suportar as seguintes plataformas virtuais:

1.9.1 VMware Workstation 17.0.2 Pro

1.9.2 VMware ESXi 8.0 Update 2

1.9.3 Microsoft Hyper-V Server 2019

1.9.4

1.10

2 Do módulo de gerenciamento avançado

2.1 A solução proposta deve suportar arquitetura cloud-native e on-premise;

2.2 A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:

2.2.1 Amazon Web Services

2.2.2 Microsoft Azure

2.3 A solução proposta deve incluir as seguintes opções de integração SIEM:

2.3.1 HP (Microfoco) ArcSight

2.3.2 IBM QRadar

2.3.3 Splunk

2.3.4 Kaspersky KUMA

2.4 A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

2.5 A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

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

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

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



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 2.9 A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.
- 2.10 A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.
- 2.11 A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.
- 2.12 A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.
- 2.13 O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.
- 2.14 O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em um único/múltiplos dispositivos com base nas seguintes regras de ativação:
- 2.14.1 Status do dispositivo
 - 2.14.2 Tag
 - 2.14.3 Diretório ativo
 - 2.14.4 Proprietários de dispositivos
 - 2.14.5 Hardware
- 2.15 A solução proposta deve suportar os seguintes canais de entrega de notificação:
- 2.15.1 E-mail
 - 2.15.2 Registro de sistema
 - 2.15.3 SMS
- 2.16 A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:
- 2.16.1.1 Atributos de rede
 - 2.16.1.2 Nome
 - 2.16.1.3 Domínio e/ou Sufixo de Domínio
 - 2.16.1.4 Endereço de IP
 - 2.16.1.5 Endereço IP para servidor de gerenciamento



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

2.16.1.6	Localização no Active Directory
2.16.1.7	Unidade organizacional
2.16.1.8	Grupo
2.16.1.9	Sistema operacional
2.16.1.10	Número do pacote de serviço
2.16.1.11	Arquitetura Virtual
2.16.1.12	Registro de aplicativos
2.16.1.13	Nome da Aplicação
2.16.1.14	Versão do aplicativo
2.16.1.15	Fabricante
2.16.1.16	Tipo e versão
2.16.1.17	Arquitetura

2.17 A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

2.18 A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

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

2.19.1 Dispositivos Desktop/Servidores

2.19.2 Dispositivos móveis

2.19.3 Dispositivos de rede

2.19.4 Dispositivos virtuais

2.19.5 Componentes OEM

2.19.6 Periféricos de computador

2.19.7 Dispositivos IoT conectados

2.19.8 Telefones VoIP

2.19.9 Repositórios de rede



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 2.20 A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:
- 2.20.1 Nome da Aplicação
 - 2.20.2 Caminho do aplicativo
 - 2.20.3 Metadados do aplicativo
 - 2.20.4 Aplicativo Certificado digital
 - 2.20.5 Categorias de aplicativos predefinidas pelo fornecedor
 - 2.20.6 SHA256 e MD5
- 2.21 A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:
- 2.21.1 Bluetooth
 - 2.21.2 Dispositivos móveis
 - 2.21.3 Modems externos
 - 2.21.4 CD/DVD
 - 2.21.5 Câmeras e scanners
 - 2.21.6 MTPs
 - 2.21.7 E a transferência de dados para dispositivos móveis
- 2.22 A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.
- 2.23 A solução proposta deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.
- 2.24 A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:
- 2.24.1 Estruturas de domínios e grupos de trabalho do Windows
 - 2.24.2 Estruturas de grupos do Active Directory
 - 2.24.3 Conteúdo de um arquivo de texto criado manualmente pelo administrador
- 2.25 A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.
- 2.26 A solução proposta deve permitir realizar as seguintes ações para endpoints:



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 2.26.1 Verificação manual;
- 2.26.2 Verificação no acesso;
- 2.26.3 Verificação por demanda;
- 2.26.4 Verificação de arquivos compactados
- 2.26.5 Verificação de arquivos individuais, pastas e unidades;
- 2.26.6 Bloqueio e verificação de scripts
- 2.26.7 Proteção contra alteração de registros;
- 2.26.8 Proteção contra estouro de buffer;
- 2.26.9 Verificação em segundo plano/inativa
- 2.27 Verificação de unidade removível na conexão com o sistema;
- 2.28 A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.
- 2.29 O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.
- 2.30 A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.
- 2.31 A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.
- 2.32 A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.
- 2.33 A solução proposta deve suportar Windows Failover Cluster.
- 2.34 A solução proposta deve ter um recurso de clustering integrado.
- 2.35 A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.
- 2.36 A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.
- 2.37 O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.
- 2.38 A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.
- 2.39 A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.
- 2.40 A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.
- 2.41 A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 2.42 A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.
- 2.43 A solução proposta deverá possuir controles para download de DLL e drivers.
- 2.44 A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo específico de prevenção de intrusão.
- 2.45 A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.
- 2.46 A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).
- 2.47 A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.
- 2.48 A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.
- 2.49 A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.
- 2.50 A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.
- 2.51 A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.
- 2.52 A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.
- 2.53 A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.
- 2.54 A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.
- 2.55 A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.
- 2.56 A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.
- 2.57 A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal. .

- 2.58 A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.
- 2.59 A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.
- 2.60 A solução proposta deve permitir ao administrador personalizar relatórios.
- 2.61 A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.
- 2.62 A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.
- 2.63 A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.
- 2.64 A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.
- 2.65 A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.
- 2.66 A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.
- 2.67 O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;
- 2.68 O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.
- 2.69 A solução proposta deve suportar integração com solução APT.
- 2.70 A solução proposta deve suportar a integração com o serviço Managed Detection and Response.
- 2.71 A solução proposta deve permitir instalar o modulo de gerenciamento on-premise nos seguintes sistemas operacionais:
- 2.71.1 Windows
- 2.71.2 Linux
- 2.72 A solução proposta deverá suportar os seguintes servidores de banco de dados:
- 2.72.1 Windows:

2.72.1.1 Microsoft SQL Server

2.72.1.2 Microsoft Banco de dados SQL do Azure



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 2.72.1.3 MySQL Standard e Enterprise
- 2.72.1.4 MariaDB
- 2.72.1.5 PostgreSQL
- 2.72.2 Linux:
 - 2.72.2.1 MySQL
 - 2.72.2.2 MariaDB
 - 2.72.2.3 PostgreSQL
- 2.73 A solução proposta deverá suportar as seguintes plataformas virtuais:
 - 2.73.1 Windows:
 - 2.73.1.1 VMware vSphere 6.7 e 7.0
 - 2.73.1.2 Estação de trabalho VMware 16 Pro
 - 2.73.1.3 Servidor Microsoft Hyper-V 2012 de 64 bits
 - 2.73.1.4 Servidor Microsoft Hyper-V 2012 R2 de 64 bits
 - 2.73.1.5 Microsoft Servidor Hyper -V 2016 de 64 bits
 - 2.73.1.6 Servidor Microsoft Hyper-V 2019 de 64 bits
 - 2.73.1.7 Servidor Microsoft Hyper-V 2022 de 64 bits
 - 2.73.1.8 Citrix XenServer 7.1 LTSR
 - 2.73.1.9 Citrix XenServer 8.x
 - 2.73.1.10 Oracle VM VirtualBox 6.x
 - 2.73.2 Linux:
 - 2.73.2.1 VMware vSphere 6.7, 7.0 e 8.0
 - 2.73.2.2 VMware Desktop 16 Pro e 17 Pro
 - 2.73.2.3 Servidor Microsoft Hyper-V 2012 de 64 bits
 - 2.73.2.4 Servidor Microsoft Hyper-V 2012 R2 de 64 bits
 - 2.73.2.5 Microsoft Servidor Hyper -V 2016 de 64 bits
 - 2.73.2.6 Servidor Microsoft Hyper-V 2019 de 64 bits
 - 2.73.2.7 Servidor Microsoft Hyper-V 2022 de 64 bits
 - 2.73.2.8 Citrix XenServer 7.1 e 8.x
 - 2.73.2.9 Oracle VM VirtualBox 6.x e 7.x
- 2.74 A solução proposta deve suportar criptografia em vários níveis:
 - 2.74.1 Criptografia completa do disco – incluindo disco do sistema
 - 2.74.2 Criptografia de arquivos e pastas
 - 2.74.3 Criptografia de mídia removível
 - 2.74.4 Gerenciamento de criptografia BitLocker e MacOS Filevault2
- 2.75 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 2.75.1 A criptografia de arquivos em unidades de computador locais.
- 2.75.2 A criação de listas de criptografia de arquivos por extensão ou grupo de extensões.
- 2.75.3 A criação de listas criptografadas de pastas em unidades de computador locais.
- 2.76 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:
 - 2.76.1 Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis.
 - 2.76.2 Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais.
- 2.77 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:
 - 2.77.1 A criptografia de todos os arquivos armazenados em unidades removíveis.
 - 2.77.2 A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.
- 2.78 A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia
- 2.79 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.
- 2.80 A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.
- 2.81 A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.
- 2.82 A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.

- 2.83 A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.
- 2.84 A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.
- 2.85 A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.
- 2.86 A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.
- 2.87 A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.
- 2.88 A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.
- 2.89 A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.
- 2.90 A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.
- 2.91 O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados, independentemente da localização e/ou usuário.
- 2.92 A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.
- 2.93 A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.
- 2.94 A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:
- 2.94.1 Uso do Trusted Platform Module e configurações de senha.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 2.94.2 Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.
- 2.95 Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).
- 2.96 A solução proposta deve suportar criptografia em Microsoft Surface Tablets.
- 2.97 A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:
- 2.97.1 Instalação remota de software de terceiros
 - 2.97.2 Relatórios sobre software e hardware existentes
 - 2.97.3 Monitoramento para instalação de software não autorizado
 - 2.97.4 Remoção de software não autorizado
- 2.98 A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.
- 2.99 A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.
- 2.100 A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.
- 2.101 A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.
- 2.102 A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.
- 2.103 A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.
- 2.104 O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.
- 2.105 A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de aplicativos, bem como do fornecedor de segurança
- 2.106 A solução proposta deve permitir ao administrador aprovar atualizações.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 2.107 A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.
- 2.108 A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.
- 2.109 A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.
- 2.110 A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.
- 2.111 A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.
- 2.112 A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).
- 2.113 A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.
- 2.114 A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.
- 2.115 A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’.
- 2.116 A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”.
- 2.117 A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.
- 2.118 A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.
- 2.119 A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.
- 2.120 A solução proposta deve apoiar a implantação do sistema operacional.
- 2.121 A solução proposta deve suportar Wake-on LAN e UEFI.
- 2.122 A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.
- 2.123 A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 2.124 A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.
- 2.125 A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.
- 2.126 A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.
- 2.127 A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.
- 2.128 A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI, bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.
- 2.129 A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.
- 2.130 A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.
- 2.131 A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:
- 2.131.1 Inicie a instalação ao reiniciar ou desligar o computador.
 - 2.131.2 Instale o gerador necessário todos os pré-requisitos do sistema.
- 2.132 Permitir a instalação de novas versões de aplicativos durante as atualizações.
- 2.133 Baixe atualizações para o dispositivo sem instalá-las.
- 2.134 A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.
- 2.135 A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.
- 2.136 O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:
- 2.136.1 CEF;
 - 2.136.2 LEEF;
- 2.137 A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.
- 2.138 O relatório da solução proposta deve conter informações CVE.
- 2.139 A solução proposta deve suportar instalação de aplicações e software de terceiros;
- 2.140

3 Do módulo de gerenciamento simplificado

- 3.1 A solução proposta deve suportar arquitetura cloud;**



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 3.2 A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.
- 3.3 O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.
- 3.4 A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.
- 3.5 A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.
- 3.6 A solução proposta deve atender as condições apontadas no item e subítemes 6.
- 3.7 A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.
- 3.8 A solução proposta deve incluir informações do endpoint:
 - 3.8.1 IP público de internet;
 - 3.8.2 IP interno do dispositivo;
 - 3.8.3 Versão do agente de proteção;
 - 3.8.4 Última comunicação com a console, contendo data e hora;
 - 3.8.5 Informações do sistema operacional;
- 3.9 A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.
- 3.10 A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.
- 3.11 A solução proposta deve incluir treinamento em segurança cibernética.

4 Requisitos gerais

- 4.1 A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:
 - 4.1.1 Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.
- 4.2 A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.
- 4.3 A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).
- 4.4 A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.
- 4.5 A solução proposta deve suportar o subsistema Linux no Windows.
- 4.6 A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:
 - 4.6.1 Proteção contra ameaças sem arquivos (Fileless);
 - 4.6.2 Fornecimento de proteção baseada em machine learning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 4.7 A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;
- 4.8 A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.
- 4.9 A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.
- 4.10 A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.
- 4.11 A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.
- 4.12 A solução proposta deve fornecer análise comportamental baseada em machine learning.
- 4.13 A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.
- 4.14 A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:
- 4.14.1 Controles de aplicativos,
 - 4.14.2 Controle web e dispositivos
 - 4.14.3 HIPS e Firewall
 - 4.14.4 Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;
 - 4.14.5 Gerenciamento de criptografia de arquivos e discos;
 - 4.14.6 Controle adaptativo para detecção de anomalias;
- 4.15 A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.
- 4.16 A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.
- 4.17 A solução proposta deve ter bancos de dados de reputação locais e globais.
- 4.18 A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 4.19 A solução proposta deve incluir um módulo capaz, no mínimo, de:
- 4.19.1 Bloqueio de aplicativos com base em sua categorização.
 - 4.19.2 Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.
 - 4.19.3 A adição de sub-redes e a modificação de permissões de atividade.
- 4.20 A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.
- 4.21 A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.
- 4.22 A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.
- 4.23 A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:
- 4.23.1 Modo silencioso;
 - 4.23.2 Discos rígidos e dispositivos removíveis;
 - 4.23.3 De todos as contas de usuários do dispositivo.
- 4.24 A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:
- 4.24.1 Exclusão imediata de dados;
 - 4.24.2 Exclusão de dados adiada.
- 4.25 A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:
- 4.25.1 Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
 - 4.25.2 Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.
- 4.26 A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.
- 4.27 A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.
- 4.28 A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 4.29 A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.
- 4.30 A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.
- 4.31 A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.
- 4.32 A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.
- 4.33 A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;
- 4.34 A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;
- 4.35 A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.
- 4.36 A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.
- 4.37 A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.
- 4.38 A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.
- 4.39 A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.
- 4.40 A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.
- 4.41 A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.
- 4.42 A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO
USB ou permitir o acesso apenas aos dispositivos permitidos.

- 4.43 A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.
- 4.44 A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.
- 4.45 A solução proposta deve ter categoria de detecção para bloquear banners de sites.
- 4.46 A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;
- 4.47 A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.
- 4.48 A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.
- 4.49 A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.
- 4.50 A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;
- 4.51 A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.
- 4.52 A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.
- 4.53 A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.
- 4.54 O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.
- 4.55 O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista de permissões.
- 4.56 A solução proposta deve suportar o controle de scripts executados em PowerShell.
- 4.57 A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.
- 4.58 A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 4.59 A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.
- 4.60 A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.
- 4.61 A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.
- 4.62 A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.
- 4.63 A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:
- 4.63.1 Filtro de anexos.
 - 4.63.2 Verificação de mensagens de email ao receber, ler e enviar.
- 4.64 A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.
- 4.65 A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;
- 4.66 A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);
- 4.67 A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registro do sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.
- 4.68 A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.
- 4.69 A solução proposta deve incluir suporte ao protocolo IPv6.
- 4.70 A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.
- 4.71 A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:
- 4.72 Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.
- 4.73 Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 4.74 A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.
- 4.75 A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.
- 4.76 A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.
- 4.77 A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.
- 4.78 A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.
- 4.79 A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.
- 4.80 A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.
- 4.81 A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia, bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.
- 4.82 A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.
- 4.83 A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.
- 4.84 A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.
- 4.85 A solução proposta deve suportar endereços IPv6.
- 4.86 A solução proposta deve suportar verificação em duas etapas (autenticação).
- 4.87 A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.
- 4.88 A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.
- 4.89 A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

criar um pacote de instalação independente para instalação do endpoint de segurança localmente.

- 4.90 A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.
- 4.91 A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.
- 4.92 A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.
- 4.93 A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.
- 4.94 A solução proposta deve permitir a gestão de um componente que controle o trabalho com dispositivos de E/S externos.
- 4.95 A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.
- 4.96 A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.
- 4.97 A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.
- 4.98 A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.
- 4.99 A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.
- 4.100 A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.
- 4.101 A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.
- 4.102 A solução proposta deve ter a capacidade de excluir atualizações baixadas.
- 4.103 A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.
- 4.104 A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.
- 4.105 A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO
tempo real dos sensores de endpoints.

- 4.106 A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.
- 4.107 Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.
- 4.108 A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.
- 4.109 A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.
- 4.110 A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.
- 4.111 A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:
- 4.112 Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.
- 4.113 Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.
- 4.114 A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.
- 4.115 A solução proposta deve gerar relatórios de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

5 Do módulo de gerenciamento de dispositivos móveis

- 5.1 O módulo deve ser integrado a console de gerenciamento;
- 5.2 A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:
 - 5.2.1 Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)
- 5.3 A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:
 - 5.3.1.1 iOS 10–17 ou iPadOS 13–17
- 5.4 A solução proposta deve oferecer suporte a dispositivos Android Device Owner.
- 5.5 A solução proposta deve suportar dispositivos iOS supervisionados.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 5.6 A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.
- 5.7 A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.
- 5.8 A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.
- 5.9 A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).
- 5.10 A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.
- 5.11 A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.
- 5.12 A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.
- 5.13 A solução proposta deve ter recursos de containerização para dispositivos Android.
- 5.14 A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:
- 5.14.1 Dados em contêineres
 - 5.14.2 Contas de e-mail corporativo
 - 5.14.3 Configurações para conexão à rede Wi-Fi corporativa e VPN
 - 5.14.4 Nome do ponto de acesso (APN)
 - 5.14.5 Perfil do Android for Work
 - 5.14.6 Recipiente KNOX
 - 5.14.7 Chave do gerenciador de licença KNOX
- 5.15 A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:
- 5.15.1 Todos os perfis de configuração instalados
 - 5.15.2 Todos os perfis de provisionamento



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

5.15.3 O perfil iOS MDM

- 5.16 Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas
- 5.17 A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo .
- 5.18 A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controle de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:
- 5.18.1 Critérios de verificação do dispositivo;
- 5.18.2 Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;
- 5.19 A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.
- 5.20 A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:
- 5.20.1 Cartões de memória e outras unidades removíveis
- 5.20.2 Câmera do dispositivo
- 5.20.3 Conexões Wi-Fi
- 5.20.4 Conexões Bluetooth
- 5.20.5 Porta de conexão infravermelha
- 5.20.6 Ativação do ponto de acesso Wi-Fi
- 5.20.7 Conexão de área de trabalho remota
- 5.20.8 Sincronização de área de trabalho
- 5.20.9 Definir configurações da caixa de correio do Exchange
- 5.20.10 Configurar caixa de e-mail em dispositivos iOS MDM
- 5.20.11 Configure contêineres Samsung KNOX.
- 5.20.12 Definir as configurações do perfil do Android for Work



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 5.20.13 Configurar e-mail/calendário/contatos
- 5.20.14 Defina as configurações de restrição de conteúdo de mídia.
- 5.20.15 Definir configurações de proxy no dispositivo móvel
- 5.20.16 Configurar certificados e SCEP
- 5.21 A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay .
- 5.22 A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:
 - 5.22.1 Google Play, Huawei App Gallery e Apple App Store
 - 5.22.2 Portal de inscrição móvel KNOX
 - 5.22.3 Pacotes de instalação pré-configurados independentes
- 5.23 A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.
- 5.24 A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.
- 5.25 A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:
 - 5.25.1 VMware AirWatch 9.3 ou posterior
 - 5.25.2 MobileIron 10.0 ou posterior
 - 5.25.3 IBM MaaS360 10.68 ou posterior
 - 5.25.4 Microsoft Intune 1908 ou posterior
 - 5.25.5 SOTI MobiControl 14.1.4 (1693) ou posterior
- 5.26 A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.
- 5.27 A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:
 - 5.27.1 Google Play
 - 5.27.2 Galeria de aplicativos Huawei
 - 5.27.3 Loja de aplicativos da Apple



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 5.28 A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.
- 5.29 A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.
- 5.30 A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.
- 5.31 A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.
- 5.32 A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.
- 5.33 A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.
- 5.34 A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.
- 5.35 A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.
- 5.36 A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.
- 5.37 A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.
- 5.38 A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.
- 5.39 A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.
- 5.40 A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
- 5.41 A solução proposta deve proteger contra ameaças online em dispositivos iOS.

6 Do módulo de EDR

- 6.1 Deve apresentar um gráfico de propagação de ameaças com os principais processos, conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 6.2 Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
- 6.3 A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
- 6.4 Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
- 6.5 Deve apresentar informações detalhadas contendo:
 - 6.5.1 Usuário que executou a ação;
 - 6.5.2 Informações acesso privileged;
- 6.6 A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.
- 6.7 A solução proposta deve suportar integração com serviço de reputação em nuvem.
- 6.8 A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.)
- 6.9 O agente EDR deve ter integração com o aplicativo de proteção de endpoint (agente único).
- 6.10 Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas;
- 6.11 A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.
- 6.12 A solução proposta deve complementar as informações do veredicto da solução Endpoint Protection com artefatos do sistema sobre a detecção.
- 6.13 A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.
- 6.14 A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.
- 6.15 A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 6.16 A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.
- 6.17 A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.
- 6.18 A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.
- 6.19 A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.
- 6.20 A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:
- 6.20.1 Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).
 - 6.20.2 Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.
 - 6.20.3 Informações gerais sobre a detecção, incluindo modo de detecção.
 - 6.20.4 Alterações no registro associadas à detecção.
 - 6.20.5 Histórico da presença de arquivos no dispositivo.
 - 6.20.6 Ações de resposta executadas pela aplicação.
- 6.21 O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.
- 6.22 A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:
- 6.22.1 Processo
 - 6.22.2 Conexões de rede
 - 6.22.3 Alterações no registro
 - 6.22.4 Detalhes do download de objeto
- 6.23 A solução proposta deve fornecer orientação de resposta (resposta guiada).



ESTADO DO MARANHÃO
MINISTÉRIO PÚBLICO
PROCURADORIA GERAL DE JUSTIÇA
COORDENADORIA DE MODERNIZAÇÃO E TECNOLOGIA DA INFORMAÇÃO

- 6.24 A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente
- 6.25 A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:
 - 6.25.1 Impedir a execução de objetos
 - 6.25.2 Isolamento de host
 - 6.25.3 Excluir objeto do host ou grupo de hosts
 - 6.25.4 Encerrar um processo no dispositivo
 - 6.25.5 Colocar um objeto em quarentena
 - 6.25.6 Execute a verificação do sistema
 - 6.25.7 Execução remota de programa/processo/comando
- 6.26 Iniciar a varredura IoC para um grupo de hosts.