



INSTITUTO DE PROJETOS AVANÇADOS PARA CIDADES, TECNOLOGIA E ADMINISTRAÇÃO
Presidência do Conselho de Administração do INPACTA
Diretoria Executiva do INPACTA
Diretoria da Presidência do INPACTA
Diretoria Administrativa e Financeira do INPACTA
Gerência de Licitações e Contratos do INPACTA
Av. XV de Novembro, 701, 2º Andar do Paço Municipal - Bairro Centro, Maringá/PR,
CEP 87013-230 Telefone: - www.inpacta.org.br

ANEXO DE EDITAL

ANEXO I - ESPECIFICAÇÃO DO OBJETO SOLUÇÃO INTEGRADA PARA CIBERSEGURANÇA

1. OBJETO

1.1. O presente Anexo especifica a estruturação de parceria especializada para disponibilização, implantação, configuração, integração, operação assistida, suporte técnico, manutenção, licenciamento, sustentação e evolução de soluções integradas e continuadas de cibersegurança, no âmbito da **SOLUÇÃO INTEGRADA PARA CIBERSEGURANÇA**.

1.2. A solução deverá operar como ecossistema único, modular, escalável e interoperável, com responsabilidade técnica unificada da PARCEIRA pela compatibilidade entre plataformas, licenças, integrações, serviços, fluxos, dados, evidências, documentação, suporte, continuidade e resultados.

1.3. O objeto abrange:

Módulo 1 - segurança ofensiva autorizada, gestão de vulnerabilidades, hardening e SOC 24x7;

Módulo 2 - CTEM/BAS;

Módulo 3 - TPRM;

Módulo 4 - CTI; e

Módulo 5 - analistas cibernéticos digitais baseados em inteligência artificial.

1.4. A parceria e os instrumentos executivos de cada implementação poderão incluir implantação, parametrização, integrações autorizadas, operação assistida, suporte, treinamento, atualização, documentação, relatórios, transferência de conhecimento e transição, conforme o escopo efetivamente autorizado.

1.5. Nenhum módulo, licença, integração, serviço ou entrega poderá ser tratado isoladamente quando sua operação depender de outro componente do ecossistema.

1.6. Toda funcionalidade declarada deverá possuir documentação, forma objetiva de

comprovação, evidência técnica e possibilidade de validação prática, quando aplicável.

1.7. Testes, varreduras intrusivas, simulações e ações com potencial de impacto somente poderão ocorrer dentro do escopo, das regras de engajamento e das autorizações estabelecidas.

1.8. A parceria destina-se ao atendimento de diferentes clientes, dentro do objeto e do público autorizados, sem quantitativos prefixados de atendimento, licenciamento, consumo ou capacidade volumétrica nos instrumentos gerais. As quantidades efetivas, as unidades de licenciamento, os recursos, a abrangência, a medição e o aceite serão definidos no instrumento executivo de cada cliente, com base em diagnóstico e nas aprovações aplicáveis, antes da execução. Não há garantia de consumo, mobilização automática ou promessa de fornecimento ilimitado.

1.8.1. Os requisitos RF-E-009, RF-E-015, RF-E-029 e RF-E-030 exigem demonstração das funcionalidades correspondentes e da metodologia de dimensionamento por cliente, sem limites volumétricos prefixados. A proponente apresentará métricas e dependências de licenciamento, mecanismos de expansão, segregação e gestão. Os testes seguirão cenários controlados previamente definidos e não importarão a carga de produção de cliente-modelo. A revisão dos requisitos e sua forma de comprovação dependem de validação antes da publicação.

2. DEFINIÇÕES OPERACIONAIS

2.1. Solução Integrada para CIBERSEGURANÇA: conjunto integrado de plataformas, serviços, processos, pessoas e controles destinado à prevenção, identificação, monitoramento, análise, validação e mitigação de riscos cibernéticos.

2.2. Ecossistema integrado de cibersegurança: conjunto formado pelos cinco módulos, licenças, integrações, APIs, serviços técnicos, documentação, suporte e entregáveis.

2.3. Ativo monitorado: domínio, subdomínio, endereço IP, aplicação, API, sistema, serviço, recurso em nuvem, endpoint, identidade ou outro elemento incluído no inventário e no escopo aprovado.

2.4. Evento de segurança: ocorrência observável com possível relevância para a segurança.

2.5. Alerta de segurança: evento ou conjunto de eventos selecionado para triagem por regra, correlação, comportamento, indicador ou contexto de risco.

2.6. Incidente de segurança: ocorrência confirmada ou provável capaz de comprometer confidencialidade, integridade, disponibilidade, autenticidade ou continuidade.

- 2.7. Vulnerabilidade: fragilidade técnica, operacional ou de configuração que possa ser explorada ou contribuir para a materialização de risco.
- 2.8. Achado de segurança: resultado de varredura, pentest, CTEM, BAS, CTI, SOC, TPRM ou analista digital, acompanhado das evidências disponíveis.
- 2.9. Evidência técnica: registro verificável que sustente alerta, achado, vulnerabilidade, incidente ou conclusão técnica.
- 2.10. IOC: artefato técnico associado a atividade maliciosa ou potencial comprometimento.
- 2.11. TTPs: padrões de comportamento utilizados por agentes de ameaça em operações cibernéticas.
- 2.12. Terceiro monitorado: fornecedor, prestador, parceiro ou organização cuja exposição possa representar risco à InPACTA.
- 2.13. Ordem de Serviço: instrumento de acionamento, autorização e acompanhamento de atividade ou entrega específica.
- 2.14. Operação assistida: etapa posterior à implantação destinada à estabilização, correção de falhas e apoio aos usuários.
- 2.15. PoC: procedimento objetivo de demonstração, teste e validação técnica, com roteiro, critérios, evidências e resultados registrados.
- 2.16. Hardening: processo de configuração segura de ativos de TI para reduzir vulnerabilidades e minimizar a superfície de ataque.
- 2.17. CVE: identificador único de vulnerabilidades de segurança conhecidas, utilizado para padronizar sua identificação e referência.
- 2.18. CVSS (Common Vulnerability Scoring System): sistema padronizado de classificação da severidade de vulnerabilidades, utilizado para priorizar as ações de tratamento com base em uma pontuação de 0,0 a 10,0.

3. COMPOSIÇÃO MÍNIMA DA SOLUÇÃO

- 3.1. A solução será composta pelos cinco módulos previstos no objeto, disponibilizados de forma integrada e com todos os recursos necessários ao funcionamento durante a vigência.
- 3.2. A camada de gestão deverá contemplar, conforme aplicável, dashboards, inventários, usuários, perfis, alertas, casos, evidências, relatórios, auditoria, integrações, exportações e acompanhamento de SLA.
- 3.3. Os serviços associados compreenderão planejamento, implantação, configuração, integração, testes, operação assistida, suporte, manutenção, atualização, treinamento, documentação e transição.
- 3.4. A governança deverá estabelecer pontos focais, matriz de responsabilidades,

canais de comunicação, reuniões, gestão de pendências e escalonamento.

3.5. A arquitetura deverá permitir evolução tecnológica sem redução das capacidades, coberturas, integrações ou níveis de serviço contratados.

4. MÓDULO 1 – SEGURANÇA OFENSIVA, GESTÃO DE VULNERABILIDADES, HARDENING E SOC 24X7

4.1. MODELO DE PRESTAÇÃO DOS SERVIÇOS

4.1.1. Os serviços serão prestados de forma contínua, sendo o monitoramento de segurança por SOC realizado em regime 24x7x365. As atividades de gestão de vulnerabilidades, recomendações de hardening e testes de intrusão autorizados serão organizadas em ciclos mensais, observados o plano de trabalho, o escopo técnico e as regras de engajamento previamente aprovadas pela InPACTA. Cada ciclo deverá contemplar, obrigatoriamente, a entrega dos produtos previstos nos itens subsequentes, sem prejuízo da comunicação imediata de vulnerabilidades críticas, indícios de exploração ativa, incidentes ou riscos que demandem tratamento urgente.

4.1.2. Cada ciclo de prestação dos serviços deverá resultar, no mínimo, na emissão dos relatórios e na entrega dos produtos previstos nos subitens seguintes, sem prejuízo da emissão de alertas, comunicações emergenciais e relatórios extraordinários quando identificados riscos críticos ou incidentes relevantes.

4.1.2.1. Relatório de identificação e validação de vulnerabilidades, contendo, no mínimo:

- a) ativo, sistema, aplicação, serviço ou componente afetado;
- b) descrição técnica da vulnerabilidade, exposição ou configuração insegura identificada;
- c) classificação de severidade, com indicação da metodologia utilizada;
- d) referências técnicas e identificadores reconhecidos, tais como CVE e CVSS, quando existentes e aplicáveis;
- e) evidências técnicas suficientes para demonstrar a existência do achado, observados os requisitos de sigilo e segurança;
- f) análise de explorabilidade, quando tecnicamente possível e autorizada pela InPACTA;
- g) data da identificação, situação atual e indicação de eventual reincidência;
- h) recomendação preliminar de correção, mitigação ou adoção de controle compensatório.

4.1.2.2. Relatório de avaliação de impacto e risco, contendo análise contextualizada das vulnerabilidades, exposições e demais achados identificados, considerando, no

mínimo:

- a) severidade técnica;
- b) probabilidade, facilidade e possibilidade de exploração;
- c) existência de código público de exploração, exploração ativa conhecida ou outros indícios relevantes de ameaça, quando disponíveis;
- d) grau de exposição do ativo, especialmente quando acessível pela internet;
- e) criticidade do ativo, sistema, serviço ou processo de negócio afetado;
- f) impacto potencial sobre a confidencialidade, a integridade, a disponibilidade, a autenticidade e a continuidade dos serviços públicos;
- g) natureza e sensibilidade dos dados potencialmente envolvidos, inclusive dados pessoais, quando aplicável;
- h) existência, cobertura e efetividade dos controles compensatórios; e
- i) priorização das medidas de tratamento, com indicação da ação recomendada, da prioridade, do prazo sugerido e do risco residual estimado.

4.1.2.3. Relatório de acompanhamento do tratamento das vulnerabilidades, contendo as informações e providências descritas no respectivo subitem.

- a) situação de cada vulnerabilidade, classificada como aberta, em tratamento, mitigada, corrigida, aceita formalmente pela InPACTA, reaberta ou encerrada;
- b) unidade ou responsável indicado pela InPACTA para o tratamento, quando informado;
- c) prazo recomendado e prazo acordado para remediação, quando definido;
- d) registro das medidas de correção ou mitigação adotadas;
- e) resultado da reavaliação, do reteste ou da validação técnica realizada;
- f) validação da eficácia das correções ou dos controles compensatórios implementados;
- g) identificação de vulnerabilidades reincidentes, pendentes ou não solucionadas; e
- h) atualização do risco residual e do perfil consolidado de risco da InPACTA.

4.1.2.4. A PARCEIRA deverá disponibilizar painel de acompanhamento das vulnerabilidades e exposições identificadas, com acesso aos usuários autorizados pela InPACTA, permitindo, no mínimo, consulta, filtragem, acompanhamento de histórico e exportação das informações por secretaria, unidade administrativa, ativo, sistema, criticidade, situação, responsável indicado, prazo recomendado e prazo acordado para tratamento, quando definido.

4.1.3. As evidências técnicas e os testes de validação não deverão provocar indisponibilidade, degradação relevante de desempenho, alteração indevida de dados ou qualquer impacto não autorizado no ambiente da InPACTA. A exploração controlada de vulnerabilidades somente poderá ocorrer nos limites previamente autorizados e de acordo com as regras de engajamento estabelecidas.

4.1.4. Os relatórios poderão ser apresentados de forma consolidada, desde que contemplem integralmente os conteúdos mínimos previstos neste item e permitam a rastreabilidade de cada vulnerabilidade durante todo o seu ciclo de vida.

4.2. TESTES DE INTRUSÃO (PENTEST)

4.2.1. Os testes de intrusão deverão ser realizados em ciclos mensais, abrangendo os ativos, sistemas, aplicações, serviços e interfaces definidos pela InPACTA e previstos no plano de trabalho de cada ciclo. Os testes deverão adotar abordagem orientada ao risco e ao impacto no ambiente, observados o escopo autorizado, as regras de engajamento, os horários permitidos e os limites técnicos previamente estabelecidos. A exploração controlada de vulnerabilidades somente poderá ocorrer quando expressamente autorizada pela InPACTA. A cada ciclo, deverão ser entregues os relatórios previstos nos itens subsequentes.

4.2.2. Relatório de identificação da superfície de ataque, contendo o mapeamento dos vetores e pontos de entrada identificados nos ativos avaliados, incluindo, quando aplicável, domínios, subdomínios, endereços IP, aplicações, APIs, serviços expostos, tecnologias identificadas, configurações relevantes e potenciais caminhos de ataque.

4.2.3. Relatório de validação de vulnerabilidades exploráveis, contendo documentação técnica das vulnerabilidades cuja explorabilidade tenha sido confirmada no ambiente da InPACTA, quando a validação tiver sido autorizada, incluindo, no mínimo, evidências técnicas, condições necessárias à reprodução controlada, classificação de severidade, referências a identificadores e metodologias reconhecidos, tais como CVE e CVSS, impacto técnico demonstrado, ativos afetados, nível de acesso ou privilégio obtido, quando aplicável, e recomendações de correção ou mitigação.

4.2.4. Relatório de avaliação do impacto no ambiente, contendo análise do impacto potencial das vulnerabilidades exploradas ou confirmadas como exploráveis, considerando a criticidade dos sistemas afetados, os dados potencialmente expostos, a possibilidade de elevação de privilégios ou movimentação lateral, os impactos sobre a confidencialidade, a integridade, a disponibilidade e a continuidade dos serviços públicos, bem como os possíveis desdobramentos operacionais, financeiros, legais e reputacionais.

4.3. GESTÃO DE VULNERABILIDADES

4.3.1. A PARCEIRA deverá realizar a gestão contínua de vulnerabilidades nos ativos, sistemas, aplicações, serviços e interfaces definidos no escopo da contratação, contemplando identificação, validação, classificação, priorização, recomendação de

tratamento, acompanhamento e reteste das vulnerabilidades e exposições identificadas.

4.3.2. A PARCEIRA deverá realizar varreduras recorrentes de vulnerabilidades, com periodicidade mínima mensal, abrangendo os ativos, sistemas, aplicações, serviços e interfaces, internos ou expostos, definidos pela InPACTA, inclusive varreduras autenticadas, quando aplicáveis e desde que disponibilizados os acessos necessários.

4.3.3. A PARCEIRA deverá realizar varreduras extraordinárias sempre que houver incidente relevante, divulgação de vulnerabilidade crítica, indício de exploração ativa, alteração significativa no ambiente tecnológico ou solicitação justificada da InPACTA, observado o seguinte prazo máximo para início da atividade, contado do registro da ocorrência ou da solicitação:

- a) em até 4 (quatro) horas, para ocorrências críticas;
- b) em até 1 (um) dia útil, para ocorrências altas;
- c) em até 3 (três) dias úteis, para ocorrências médias; e
- d) conforme programação acordada com a InPACTA, para ocorrências baixas.

4.3.3.1. A realização de varreduras que exijam acesso, autorização específica, janela de manutenção ou providência da InPACTA deverá observar tais condições, sem prejuízo da comunicação imediata, da orientação técnica e da adoção de medidas de análise compatíveis.

4.3.4. A PARCEIRA deverá efetuar a validação técnica dos achados identificados nas varreduras, confirmando, quando tecnicamente possível e autorizado, sua existência, relevância e potencial de exploração no contexto do ambiente da InPACTA.

4.3.5. A PARCEIRA deverá identificar, classificar e registrar falsos positivos, duplicidades e achados sem impacto relevante, de modo que os relatórios priorizem vulnerabilidades efetivamente verificadas e reduzam esforços desnecessários das equipes técnicas da InPACTA.

4.3.6. A PARCEIRA deverá priorizar as vulnerabilidades identificadas com base em análise de risco contextualizada, considerando, no mínimo, a criticidade do ativo afetado, a exposição à internet, a facilidade de exploração, a existência de código público de exploração, indícios de exploração ativa ou informações de inteligência de ameaças relevantes, o impacto potencial, a sensibilidade dos dados envolvidos, o risco de interrupção dos serviços públicos e o contexto operacional da InPACTA.

4.3.7. A PARCEIRA deverá classificar as vulnerabilidades por níveis de severidade - crítico, alto, médio, baixo e informativo - utilizando metodologias reconhecidas de mercado, tais como CVSS, complementadas pela avaliação de risco contextualizada do ambiente.

4.3.8. Os relatórios técnicos relacionados à gestão de vulnerabilidades deverão

observar os conteúdos mínimos, os critérios de priorização e os requisitos de rastreabilidade previstos no item 4.1.2 e respectivos subitens deste instrumento.

4.3.9. A PARCEIRA deverá acompanhar a evolução do tratamento das vulnerabilidades priorizadas, mediante atualização de status, recomendação de providências, validação de correções implementadas pela InPACTA e identificação de vulnerabilidades reincidentes ou pendentes.

4.4. REVISÃO DE HARDENING

4.4.1. Avaliar as configurações de segurança dos sistemas, dispositivos, aplicações e demais ativos em escopo, identificando desvios em relação a boas práticas e padrões reconhecidos de hardening.

4.4.2. Fornecer recomendações práticas de configurações seguras, considerando as restrições técnicas, funcionais e operacionais de cada ambiente da InPACTA, com indicação, quando aplicável, do impacto esperado, das dependências técnicas, dos pré-requisitos de implementação e das medidas de mitigação ou reversão recomendadas.

4.4.3. Priorizar as recomendações de hardening com base no risco associado a cada desvio identificado, considerando a criticidade do ativo, sua exposição, o impacto potencial, a existência de indícios de exploração ativa ou de ameaças relevantes e a viabilidade de implementação no ambiente da InPACTA, orientando a equipe técnica sobre as ações de maior impacto na redução da superfície de ataque.

4.4.4. Apresentar relatório técnico contendo os desvios identificados, o risco associado, as recomendações de correção ou mitigação e a respectiva prioridade de tratamento.

4.5. RETESTES E VALIDAÇÃO DE CORREÇÕES

4.5.1. Realizar retestes direcionados após a implementação de correções pela InPACTA, verificando se as vulnerabilidades apontadas foram efetivamente remediadas.

4.5.2. Validar a efetividade das medidas adotadas, confirmando que as correções implementadas mitigam ou eliminam o risco identificado, sem introduzir novas exposições relevantes.

4.5.3. Atualizar o status de risco de cada vulnerabilidade com base nos resultados dos retestes, mantendo histórico atualizado da evolução do perfil de segurança do ambiente.

4.6. SOC 24X7 – CENTRO DE OPERAÇÕES DE SEGURANÇA

4.6.1. A PARCEIRA deverá realizar o monitoramento contínuo dos serviços da InPACTA, em regime 24x7x365, a partir de logs, alertas e telemetrias gerados por soluções de segurança, infraestrutura, aplicações, identidades, serviços em nuvem e demais fontes de dados integradas ao escopo contratado.

4.6.2. A PARCEIRA deverá acompanhar a disponibilidade, a integridade e a continuidade da coleta de logs, alertas e telemetrias das fontes integradas, comunicando à InPACTA eventuais falhas, lacunas ou degradações que possam comprometer o monitoramento.

4.6.3. A PARCEIRA deverá realizar a triagem, a correlação, o enriquecimento e a classificação dos alertas e incidentes identificados, diferenciando eventos relevantes de ruídos operacionais e priorizando o atendimento conforme a severidade, a criticidade dos ativos afetados, o impacto potencial, as evidências disponíveis e as informações de inteligência de ameaças pertinentes.

4.6.4. A PARCEIRA deverá registrar e documentar os eventos de segurança monitorados e processados no escopo contratado, incluindo alertas, incidentes, achados, evidências e ações realizadas, com data, origem, ativo, severidade, responsável e status, mantendo trilha de auditoria íntegra, consultável e exportável, observada a política de retenção aplicável.

4.6.5. A PARCEIRA deverá emitir alertas e notificações conforme a criticidade da ocorrência e os níveis de serviço definidos no contrato, comunicando imediatamente a InPACTA sobre incidentes críticos e fornecendo orientações iniciais de contenção, mitigação ou investigação.

4.6.5.1. Para incidente crítico, a PARCEIRA deverá iniciar a triagem e a investigação técnica em até 2 (duas) horas, em regime 24x7x365, comunicar o ponto focal da InPACTA, preservar logs, evidências e indicadores e emitir relatório técnico preliminar em até 24 (vinte e quatro) horas, contendo, quando aplicável, escopo, ativos afetados, linha do tempo, indícios, IOCs, impacto e recomendações. A PARCEIRA deverá apoiar tecnicamente eventual apuração pelas autoridades competentes, sem garantia de identificação, localização, prisão ou responsabilização do agente malicioso.

4.6.6. A PARCEIRA deverá realizar análise técnica dos incidentes relevantes, incluindo, quando aplicável, investigação inicial, correlação de evidências, identificação de ativos afetados, análise de possível causa, impacto, risco e recomendações de providências.

4.6.7. As ações de bloqueio, isolamento, alteração de configuração, remoção de artefatos ou qualquer outra intervenção ativa no ambiente da InPACTA dependerão de autorização prévia, ressalvadas as medidas expressamente autorizadas em procedimento previamente aprovado.

4.6.8. A PARCEIRA deverá promover o escalonamento técnico e gerencial das ocorrências quando necessário, mantendo a InPACTA informada sobre a evolução, as medidas recomendadas, as pendências e as condições para encerramento.

4.6.9. A PARCEIRA deverá revisar e aperfeiçoar continuamente os casos de uso, regras de correlação, parâmetros de alerta e mecanismos de redução de falsos positivos, considerando os incidentes identificados, as mudanças no ambiente e as informações de inteligência de ameaças.

4.6.10. Os resultados das atividades do SOC deverão subsidiar os relatórios, indicadores, reuniões de governança e recomendações técnicas previstos neste Anexo.

4.7. DIMENSIONAMENTO POR CLIENTE E ENTREGÁVEIS

4.7.1. Os serviços observarão as frequências e os parâmetros mínimos indicados na tabela, sem prejuízo de acionamentos extraordinários por risco crítico ou incidente relevante.

4.7.2. O monitoramento abrangerá os ativos tecnológicos internos definidos no diagnóstico e no instrumento executivo de cada cliente, sem volume prefixado para a parceria. O escopo efetivo poderá abranger estações de trabalho, notebooks, servidores físicos e virtuais, equipamentos de rede e segurança, dispositivos institucionais, ativos em nuvem, aplicações, bancos de dados e demais componentes autorizados. A metodologia de dimensionamento indicará unidades de licenciamento, recursos, dependências e mecanismos de expansão.

4.7.3. Para fins de licenciamento e aferição da capacidade, cada ativo deverá ser contabilizado de forma única, evitando-se dupla contagem decorrente de múltiplos endereços IP, eventos, agentes, telemetrias ou fontes de log associados ao mesmo equipamento, sistema ou componente tecnológico.

4.7.4. O inventário real, a unidade de contabilização, o tratamento de duplicidades e a métrica de licenciamento serão definidos no levantamento de cada implementação e formalizados no respectivo instrumento executivo antes do início da obrigação operacional.

ITEM	FREQUÊNCIA MÍNIMA	PARÂMETRO DE ENTREGA
Gestão de vulnerabilidades	Mensal	Execução de ciclo de identificação, priorização, recomendação de tratamento e acompanhamento das vulnerabilidades no escopo definido pela InPACTA.

ITEM	FREQUÊNCIA MÍNIMA	PARÂMETRO DE ENTREGA
Testes de intrusão autorizados	Mensal	Realização de testes orientados ao risco, observados o escopo, as regras de engajamento e as autorizações previamente estabelecidas.
Recomendações de hardening	Mensal	Emissão de recomendações de fortalecimento de configuração e acompanhamento das medidas adotadas pela InPACTA.
SOC e monitoramento de segurança	Contínuo, em regime 24x7x365	Monitoramento, triagem, correlação, registro e comunicação de eventos, alertas e incidentes de segurança.
Relatório formal do SOC	Mensal	Consolidação dos eventos relevantes, alertas, incidentes, indicadores, recomendações e status das ações de tratamento.
Reteste e validação de correções	Sob demanda, observado o mínimo bimestral	Realização após comunicação de remediação pela InPACTA, conforme criticidade, disponibilidade do ambiente e regras de engajamento.

5. MÓDULO 2 – GESTÃO CONTÍNUA DA EXPOSIÇÃO A AMEAÇAS E SIMULAÇÃO DE VIOLAÇÃO E ATAQUE (CTEM/BAS)

5.1 DESCOBERTA E GESTÃO DE SUPERFÍCIE DE ATAQUE (CTEM)

5.1.1. A plataforma deverá realizar descoberta passiva, contínua e baseada em fontes abertas de inteligência — OSINT — para mapear a superfície digital externa da InPACTA a partir de domínios e endereços IP informados ou identificados pela própria solução. A descoberta deverá identificar, correlacionar e apresentar, no mínimo, domínios, subdomínios, endereços IPv4 públicos, portas, serviços expostos, tecnologias identificadas e conexões técnicas relevantes entre os ativos descobertos.

5.1.2. A plataforma deverá identificar e listar domínios relacionados à InPACTA a partir de seu nome institucional, domínios de referência ou outros indicadores técnicos, apresentando as evidências de relacionamento identificadas. Cada domínio relacionado deverá ser registrado como ativo descoberto e poderá ser associado a um alvo de monitoramento e análise de seus respectivos subdomínios, endereços IP,

portas, serviços e demais atributos técnicos identificados.

5.1.3. A plataforma deverá identificar subdomínios vinculados aos domínios monitorados e correlacioná-los aos respectivos endereços IP, portas, serviços expostos e demais informações técnicas disponíveis. Os ativos descobertos deverão poder ser classificados, validados, associados a alvos de monitoramento e submetidos às verificações previstas no escopo contratado.

5.1.4. A plataforma deverá classificar os ativos descobertos em categorias e apresentar, para cada ativo, as informações técnicas e de contexto disponíveis, incluindo endereços IP associados, portas detectadas, serviços, tecnologias, dados provenientes de fontes OSINT e relacionamentos identificados, permitindo a organização e a priorização estruturada da superfície de ataque.

5.1.5. A plataforma deverá permitir a seleção e a associação dos ativos descobertos a alvos de monitoramento contínuo, submetendo-os, conforme o nível e o cronograma de varredura configurados, a mecanismos de detecção de serviços expostos, tecnologias desatualizadas, vulnerabilidades conhecidas, configurações inseguras e demais atributos relevantes à avaliação da superfície externa de ataque.

5.1.6. A plataforma deverá identificar domínios e ativos potencialmente relacionados à InPACTA por meio da correspondência de favicons, permitindo a descoberta de infraestruturas associadas que utilizem elementos visuais idênticos ou tecnicamente correlacionados aos ativos monitorados.

5.1.7. A plataforma deverá reprocessar recursivamente os resultados da descoberta para identificar domínios relacionados, dependências técnicas, integrações de terceiros e novos ativos associados à superfície de ataque da InPACTA. O mecanismo de descoberta deverá utilizar, no mínimo, correlações baseadas em registros WHOIS, certificados SSL/TLS, redirecionamentos, links e backlinks, domínios hospedados conjuntamente, análise de código-fonte HTML, descoberta de buckets, resolução de registros CNAME e A, pesquisas reversas de certificados, descoberta de subdomínios e varredura passiva de portas.

5.1.8. A plataforma deverá realizar correlação cruzada das descobertas em nível de ativo, consolidando, em uma única visão, os domínios relacionados, subdomínios, endereços IP, portas, certificados SSL/TLS, dados WHOIS, tecnologias identificadas, serviços expostos, indicadores de inteligência de ameaças e demais metadados coletados. A solução deverá apresentar os relacionamentos técnicos entre tais elementos, permitindo a análise contextualizada de cada ativo e de sua posição na superfície externa de ataque.

5.1.9. A plataforma deverá permitir a criação de alvos de monitoramento a partir de nomes de domínio plenamente qualificados — FQDNs — e endereços IPv4 públicos atribuídos ou formalmente autorizados pela InPACTA. Para os ativos associados aos

alvos, a solução deverá permitir a execução de verificações e varreduras ativas controladas, destinadas à identificação de serviços expostos, tecnologias desatualizadas, vulnerabilidades conhecidas, configurações inseguras e outros atributos relevantes à avaliação da exposição externa.

5.1.10. A plataforma deverá permitir a configuração individualizada, por alvo de monitoramento, da intensidade das verificações e de sua periodicidade de execução. Deverá disponibilizar diferentes níveis de varredura e permitir a definição de cronogramas recorrentes, inclusive com ciclos diários, conforme a criticidade do ativo e a necessidade operacional da InPACTA.

5.1.11. A plataforma deverá identificar vulnerabilidades potencialmente exploráveis e ativos corporativos expostos ou indevidamente divulgados na superfície externa de ataque, permitindo a priorização de vetores de violação e a adoção preventiva de medidas de tratamento antes de sua exploração por agentes maliciosos.

5.2 SIMULAÇÃO DE VIOLAÇÃO E ATAQUE (BAS)

5.2.1. Para cada vetor de ataque, vulnerabilidade ou tecnologia desatualizada identificada, a plataforma deverá apresentar recomendações de remediação associadas ao respectivo achado, permitindo o acompanhamento individual das etapas de tratamento e a atualização de seu status após a correção.

5.2.2. A plataforma deverá permitir a emulação controlada de vetores de ataque identificados nos ativos-alvo, para validação técnica das fraquezas encontradas e verificação da efetividade dos controles de segurança, observados os ativos autorizados, os limites de escopo e as regras de engajamento definidas pela InPACTA.

5.2.3. A plataforma deverá executar validações de explorabilidade mediante mecanismos dinâmicos e não invasivos, capazes de simular o comportamento de um potencial atacante sem provocar impacto indevido no ambiente. Para cada vetor validado, deverá disponibilizar evidências técnicas suficientes, incluindo ativo, endereço IP, porta, detalhes da prova de conceito e registros de requisição e resposta, quando aplicáveis.

5.2.4. A plataforma deverá monitorar continuamente os ativos e atualizar automaticamente a situação dos vetores identificados. Quando um vetor deixar de ser válido em razão de correção, mitigação ou atualização tecnológica, a respectiva ação de tratamento deverá ser registrada como concluída; caso novos vetores sejam identificados, o ativo deverá voltar a ser sinalizado como exposto.

5.2.5. Para os vetores cuja validação comportar prova de conceito, a plataforma deverá disponibilizar os elementos técnicos necessários à reprodução controlada, incluindo, quando aplicáveis, método HTTP, caminho ou recurso vulnerável,

parâmetro afetado, demonstração de exploração, bem como registros de requisição e resposta utilizados na validação.

5.2.6. A plataforma deverá executar monitoramento contínuo dos ativos selecionados para verificar a permanência das correções implementadas, identificar regressões, novas exposições ou reaparecimento de vetores anteriormente tratados e atualizar o status de remediação de forma automática.

5.2.7. A plataforma deverá permitir o registro de comentários, observações e atualizações pelos usuários autorizados em cada vetor ou achado identificado, mantendo histórico das interações para apoio à colaboração, à investigação e ao acompanhamento das medidas de tratamento.

5.2.8. A plataforma deverá permitir a geração e a exportação de relatórios personalizados sobre a superfície de ataque, os ativos descobertos, os vetores identificados, as vulnerabilidades validadas e as ações de remediação, em formato eletrônico amplamente utilizado e adequado ao compartilhamento com públicos técnicos e gerenciais.

5.2.9. A plataforma deverá disponibilizar painéis de acompanhamento por alvo de monitoramento, apresentando visão consolidada dos ativos, vetores de ataque, descobertas de superfície externa, vulnerabilidades e respectiva evolução de tratamento.

5.2.10. A plataforma deverá disponibilizar mecanismo de notificação para comunicação da identificação de novos vetores, vulnerabilidades ou exposições relevantes nos ativos monitorados, contendo informações suficientes para sua classificação, priorização e encaminhamento às equipes responsáveis.

5.2.11. A plataforma deverá disponibilizar perfis distintos de acesso, com permissões compatíveis com as atribuições de administração, operação, consulta e acompanhamento, permitindo a segregação de funções e o controle das ações executadas pelos usuários autorizados.

5.2.12. A plataforma deverá permitir a organização dos ativos, alvos e descobertas por secretaria, unidade administrativa, sistema, equipe responsável ou outro critério definido pela InPACTA, possibilitando a gestão segmentada da superfície de ataque e a atribuição de responsabilidades de tratamento.

5.2.13. A plataforma deverá permitir a integração dos achados relevantes aos fluxos de gestão de vulnerabilidades, incidentes ou service desk da InPACTA, mediante abertura ou atualização de chamados, quando tecnicamente viável e previsto no escopo de integração.

5.3. RELATÓRIOS E GESTÃO OPERACIONAL

5.3.1. As funcionalidades de relatórios, painéis, notificações, perfis de acesso,

organização das informações e integração com service desk estão previstas nos itens 5.2.8 a 5.2.13 e deverão ser mantidas disponíveis durante toda a execução dos serviços.

5.3.2. A PARCEIRA deverá consolidar, em cada ciclo de prestação, os resultados do monitoramento, as exposições identificadas, as providências recomendadas, o status de tratamento e os principais indicadores operacionais, para acompanhamento técnico e gerencial da InPACTA.

5.3.3. A PARCEIRA deverá manter atualizados os registros, painéis, notificações e chamados relacionados aos achados, assegurando a rastreabilidade das ações, dos responsáveis, dos prazos e das validações realizadas.

5.4 REQUISITOS DE IMPLANTAÇÃO E INFRAESTRUTURA

5.4.1. Garantir compatibilidade com os ambientes tecnológicos do InPACTA, com documentação técnica detalhada de requisitos de implantação para cada modalidade.

5.4.2. Assegurar que a opção on-premise não comprometa as capacidades funcionais da solução em relação à versão cloud.

5.5. DIMENSIONAMENTO POR CLIENTE

5.5.1. A solução deverá permitir a descoberta automatizada, o inventário dinâmico, o monitoramento contínuo e a avaliação da exposição cibernética dos ativos externos incluídos no escopo autorizado de cada cliente, compreendendo domínios, subdomínios, endereços IP públicos, aplicações, serviços expostos, interfaces, APIs, certificados digitais, ativos em nuvem e outros recursos da superfície de ataque externa. A metodologia deverá explicitar a unidade de contabilização, o licenciamento, as dependências e os mecanismos de expansão, sem volume prefixado para a parceria.

6. MÓDULO 3 – GERENCIAMENTO DE RISCO CIBERNÉTICO DE TERCEIROS (TPRM)

A plataforma deverá ser do tipo SaaS, com interface web e API RESTful.

6.1 GERENCIAMENTO DE RISCO CIBERNÉTICO DE TERCEIROS

6.1.1. A plataforma deverá realizar descoberta automática de ativos digitais relacionados aos fornecedores e parceiros monitorados, identificando domínios, subdomínios e endereços IP associados. Para tanto, deverá utilizar, entre outros mecanismos de correlação, dados de certificados SSL/TLS, registros WHOIS, fontes

externas de inteligência e recursos próprios de descoberta.

6.1.2. A plataforma deverá consolidar, para cada terceiro monitorado, informações de risco provenientes de fontes de cibercrime, dark web e deep web, gestão de superfície de ataque, inteligência técnica e avaliações de exposição ou configuração, permitindo análise integrada da postura cibernética do fornecedor.

6.1.3. A plataforma deverá disponibilizar visão consolidada do portfólio de fornecedores e parceiros cadastrados, permitindo acompanhar, ao longo do tempo, a evolução da postura de segurança, as tendências de risco e a distribuição dos terceiros por faixa de risco, criticidade, setor ou outros critérios definidos pela InPACTA.

6.1.4. A plataforma deverá monitorar a exposição de credenciais, contas comprometidas e acessos iniciais relacionados aos domínios e ativos dos terceiros cadastrados, incluindo dados oriundos de fontes de cibercrime, infecções por infostealers, fóruns clandestinos e anúncios de acessos corporativos comercializados ilicitamente.

6.1.5. A plataforma deverá monitorar a superfície externa de ataque dos terceiros avaliados, identificando portas abertas, serviços expostos, tecnologias desatualizadas, vulnerabilidades conhecidas, falhas de configuração, exposição indevida de chaves SSH ou chaves de API e problemas de segurança de e-mail que possam facilitar phishing, roubo de dados ou distribuição de malware.

6.1.6. A plataforma deverá gerar relatórios detalhados de risco cibernético, incluindo relatório de portfólio, com visão evolutiva dos riscos do conjunto de terceiros monitorados, e relatório individual por fornecedor, destacando as principais exposições, evidências disponíveis, classificação de risco e recomendações de tratamento.

6.1.7. A plataforma deverá permitir o cadastro e o início célere da avaliação de risco de múltiplos fornecedores em paralelo, viabilizando a inclusão em escala de terceiros no processo de monitoramento e gerenciamento de risco cibernético.

6.2 COMPLIANCE

6.2.1. A plataforma deverá permitir o envio de questionários de segurança e conformidade aos fornecedores e parceiros cadastrados, com acompanhamento centralizado das respostas, pendências, prazos e evolução da postura de segurança de cada terceiro ao longo do tempo.

6.2.2. A plataforma deverá permitir a personalização dos questionários conforme o perfil, a criticidade, o tipo de serviço contratado e o nível de risco de cada fornecedor, inclusive mediante utilização de questionários próprios definidos pela InPACTA.

6.2.3. A plataforma deverá avaliar as respostas dos fornecedores em relação a

requisitos regulatórios, normas, padrões de segurança e critérios de conformidade definidos pela InPACTA, incluindo, quando aplicáveis, referências como NIS2, DORA, HIPAA ou outros referenciais setoriais.

6.2.4. A plataforma deverá consolidar os resultados dos questionários em painéis e relatórios de conformidade, permitindo visualizar o nível de aderência de cada terceiro, as respostas pendentes, as lacunas identificadas e a severidade dos riscos associados, com preservação das evidências e da trilha de auditoria.

6.2.5. A plataforma deverá permitir a correlação dos resultados de conformidade e das respostas aos questionários com a avaliação de risco cibernético do respectivo fornecedor, apoiando a priorização de medidas de tratamento e o acompanhamento da evolução de sua postura de segurança.

6.3 EXPOSIÇÃO DE AMEAÇAS

6.3.1. A plataforma deverá monitorar continuamente credenciais vazadas, contas comprometidas e indícios de acessos indevidos associados aos domínios, ativos e identidades dos fornecedores cadastrados.

6.3.2. A plataforma deverá emitir alertas quando identificar credenciais, contas comprometidas, acessos corporativos anunciados para venda ou outros indícios relevantes de exposição relacionados aos terceiros monitorados.

6.3.3. Para cada alerta de exposição, a plataforma deverá disponibilizar o contexto técnico disponível, incluindo a fonte de identificação, a data ou período associado ao achado, o tipo de informação exposta, os domínios ou ativos relacionados e outros elementos que apoiem a avaliação do risco.

6.3.4. A plataforma deverá permitir a priorização dos alertas e das recomendações de tratamento conforme a criticidade do fornecedor, a natureza do serviço prestado, a sensibilidade dos dados potencialmente envolvidos e o risco de impacto sobre a continuidade dos serviços da InPACTA.

6.4 SUPERFÍCIE DE MONITORAMENTO DA SUPERFÍCIE DE ATAQUE DE TERCEIRO

6.4.1. A plataforma deverá identificar e monitorar, nos ativos externos atribuíveis aos terceiros cadastrados, portas abertas, serviços acessíveis pela internet, tecnologias desatualizadas, vulnerabilidades conhecidas e configurações inseguras que possam representar risco à cadeia de fornecimento.

6.4.2. A plataforma deverá identificar riscos de segurança de e-mail nos domínios dos terceiros, incluindo falhas de configuração de SPF, DKIM e DMARC, quando aplicáveis, bem como outras exposições que possam facilitar phishing, roubo de

dados ou distribuição de malware.

6.4.3. A plataforma deverá detectar indícios de divulgação indevida de informações técnicas sensíveis nos ativos externos dos terceiros, incluindo chaves SSH, chaves de API, arquivos de configuração, credenciais ou outros dados expostos de forma não intencional.

6.4.4. A plataforma deverá apresentar visão consolidada da superfície de ataque de cada terceiro monitorado, correlacionando domínios, subdomínios, endereços IP, portas, serviços, tecnologias e demais ativos técnicos identificados, sob a perspectiva de um potencial agente externo.

6.4.5. A plataforma deverá emitir alertas sobre novas exposições, alterações relevantes, vulnerabilidades críticas ou indícios de comprometimento identificados nos ativos dos terceiros, com classificação de risco, evidências técnicas disponíveis e recomendação de tratamento.

6.4.6. A plataforma deverá monitorar fontes relacionadas a grupos de ransomware, incluindo blogs de divulgação de vítimas, portais de negociação e sites de vazamento de dados, para identificar fornecedores e parceiros cadastrados que possam ter sido afetados.

6.4.7. A plataforma deverá emitir alerta quando identificar fornecedor ou parceiro monitorado como possível vítima de ransomware, permitindo a rápida avaliação da exposição da cadeia de fornecimento.

6.4.8. Para cada ocorrência identificada, a plataforma deverá disponibilizar o contexto técnico disponível, incluindo o grupo de ransomware associado, a data da divulgação, as informações ou dados potencialmente expostos e os ativos ou domínios relacionados, quando identificáveis.

6.4.9. A plataforma deverá apoiar a avaliação do risco de interrupção, contaminação ou indisponibilidade dos serviços prestados pelo terceiro afetado, considerando sua criticidade para as atividades da InPACTA e as dependências operacionais existentes.

6.5. DIMENSIONAMENTO POR CLIENTE

6.5.1. A PARCEIRA deverá disponibilizar acesso à plataforma aos usuários autorizados de cada cliente, com perfil de administração, autenticação multifator e controles compatíveis com as atribuições. O instrumento executivo definirá usuários, direitos de uso e recursos necessários, sem quantidade prefixada no instrumento geral.

6.5.2. A solução deverá permitir o cadastramento, a classificação, o monitoramento e a avaliação de risco dos fornecedores, parceiros, prestadores de serviços e demais terceiros incluídos no escopo autorizado de cada cliente. O dimensionamento, o

licenciamento e a expansão serão definidos no instrumento executivo, mediante metodologia documentada.

7. MÓDULO 4 – PLATAFORMA DE INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS (CTI)

7.1 REQUISITOS GERAIS DA PLATAFORMA

7.1.1. A plataforma deverá disponibilizar inteligência de ameaças cibernéticas contextualizada e acionável, proveniente de fontes associadas ao ecossistema de cibercrime, para apoiar a prevenção, a identificação, a análise e a mitigação de riscos relacionados aos ativos da InPACTA.

7.1.2. A plataforma deverá processar, pesquisar e apresentar informações de inteligência em múltiplos idiomas, com recursos de tradução automática integrada e suporte técnico especializado para análise de fontes relevantes em diferentes idiomas e regiões geográficas.

7.1.3. A plataforma deverá disponibilizar dados de vazamentos, bases comprometidas e demais informações de inteligência acompanhados, quando disponíveis, de contexto e metadados que permitam identificar a origem, a data, o autor ou identificador associado, a fonte de publicação e outros elementos úteis à investigação.

7.1.4. A PARCEIRA deverá disponibilizar canal para solicitação de novas fontes especializadas de inteligência, pesquisas direcionadas ou mecanismos de coleta sob demanda, cabendo à equipe especializada analisar a viabilidade, validar a fonte e, quando aplicável, implementar o respectivo mecanismo de coleta.

7.1.5. A plataforma deverá permitir a submissão de Solicitações de Inteligência — RFI sobre temas relacionados à cibersegurança, incluindo análise de atores de ameaça, grupos de ransomware, campanhas, técnicas utilizadas por adversários ou outros assuntos definidos pela InPACTA, com escopo e entregáveis previamente acordados.

7.1.6. A plataforma deverá aplicar Reconhecimento Óptico de Caracteres (OCR) às imagens coletadas em fontes principais e complementares de inteligência, permitindo a extração e a pesquisa dos textos nelas contidos para identificação de informações potencialmente expostas.

7.1.7. A plataforma deverá detectar credenciais comprometidas e outros dados sensíveis divulgados em fontes monitoradas mediante técnicas automatizadas de mineração e análise de texto, com geração de alertas e informações que apoiem a investigação e a mitigação do risco.

7.1.8. A plataforma deverá identificar, quando relacionados aos ativos e indicadores fornecidos pela InPACTA, indícios de vazamento de dados pessoais de colaboradores, referências a projetos, iniciativas ou informações institucionais sensíveis potencialmente expostas.

7.1.9. A plataforma deverá disponibilizar inteligência e relatórios sobre intenções de ataque contra órgãos públicos, setores específicos ou ativos monitorados, bem como sobre campanhas hacktivistas relevantes, contendo contexto, riscos e informações disponíveis para apoio à prevenção.

7.1.10. A plataforma deverá monitorar fóruns restritos, comunidades fechadas e outros ambientes de acesso controlado associados ao ecossistema de cibercrime, para identificação de ameaças, discussões e informações relevantes aos ativos da InPACTA.

7.1.11. A plataforma deverá monitorar sites, fóruns e mercados ilícitos que anunciem ou disponibilizem bases de dados comprometidas, permitindo a identificação de vazamentos e a análise do contexto e dos metadados associados.

7.1.12. A plataforma deverá identificar mercados ilícitos, anúncios e outras fontes que ofereçam acesso a máquinas infectadas, servidores, websites, contas corporativas ou demais ativos comprometidos.

7.1.13. A plataforma deverá monitorar canais, grupos e comunidades em plataformas privadas ou criptografadas de mensageria instantânea utilizadas por atores de ameaça, incluindo, quando disponíveis nas fontes monitoradas, ambientes como Telegram, Discord e tecnologias similares.

7.1.14. A plataforma deverá monitorar serviços de compartilhamento de texto, repositórios em nuvem, diretórios públicos e redes de compartilhamento de arquivos, visando identificar a exposição de informações confidenciais, dados sensíveis, vazamentos ou inteligência privada relacionada à InPACTA.

7.1.15. A plataforma deverá extrair e disponibilizar metadados relevantes das fontes monitoradas, incluindo, quando disponíveis, identificador ou pseudônimo do autor, identificadores de bot, data original de publicação, capturas de tela, links para a fonte de origem e demais elementos úteis à contextualização da inteligência.

7.1.16. A plataforma deverá manter acesso a dados históricos coletados e preservados em sua base de inteligência, inclusive quando a fonte original deixar de estar disponível na internet, permitindo análises retrospectivas e investigação de eventos anteriores.

7.1.17. A coleta de inteligência deverá observar procedimentos de controle de qualidade, rastreabilidade e preservação histórica, cabendo à PARCEIRA a responsabilidade pela qualidade e pela integridade dos dados disponibilizados na plataforma.

7.1.18. A plataforma deverá realizar coleta automatizada e passiva das fontes monitoradas, processando os dados brutos, extraindo metadados e incorporando as informações relevantes à sua base de inteligência sem expor os ativos, consultas ou indicadores da InPACTA às fontes de cibercrime.

7.1.19. A plataforma deverá disponibilizar API RESTful documentada, com suporte à integração bidirecional para consulta de dados, envio de indicadores, acionamento de fluxos autorizados e interoperabilidade com os sistemas de segurança da InPACTA.

7.1.20. As consultas realizadas pela InPACTA deverão ocorrer na base de inteligência da plataforma, sem interação direta com as fontes monitoradas, de modo a preservar o anonimato dos usuários e dos indicadores pesquisados.

7.1.21. A plataforma deverá permitir a integração de alertas, informações de inteligência e resultados de monitoramento com plataformas externas por meio de API, possibilitando o consumo automatizado das informações por sistemas da InPACTA.

7.1.22. A plataforma deverá suportar integração com soluções de SIEM, SOAR e demais ferramentas de segurança, inclusive por meio de APIs, webhooks, conectores ou mecanismos equivalentes, permitindo o enriquecimento de alertas e a automação de fluxos de resposta.

7.1.23. A plataforma deverá coletar e preservar evidências visuais das fontes monitoradas, incluindo capturas de tela associadas a publicações, anúncios, discussões ou demais conteúdos relevantes à investigação.

7.1.24. A PARCEIRA deverá adotar procedimento de validação, verificação de integridade e controle de qualidade antes de incorporar novas fontes à plataforma de inteligência, assegurando a confiabilidade, a relevância e a rastreabilidade dos dados coletados.

7.1.25. A plataforma deverá disponibilizar ambiente sandbox isolado para abertura e análise segura de arquivos potencialmente maliciosos, sem necessidade de instalação de componentes adicionais na infraestrutura da InPACTA.

7.1.26. A PARCEIRA deverá disponibilizar relatórios, pesquisas e análises de inteligência sob demanda, incluindo estudos sobre tendências setoriais, atores de ameaça, campanhas, táticas, técnicas e procedimentos — TTPs — e demais temas definidos pela InPACTA.

7.1.27. A PARCEIRA deverá disponibilizar apoio especializado para ações de takedown ou mitigação de conteúdos, domínios, páginas fraudulentas ou outros ativos maliciosos identificados, mediante solicitação, autorização prévia da InPACTA e observância da legislação aplicável.

7.1.28. A plataforma deverá disponibilizar base histórica de inteligência sobre vítimas e campanhas de ransomware, com cobertura, atualização, pesquisa e correlação

demonstráveis em relação aos ativos autorizados.

7.1.29. A plataforma deverá monitorar e coletar inteligência de canais e grupos de mensageria associados a agentes cibercriminosos, observadas a legalidade do acesso, a relevância, a atualização e a rastreabilidade das fontes.

7.1.30. A plataforma deverá manter dados atualizados sobre dispositivos comprometidos por malwares do tipo infostealer, com evidências suficientes de cobertura, origem, temporalidade e utilidade operacional.

7.1.31. A plataforma deverá coletar inteligência em tempo real de mercados ilícitos de acesso remoto, contemplando ampla cobertura de websites, servidores, contas corporativas de e-mail ou outros ativos comprometidos anunciados nessas fontes.

7.1.32. A plataforma deverá manter base pesquisável e atualizada de credenciais expostas provenientes de fontes legalmente acessíveis, com controles de acesso, rastreabilidade e evidências de abrangência e qualidade.

7.1.33. A plataforma deverá disponibilizar inteligência sobre grupos cibercriminosos e campanhas de ransomware relevantes, incluindo informações que apoiem a análise de atividades, táticas, técnicas, procedimentos e alvos.

7.1.34. A plataforma deverá abranger fontes de compartilhamento ou transferência de texto relevantes à inteligência de ameaças, com critérios demonstráveis de cobertura, atualização, legalidade e qualidade.

7.1.35. A PARCEIRA deverá apoiar a identificação, a análise e a mitigação de dispositivos, contas ou ativos comprometidos identificados em infraestruturas associadas a botnets, mercados de máquinas infectadas ou demais fontes de cibercrime.

7.1.36. A plataforma deverá realizar coleta e monitoramento contínuos de inteligência na web aberta, deep web e dark web, incluindo fóruns, blogs de ransomware, serviços de compartilhamento de texto, canais de mensageria instantânea e serviços onion acessíveis por meio da rede Tor, entre outras fontes relevantes.

7.1.37. A plataforma deverá disponibilizar histórico operacional e acervo de dados de inteligência compatíveis com a complexidade do objeto, comprovados por documentação técnica, demonstração na Prova de Conceito e demais evidências requeridas pela InPACTA.

7.1.38. A solução de Inteligência de Ameaças Cibernéticas - CTI efetivamente ofertada deverá apresentar comprovação verificável de adoção, maturidade e reconhecimento de mercado por fontes independentes, avaliações públicas, atestados, estudos de caso ou documentos equivalentes, sem dependência exclusiva de uma única instituição, plataforma ou fabricante.

7.1.38.1. A comprovação deverá identificar a solução ofertada, a fonte, o escopo da avaliação ou experiência, a data de referência e o mecanismo de verificação,

admitidos documentos equivalentes e fontes independentes.

7.1.38.2. A ausência de vínculo com ranking ou base específica não impedirá a comprovação por evidências independentes materialmente equivalentes, desde que verificáveis e relacionadas à solução efetivamente ofertada.

7.2. SERVIÇOS ESPECIALIZADOS SOB DEMANDA:

7.2.1. A PARCEIRA deverá disponibilizar, mediante solicitação da InPACTA, pesquisas direcionadas, análises de inteligência, relatórios especiais e Solicitações de Inteligência — RFI, com escopo, prazo e entregáveis previamente acordados.

7.2.2. A PARCEIRA poderá avaliar solicitações para inclusão de novas fontes de inteligência ou desenvolvimento de mecanismos de coleta especializados, observadas a viabilidade técnica, a legalidade, os requisitos de segurança e as condições comerciais aplicáveis.

7.2.3. A PARCEIRA poderá disponibilizar ambiente sandbox isolado para análise controlada de arquivos potencialmente maliciosos, quando acionado pela InPACTA.

7.2.4. A PARCEIRA poderá, mediante solicitação e autorização expressa da InPACTA, prestar apoio técnico a procedimentos de takedown, mitigação de conteúdos maliciosos ou interação controlada com fontes do ecossistema de cibercrime, desde que observadas a viabilidade técnica, a legislação aplicável e as regras de engajamento definidas pela InPACTA.

7.3. FUNÇÃO MONITORAMENTO CONTÍNUO

7.3.1. A plataforma deverá realizar monitoramento contínuo de iniciativas ativistas, campanhas hacktivistas, ameaças direcionadas e indicadores de intenção de ataque contra a InPACTA, órgãos públicos, setores de atuação ou ativos monitorados, produzindo alertas e relatórios de inteligência contextualizados.

7.3.2. A plataforma deverá identificar anúncios, discussões e indícios de comercialização ilícita de acessos não autorizados, credenciais, privilégios de rede, servidores, websites ou outros ativos comprometidos relacionados aos domínios, endereços IP e demais indicadores fornecidos pela InPACTA.

7.3.3. A plataforma deverá monitorar vulnerabilidades recentemente divulgadas que possam afetar os ativos da InPACTA e emitir informações contextualizadas sobre riscos, vetores de ataque e indícios de exploração relacionados.

7.3.4. A plataforma deverá realizar monitoramento passivo e contínuo da superfície externa dos ativos fornecidos pela InPACTA, identificando portas abertas, serviços expostos, tecnologias vulneráveis ou desatualizadas, configurações inseguras, bancos de dados expostos e demais fragilidades relevantes à avaliação da exposição

cibernética.

7.3.5. A plataforma deverá identificar páginas, aplicações, nomes de hosts, servidores e outros ativos sensíveis expostos à internet, especialmente aqueles que revelem informações críticas, configurações inadequadas ou potenciais pontos de exploração.

7.3.6. A plataforma deverá identificar e reportar indícios de intenção maliciosa relacionados à exploração de vulnerabilidades divulgadas que possam afetar os ativos da InPACTA, permitindo o aprofundamento da investigação e a adoção de medidas preventivas.

7.3.7. A plataforma deverá realizar descoberta automatizada de ativos de rede associados à InPACTA e disponibilizar representação visual da superfície externa identificada, permitindo a análise de domínios, endereços IP, portas, serviços, tecnologias e relacionamentos técnicos relevantes.

7.3.8. A plataforma deverá permitir o cadastro de Pessoas Expostas Politicamente — PEPs, autoridades, executivos e outros perfis estratégicos definidos pela InPACTA, emitindo alertas sobre possíveis intenções de ataque, exposição de credenciais, menções, discussões ou divulgação de informações relacionadas à sua movimentação, rotina ou segurança digital.

7.3.9. A plataforma deverá identificar vazamentos de bases de dados, informações sensíveis, dados corporativos e contas potencialmente comprometidas relacionadas à InPACTA, seus colaboradores, ativos, domínios ou ambientes tecnológicos, permitindo a investigação contextualizada dos achados.

7.3.10. A plataforma deverá emitir alertas em tempo próximo ao real sobre novas ameaças, exposições, credenciais comprometidas, vendas de acessos, vulnerabilidades, dados vazados e demais eventos relevantes identificados nas fontes monitoradas. Deverá, ainda, permitir a criação de alertas por e-mail a partir de consultas, termos, ativos e critérios personalizados pelos usuários autorizados.

7.3.11. A plataforma deverá permitir a exportação de informações, alertas e resultados de monitoramento em formato CSV ou outro formato estruturado amplamente utilizado, diretamente por sua interface gráfica ou por integração automatizada.

7.3.12. A plataforma deverá suportar arquitetura multi-tenant ou mecanismo equivalente de segregação lógica, permitindo o gerenciamento independente de múltiplas entidades, secretarias, unidades administrativas ou ambientes vinculados à InPACTA.

7.3.13. A plataforma deverá permitir a navegação e o aprofundamento de um alerta ou achado para outros módulos de inteligência e investigação relacionados, bem como disponibilizar recursos de comunicação ou registro colaborativo e

configurações específicas de monitoramento por ativo, entidade ou usuário autorizado.

7.3.14. A plataforma deverá disponibilizar recursos integrados para geração de relatórios executivos e técnicos em formato PDF, contendo informações adequadas aos públicos gerencial e operacional.

7.3.15. Quando aplicável aos cartões corporativos indicados pela InPACTA, a plataforma deverá identificar indícios de vazamento ou comercialização de dados de pagamento em fontes de cibercrime, permitindo consultas por BIN de seis dígitos ou por outro identificador seguro fornecido pela InPACTA. A validação pelo algoritmo de Luhn poderá ser utilizada exclusivamente para verificação de formato, sem caracterizar confirmação de comprometimento.

7.3.16. A plataforma deverá permitir o monitoramento contínuo e automatizado de palavras-chave, termos estratégicos, indicadores e demais critérios definidos pela InPACTA, com geração de alertas sobre novas ocorrências identificadas nas fontes monitoradas.

7.4. FUNÇÃO INVESTIGAÇÃO

7.4.1. A plataforma deverá disponibilizar interface gráfica para acesso unificado à base de inteligência cibernética, permitindo consultas centralizadas em diferentes conjuntos de dados, incluindo discussões de hacking, credenciais expostas, informações sobre acessos comprometidos, vazamentos, indicadores técnicos e relatórios de inteligência.

7.4.2. A plataforma deverá suportar pesquisas avançadas por meio de operadores booleanos, agrupamentos, busca aproximada, operadores de proximidade, curingas, campos de metadados e demais mecanismos que permitam a elaboração de consultas investigativas específicas.

7.4.3. A plataforma deverá permitir a execução de uma única consulta em múltiplos tipos de dados e fontes de inteligência, possibilitando a correlação integrada das informações e a navegação entre os resultados relacionados.

7.4.4. A plataforma deverá disponibilizar recursos de filtragem e refinamento dos resultados por propriedades, metadados, palavras-chave adicionais, tipo de dado, fonte, período, autor, ativo, indicador ou demais atributos relevantes à investigação.

7.4.5. A plataforma deverá permitir a criação, o armazenamento e o gerenciamento de consultas personalizadas, com geração de alertas por e-mail sobre novas ocorrências, resultados atualizados ou informações identificadas a partir dos critérios definidos pelo usuário autorizado.

7.4.6. A plataforma deverá permitir a identificação e a análise de atividades relacionadas a atores de ameaça ou fontes específicas a partir de consultas simples,

utilizando campos de metadados e mecanismos de correlação disponíveis na base de inteligência.

7.4.7. A plataforma deverá disponibilizar recursos de pesquisa de imagens e de mineração de texto em documentos, arquivos e demais conteúdos coletados, permitindo localizar menções, indicadores, termos relevantes e evidências visuais relacionadas às investigações.

7.4.8. A plataforma deverá permitir o download de configurações de bots, arquivos, artefatos digitais, bases de dados ou documentos identificados durante investigações, inclusive em formato compactado, exclusivamente por usuários expressamente autorizados pela InPACTA, conforme seus perfis de acesso e observados os requisitos de segurança e a legislação aplicável.

7.4.9. A plataforma deverá disponibilizar tradução automática integrada para dados e conteúdos coletados em múltiplos idiomas, permitindo a análise das informações diretamente no ambiente de investigação.

7.4.10. A plataforma deverá permitir o encaminhamento ou aprofundamento de resultados de investigação para outros módulos de inteligência, monitoramento ou análise relacionados, preservando o contexto e os elementos pesquisados.

7.4.11. A plataforma deverá disponibilizar integração por API documentada, permitindo consultas, exportações, intercâmbio de dados e conexão com ferramentas externas de segurança ou investigação.

7.4.12. A plataforma deverá fornecer acesso a uma base de conhecimento de inteligência cibernética produzida por analistas especializados, contendo relatórios finalizados, análises de eventos relevantes, novos riscos, fontes de interesse e contexto sobre ameaças identificadas.

7.4.13. A plataforma deverá disponibilizar consultas, painéis ou modelos pré-configurados para temas estratégicos, incluindo vítimas recentes de ransomware, corretores de acesso inicial, grupos hacktivistas, atores de ameaça e outros temas relevantes ao cenário de cibercrime.

7.4.14. A plataforma deverá manter acesso a dados históricos e informações arquivadas, inclusive quando as fontes originais deixarem de estar disponíveis publicamente.

7.4.15. A plataforma deverá apoiar atividades de threat hunting, investigação cibernética e análise de inteligência, fornecendo informações contextuais sobre Táticas, Técnicas e Procedimentos — TTPs, perfis de atores, identidades, infraestrutura utilizada, discussões e demais evidências relacionadas ao ecossistema de ameaças.

7.5. FUNÇÃO PANORAMA DE AMEAÇAS

7.5.1. A plataforma deverá disponibilizar relatórios e painéis de inteligência sobre campanhas de ransomware, contemplando classificação de severidade, contexto, impacto potencial e monitoramento de fontes relacionadas a vazamentos e extorsão digital.

7.5.2. A plataforma deverá enriquecer dados, eventos e alertas com informações provenientes de fontes de cibercrime, transformando dados brutos em inteligência contextualizada para apoio à prevenção, detecção, investigação e resposta a ameaças.

7.5.3. A plataforma deverá apresentar visão consolidada das principais atividades em evolução no ecossistema de cibercrime, incluindo eventos de ransomware, grupos APT, comercialização de acessos, vazamentos de dados, atividades hacktivistas e outras tendências relevantes, acompanhadas de estatísticas e indicadores analíticos.

7.5.4. A plataforma deverá disponibilizar destaques diários sobre atividades relevantes identificadas em fontes monitoradas, incluindo, quando disponíveis, indicadores de comprometimento, técnicas utilizadas, atores envolvidos, setores afetados e possíveis impactos para a InPACTA.

7.5.5. A plataforma deverá disponibilizar feed de inteligência finalizada, produzida ou validada por equipe especializada, contendo análises sobre o contexto, as motivações, os métodos e os riscos associados às ameaças emergentes.

7.5.6. A plataforma deverá disponibilizar dashboards executivos e operacionais sobre tendências do cenário de ameaças, alertas prioritários, eventos relevantes, análises diárias e informações estratégicas que apoiem a tomada de decisão pela Administração.

7.5.7. A PARCEIRA deverá disponibilizar, quando solicitado pela InPACTA, relatórios de inteligência segmentados por setor, segmento de atuação ou contexto institucional, contemplando tendências de malware, vulnerabilidades emergentes, campanhas de ataque e técnicas relevantes.

7.5.8. A plataforma deverá fornecer inteligência estratégica sobre campanhas de ransomware, comercialização de acessos indevidos, vazamentos de bases de dados, exposição de credenciais e ameaças direcionadas, permitindo a priorização de medidas de segurança conforme o contexto da InPACTA.

7.6 FUNÇÃO INTELIGÊNCIA TÉCNICA

7.6.1. A plataforma deverá identificar automaticamente serviços de acesso remoto, incluindo RDP, potencialmente comprometidos ou envolvidos em atividades de cibercrime, permitindo a antecipação de riscos de acesso indevido à infraestrutura da InPACTA.

7.6.2. A plataforma deverá identificar proxies, infraestruturas intermediárias e demais

recursos técnicos potencialmente associados a atividades de cibercrime, com informações que apoiem a análise de sua utilização por agentes de ameaça.

7.6.3. A plataforma deverá identificar endereços IP potencialmente associados a vítimas de phishing, contas comprometidas ou outras atividades maliciosas identificadas em fontes de inteligência de cibercrime.

7.6.4. A plataforma deverá identificar websites, domínios, servidores e endpoints potencialmente comprometidos ou utilizados em atividades maliciosas, incluindo distribuição de malware, phishing, campanhas de fraude e demais operações cibernéticas.

7.6.5. A plataforma deverá disponibilizar repositório de Indicadores de Comprometimento — IOCs provenientes de fontes underground e demais fontes de inteligência, com dados técnicos contextualizados e adequados à integração com ferramentas de segurança.

7.6.6. A plataforma deverá permitir a exportação de informações técnicas, indicadores, resultados de investigação e dados relacionados a ativos comprometidos em formato CSV ou outro formato estruturado amplamente utilizado.

7.6.7. A plataforma deverá disponibilizar dados técnicos por API em formato legível por máquinas, permitindo a integração de feeds de IPs, domínios, indicadores e demais informações com soluções de segurança da InPACTA.

7.6.8. A plataforma deverá suportar os padrões STIX/TAXII para compartilhamento, ingestão e intercâmbio automatizado de inteligência de ameaças com plataformas TIP, SIEM, SOAR e demais ferramentas compatíveis.

7.7 FUNÇÃO ATORES DE AMEAÇA E INTELIGÊNCIA APT

7.7.1. A plataforma deverá consolidar inteligência sobre atores de ameaça a partir de fontes de cibercrime, pesquisas especializadas, dados de fontes abertas e análises produzidas por especialistas, permitindo visão unificada dos perfis, atividades e relacionamentos identificados.

7.7.2. A plataforma deverá disponibilizar painel centralizado de atores de ameaça, contendo perfis categorizados, histórico de atividades, campanhas, infraestrutura utilizada, alvos, informações relevantes e, quando disponível, resumo analítico elaborado por especialistas ou enriquecido por inteligência artificial.

7.7.3. A plataforma deverá analisar padrões de atividade, afiliações, motivações, setores e regiões geográficas alvo dos atores de ameaça, permitindo a identificação de suas preferências, estratégias e tendências de atuação.

7.7.4. A plataforma deverá correlacionar aliases, perfis, contas, pseudônimos, assinaturas e demais identidades digitais potencialmente associadas a um mesmo ator de ameaça, preservando o histórico de alterações e a origem das evidências

disponíveis.

7.7.5. A plataforma deverá disponibilizar filtros avançados para pesquisa de atores de ameaça por motivação, origem, setor alvo, localização geográfica, tipo de ameaça, atividade, alias, dados de contato disponíveis ou outros atributos relevantes.

7.7.6. Quando houver informação confiável, disponível e legalmente utilizável, a plataforma poderá apresentar dados de atribuição relativos a indivíduos, grupos ou entidades associados a atividades cibernéticas maliciosas, acompanhados das evidências e das limitações de confiabilidade aplicáveis.

7.7.7. A plataforma deverá integrar Táticas, Técnicas e Procedimentos - TTPs aos perfis de atores de ameaça, utilizando o framework MITRE ATT&CK ou referência equivalente, e manter os perfis atualizados à medida que novas atividades forem identificadas.

7.7.8. A plataforma deverá disponibilizar inteligência sobre grupos APT e atores patrocinados por Estados, incluindo objetivos estratégicos, campanhas, setores e regiões alvo, aliases, campos operacionais, estrutura de atribuição e relacionamentos hierárquicos identificados, quando disponíveis.

7.7.9. A plataforma deverá disponibilizar IOCs relacionados a grupos APT e demais atores de ameaça, incluindo domínios, endereços IP, hashes, ferramentas e outros artefatos técnicos, com possibilidade de exportação ou integração com sistemas externos.

7.7.10. A plataforma deverá disponibilizar relatórios, referências de fontes abertas e de cibercrime, perfis exportáveis e apoio de analistas especializados para pesquisas aprofundadas sobre atores de ameaça ou grupos APT, mediante solicitação da InPACTA.

7.8 FUNÇÃO PROTEÇÃO DE IDENTIDADE

7.8.1. A plataforma deverá identificar credenciais, contas, cookies de sessão e demais dados de identidade potencialmente comprometidos, especialmente aqueles originados de logs de malwares do tipo infostealer, vazamentos, listas compiladas de credenciais e fontes de cibercrime.

7.8.2. A plataforma deverá realizar classificação automática dos incidentes e exposições de identidade por categoria, tipo de ameaça, severidade e risco, permitindo a priorização de ocorrências relacionadas a ransomware, roubo de dados, credenciais vazadas, acesso à infraestrutura e demais atividades maliciosas.

7.8.3. A plataforma deverá permitir o cadastramento, a importação e a configuração de ativos de identidade a serem monitorados, incluindo domínios, FQDNs, endereços IP, faixas de IP, endereços de e-mail, portais específicos e serviços SaaS utilizados pela InPACTA.

7.8.4. Os alertas de comprometimento de identidade deverão disponibilizar, quando disponíveis e pertinentes, dados como usuário, endereço IP da máquina infectada, sistema operacional, datas de comprometimento e descoberta, origem do dado, família de malware, hostname, serviços adicionais comprometidos e demais metadados necessários à investigação.

7.8.5. A plataforma deverá correlacionar dados de contas comprometidas, máquinas infectadas, serviços acessados, origem da infecção, malware associado e demais informações disponíveis, permitindo análise contextualizada da exposição de cada identidade.

7.8.6. A plataforma deverá identificar e reduzir ocorrências duplicadas ou já tratadas, mediante mecanismos de deduplicação e supressão configurável, preservando a rastreabilidade do incidente original e o histórico das decisões adotadas.

7.8.7. A plataforma deverá permitir pesquisa, filtragem, ordenação e criação de visões salvas sobre incidentes de identidade, utilizando critérios como serviço, usuário, domínio, FQDN, endereço IP, identificador de bot, criticidade, categoria, data de infecção, data de criação, situação de tratamento e outros atributos disponíveis.

7.8.8. A plataforma deverá disponibilizar linha do tempo das infecções e dos comprometimentos identificados, distinguindo detecções iniciais de ocorrências recorrentes e apresentando os metadados disponíveis sobre a origem e a evolução da exposição.

7.8.9. A plataforma deverá permitir a classificação diferenciada de credenciais de colaboradores, clientes, fornecedores ou outros grupos definidos pela InPACTA, com base em regras configuráveis e informações de contexto.

7.8.10. A plataforma deverá permitir o registro e o acompanhamento do tratamento de cada ocorrência, incluindo a marcação de resultados como resolvidos, mitigados ou pendentes, sem prejuízo da preservação das evidências e do histórico de auditoria.

7.8.11. A plataforma deverá suportar integração por API, webhooks, playbooks ou mecanismos equivalentes com soluções de segurança e resposta a incidentes, permitindo o encaminhamento automatizado de alertas e a orquestração de fluxos aprovados pela InPACTA.

7.8.12. A plataforma deverá disponibilizar arquitetura multi-tenant ou mecanismo equivalente de segregação lógica, permitindo a gestão separada de dados, ativos, configurações e permissões por entidade, secretaria, unidade administrativa ou ambiente monitorado.

7.8.13. A plataforma deverá permitir o monitoramento de mercados de acesso remoto, mercados de máquinas infectadas e outras fontes especializadas associadas à comercialização ou exploração de contas e ativos comprometidos.

7.8.14. A plataforma deverá monitorar cookies de sessão comprometidos associados a usuários e ativos da InPACTA, fornecendo, quando disponíveis, informações sobre a máquina infectada, família de malware, data da infecção, expiração da sessão e outros serviços comprometidos no mesmo host.

7.9 FUNÇÃO PROTEÇÃO DE MARCA

7.9.1. A plataforma deverá identificar registros de novos domínios similares aos domínios institucionais da InPACTA, permitindo a detecção preventiva de tentativas de impersonação, fraude ou phishing.

7.9.2. A plataforma deverá identificar websites, páginas, aplicações e contas em redes sociais que utilizem indevidamente o nome, marcas, logotipos ou demais elementos de identidade institucional da InPACTA.

7.9.3. A plataforma deverá identificar e classificar websites de phishing, domínios fraudulentos e demais recursos digitais que simulem a identidade institucional da InPACTA com o objetivo de capturar credenciais, aplicar golpes ou distribuir conteúdo malicioso.

7.9.4. A plataforma deverá disponibilizar informações WHOIS ou dados equivalentes sobre domínios suspeitos, incluindo, quando disponíveis, informações de registro, contatos, datas relevantes e demais elementos que apoiem a investigação e as medidas de resposta.

7.9.5. A plataforma deverá preservar evidências visuais dos websites, domínios ou contas identificados, incluindo capturas de tela e referências à fonte original, para apoio à investigação, instrução de procedimentos administrativos e eventual solicitação de remoção.

7.9.6. A PARCEIRA deverá prestar apoio ao processo de takedown de websites, domínios, páginas fraudulentas ou contas de redes sociais identificadas, mediante solicitação e autorização da InPACTA, observadas a viabilidade técnica, as políticas das plataformas e a legislação aplicável.

7.9.7. A plataforma deverá permitir o acompanhamento da situação dos achados de proteção de marca, incluindo a identificação, a validação, a solicitação de remoção, a situação do atendimento e as evidências disponíveis.

7.10 FUNÇÃO INDICADORES DE COMPROMETIMENTO

7.10.1. A plataforma deverá disponibilizar painel centralizado de Indicadores de Comprometimento — IOCs, contendo indicadores coletados, validados, classificados e enriquecidos a partir de múltiplas fontes de inteligência.

7.10.2. A plataforma deverá manter feed de IOCs continuamente atualizado, com

validação e enriquecimento dos indicadores provenientes de fontes de cibercrime, campanhas maliciosas, eventos de segurança e demais fontes relevantes.

7.10.3. A plataforma deverá permitir que a InPACTA inclua seus próprios IOCs para correlação, enriquecimento, monitoramento, pesquisa e geração de alertas.

7.10.4. A plataforma deverá enriquecer cada IOC com informações de contexto, incluindo, quando disponíveis, campanhas relacionadas, fonte de origem, registros temporais, discussões em ambientes underground, reputação, infraestrutura associada e referências técnicas relevantes.

7.10.5. A plataforma deverá correlacionar IOCs com atores de ameaça, grupos APT, famílias de malware, campanhas, ferramentas, técnicas e demais entidades relacionadas.

7.10.6. A plataforma deverá permitir investigação por pivô a partir de qualquer IOC, possibilitando a navegação e a correlação com atores, campanhas, infraestrutura maliciosa, malware, relatórios de inteligência e discussões em fontes monitoradas.

7.10.7. A plataforma deverá disponibilizar integração de IOCs por API e suportar os padrões STIX/TAXII para compartilhamento, ingestão e intercâmbio automatizado de inteligência com plataformas TIP, SIEM, SOAR e demais ferramentas compatíveis.

7.10.8. A plataforma deverá permitir a exportação de IOCs e de seus respectivos atributos em formato estruturado e legível por máquinas, observados os controles de acesso e as políticas de segurança aplicáveis.

7.11 FUNÇÃO MAPEAMENTO DE INFRAESTRUTURA MALICIOSA

7.11.1. A plataforma deverá permitir a investigação de infraestrutura maliciosa a partir de um indicador inicial, como endereço IP ou domínio, expandindo a análise para entidades relacionadas e apresentando os vínculos técnicos identificados.

7.11.2. A plataforma deverá consolidar, em ambiente unificado de investigação, dados de fontes internas e externas, incluindo logs NetFlow, IOCs, dados de reputação, portas, banners, ativos, credenciais comprometidas, informações de infostealers, discussões de cibercrime e demais fontes disponíveis.

7.11.3. A plataforma deverá suportar a análise e o relacionamento entre diferentes tipos de entidades, incluindo endereços IP, domínios, FQDNs, certificados SSL/TLS, páginas web, hashes de arquivos, indicadores de rede e demais artefatos técnicos.

7.11.4. A plataforma deverá realizar análise automatizada dos ativos e entidades pesquisados, apresentando informações de contexto, classificação de possível função maliciosa, pontuação indicativa de risco ou maliciosidade e hipóteses de atribuição, sempre acompanhadas das evidências disponíveis.

7.11.5. A plataforma deverá permitir o monitoramento contínuo das entidades investigadas, registrando novas informações, alterações, atualizações e histórico de

atividades relacionadas aos ativos acompanhados.

7.11.6. A plataforma deverá permitir a expansão da investigação a partir de qualquer entidade descoberta, possibilitando a identificação de novos relacionamentos, infraestrutura associada, campanhas, possíveis vítimas e demais elementos conexos.

7.11.7. A plataforma deverá identificar e classificar entidades potencialmente maliciosas por sua função, incluindo, quando aplicável, servidores de comando e controle — C2, proxies, servidores de salto, VPNs, infraestrutura de hospedagem e demais componentes utilizados em operações cibernéticas.

7.11.8. A plataforma deverá disponibilizar visualização gráfica das relações entre entidades, atividades, cadeias de infraestrutura e possíveis hierarquias de controle, permitindo a análise de vínculos entre ativos aparentemente distintos.

7.11.9. A plataforma deverá disponibilizar gerenciamento centralizado de casos de investigação, permitindo organizar ativos, evidências, hipóteses, atividades, anotações, classificações e resultados relacionados a cada caso.

7.11.10. A plataforma deverá apresentar inteligência técnica enriquecida sobre os ativos investigados, incluindo, quando disponíveis, portas abertas, detalhes DNS, dados de registro, logs NetFlow, reputação, histórico de atividade e informações de infraestrutura.

7.11.11. A plataforma deverá permitir a identificação de encadeamentos de infraestrutura e de relações de controle entre servidores, domínios, certificados, páginas maliciosas, hashes e demais entidades, apoiando a reconstrução de operações de agentes de ameaça.

7.11.12. A plataforma deverá disponibilizar fluxos de investigação personalizáveis, com recursos para filtrar, classificar, etiquetar, organizar e exportar informações conforme critérios definidos pela InPACTA.

7.12 COMPROVAÇÃO DE RECONHECIMENTO DE MERCADO E VALIDAÇÃO POR USUÁRIOS CORPORATIVOS

7.12.1. Para fins de avaliação complementar da maturidade, da aceitação e da experiência de uso da solução ofertada, a interessada poderá apresentar evidências de reconhecimento de mercado ou validação por usuários corporativos.

7.12.2. Serão aceitos, entre outros meios de comprovação, relatórios, avaliações, estudos de mercado, certificações, referências de clientes, casos de uso, premiações, distinções ou documentos emitidos por entidades independentes, desde que relacionados ao produto ou à solução efetivamente ofertada.

7.12.3. A documentação apresentada deverá permitir identificar, quando aplicável, o produto avaliado, a entidade responsável pela avaliação, a data de emissão ou extração, a metodologia utilizada e os elementos que evidenciem a experiência de

uso ou a adoção corporativa da solução.

7.13. DIMENSIONAMENTO POR CLIENTE

7.13.1. A PARCEIRA deverá disponibilizar acesso à plataforma de Inteligência de Ameaças Cibernéticas aos usuários autorizados, com perfil de administração, autenticação multifator, gestão de perfis e trilha de auditoria. O dimensionamento dos acessos e dos direitos de uso será definido por cliente.

7.13.2. A solução deverá permitir o monitoramento contínuo dos domínios institucionais incluídos no escopo de cada cliente, incluindo domínios principais, secretarias, portais, serviços digitais e demais ambientes eletrônicos oficialmente indicados. A abrangência será definida no instrumento executivo.

7.13.3. A solução deverá permitir o monitoramento dos endereços de correio eletrônico institucionais prioritários definidos no escopo de cada cliente, incluindo, quando aplicável, contas de administradores, gestores, autoridades, equipes de tecnologia, usuários com acesso privilegiado e responsáveis por serviços públicos críticos.

7.13.4. A plataforma deverá permitir consultas avançadas, incluindo pesquisas relacionadas a domínios, endereços IP, endereços de correio eletrônico, credenciais expostas, hashes, URLs, malwares, atores de ameaça, campanhas, vulnerabilidades, grupos, palavras-chave e demais entidades técnicas relevantes. As métricas, os direitos de uso e as condições de execução e remuneração serão definidos no instrumento executivo de cada cliente, sem franquia geral prefixada.

7.13.5. A solução deverá permitir o monitoramento contínuo dos objetos de interesse incluídos no escopo de cada cliente, compreendendo domínios, subdomínios, endereços IP, endereços de correio eletrônico, marcas, nomes institucionais, sistemas, serviços, fornecedores, palavras-chave, vulnerabilidades, autoridades e demais elementos autorizados.

7.13.6. A solução deverá permitir o monitoramento contínuo de marcas, nomes, siglas, logotipos, domínios institucionais, programas, serviços públicos e outros identificadores oficiais incluídos no escopo autorizado de cada cliente, conforme dimensionamento do instrumento executivo.

7.13.7. A PARCEIRA deverá disponibilizar suporte a solicitações de remoção, bloqueio, denúncia ou notificação de conteúdo, domínio, perfil, página ou recurso fraudulento identificado, observadas a análise de viabilidade, as regras dos provedores e as medidas jurídicas ou administrativas necessárias. O acionamento e as condições de atendimento serão definidos no instrumento executivo, sem quantidade geral prefixada.

7.13.8. A solução deverá permitir mapeamentos investigativos de infraestrutura

maliciosa a partir de domínios, endereços IP, URLs, hashes, certificados digitais, endereços de correio eletrônico, malwares, campanhas, atores de ameaça ou outros artefatos técnicos relacionados aos riscos do cliente. O escopo e as condições de acionamento serão definidos por implementação, sem volume de entregas prefixado.

8. MÓDULO 5 – ANALISTAS CIBERNÉTICOS DIGITAIS BASEADOS EM INTELIGÊNCIA ARTIFICIAL

8.1 VISÃO GERAL DA SOLUÇÃO

8.1.1. A solução deverá disponibilizar analistas cibernéticos digitais baseados em Inteligência Artificial, utilizando modelos de linguagem de grande escala, mecanismos de automação e fluxos de trabalho orientados por agentes para apoiar as atividades de Inteligência de Ameaças Cibernéticas — CTI.

8.1.2. Os analistas cibernéticos digitais deverão apoiar, no mínimo, a geração de briefings executivos e operacionais, a triagem e a contextualização de credenciais comprometidas, campanhas de phishing, domínios fraudulentos, abuso de marca, IOCs, assinaturas de malware e atividades de atores de ameaça.

8.1.3. A solução deverá permitir consultas em linguagem natural, fornecendo respostas contextualizadas, referências às fontes disponíveis, recomendações técnicas e informações que apoiem investigações, threat hunting, priorização de riscos e tomada de decisão.

8.1.4. A solução deverá correlacionar informações provenientes de múltiplas fontes de inteligência e segurança, produzindo análises, hipóteses investigativas, recomendações de mitigação e priorização de riscos conforme o contexto operacional da InPACTA.

8.1.5. As respostas, classificações, recomendações e análises produzidas por Inteligência Artificial deverão possuir caráter assistivo e não substituirão a validação humana em decisões críticas, investigações conclusivas ou ações que possam produzir impacto relevante no ambiente da InPACTA.

8.2 AGENTES ESPECIALIZADOS PARA AMBIENTES CORPORATIVOS E SETOR PÚBLICO

8.2.1. A solução deverá disponibilizar recursos de IA capazes de apoiar ambientes corporativos, SOCs, MSSPs e órgãos públicos na identificação, na correlação, na priorização e na investigação de ameaças relacionadas aos ativos monitorados.

8.2.2. Os agentes deverão produzir resultados contextualizados com base nos ativos,

indicadores, setores, localização geográfica, cadeia de fornecedores e demais parâmetros autorizados pela InPACTA.

8.3 INTERAÇÃO POR FERRAMENTAS DE COLABORAÇÃO

8.3.1. A solução deverá permitir a interação entre usuários autorizados e os analistas digitais por meio de portal web, correio eletrônico, plataformas corporativas de colaboração ou outros canais compatíveis com o ambiente da InPACTA.

8.3.2. A solução deverá permitir o envio e o recebimento de alertas, investigações, recomendações, solicitações de análise, aprovação e escalonamentos pelos canais integrados, mantendo sincronização e rastreabilidade com a plataforma de inteligência.

8.3.3. Os usuários autorizados deverão poder consultar os agentes em linguagem natural para solicitar análises, validar hipóteses, obter contexto sobre ameaças e acompanhar investigações ou incidentes em andamento.

8.4 ACESSO À BASE DE INTELIGÊNCIA DE AMEAÇAS

8.4.1. Os analistas cibernéticos digitais deverão possuir acesso integrado, contínuo e direto à base de Inteligência de Ameaças Cibernéticas da solução ofertada, permitindo a correlação automática de informações e o enriquecimento contextual das consultas, análises e recomendações produzidas, observados o escopo contratado, os perfis de acesso, as licenças aplicáveis e os requisitos legais e de segurança.

8.4.2. A base utilizada pelos agentes deverá contemplar, quando contratados e aplicáveis, dados sobre credenciais comprometidas, IOCs, malware, vulnerabilidades, TTPs, infraestrutura maliciosa, discussões em fontes de cibercrime, phishing, fraude digital, abuso de marca, atores de ameaça, grupos APT, tendências, alertas e relatórios de inteligência.

8.4.3. A solução deverá apresentar, sempre que tecnicamente possível, a origem, a data, o grau de confiança e as limitações das informações utilizadas na elaboração das respostas, análises e recomendações.

8.5 AÇÕES ORQUESTRADAS, TRIAGEM E RELATÓRIOS

8.5.1. Os analistas cibernéticos digitais deverão apoiar a triagem, a validação, a classificação, a priorização e o enriquecimento de alertas e incidentes, reduzindo o tempo de análise e auxiliando na identificação de falsos positivos.

8.5.2. A solução deverá permitir a geração de relatórios técnicos e executivos sobre investigações, ameaças, atores maliciosos, IOCs, evidências coletadas, análises

produzidas e recomendações de mitigação.

8.5.3. A solução poderá executar ou recomendar ações automatizadas e semi automatizadas apenas conforme políticas, fluxos de aprovação, perfis de acesso e níveis de autonomia previamente definidos pela InPACTA.

8.5.4. Qualquer ação que possa bloquear, isolar, alterar, excluir, redefinir credenciais, revogar sessões, modificar configurações ou impactar ativos da InPACTA dependerá de autorização humana prévia, exceto quando existir playbook expressamente aprovado para execução automática.

8.6 INTEGRAÇÃO COM SISTEMAS DE ENDPOINT, REDE E SEGURANÇA

8.6.1. A solução deverá integrar-se às ferramentas indicadas pela InPACTA por APIs, conectores ou padrões documentados previstos na proposta e na matriz de integração.

8.6.2. As integrações deverão permitir a correlação entre a inteligência de ameaças e os eventos, alertas e telemetrias de endpoints, servidores, identidades, aplicações, serviços em nuvem e infraestrutura de rede.

8.6.3. A solução deverá apoiar a investigação e a resposta a incidentes por meio do enriquecimento de alertas, da correlação de IOCs, da recomendação de procedimentos e da orquestração controlada de fluxos autorizados.

8.7 INTEGRAÇÃO COM GERENCIAMENTO DE IDENTIDADE E ACESSO

8.7.1. A solução deverá permitir integração com plataformas de IAM e provedores de identidade, por meio de mecanismos compatíveis com o ambiente da InPACTA.

8.7.2. A integração deverá permitir correlacionar eventos de identidade, credenciais vazadas, atividades suspeitas, indicadores de comprometimento e riscos associados a usuários, contas, acessos privilegiados e identidades digitais.

8.7.3. A solução deverá apoiar a investigação e a resposta a incidentes de comprometimento de identidade, respeitados os fluxos de autorização e as competências da InPACTA.

8.8 INTEGRAÇÃO COM FONTES EXTERNAS DE ENRIQUECIMENTO

8.8.1. A solução poderá integrar fontes externas confiáveis de inteligência, dados empresariais ou dados públicos para enriquecimento contextual de entidades, organizações, ativos e demais elementos envolvidos em investigações cibernéticas.

8.8.2. A utilização de dados pessoais, dados de contato ou informações provenientes de fontes externas deverá observar finalidade legítima, necessidade, controles de acesso, rastreabilidade e a legislação aplicável à proteção de dados pessoais.

8.9 SUPORTE A MÚLTIPLOS IDIOMAS

8.9.1. A solução deverá permitir consultas, análises, investigações e apresentação de resultados em múltiplos idiomas, com recursos de tradução e interpretação contextual que preservem, tanto quanto tecnicamente possível, o significado técnico das informações processadas.

8.10 VALIDAÇÃO AUTOMATIZADA DE CREDENCIAIS COMPROMETIDAS

8.10.1. A solução deverá realizar a validação automatizada e controlada de credenciais potencialmente comprometidas, utilizando mecanismos seguros para verificar sua condição de exposição e eventual validade, sem comprometer a integridade dos sistemas ou dos serviços envolvidos.

8.10.2. A validação poderá incluir, quando tecnicamente aplicável e autorizada pela InPACTA, a verificação de credenciais em serviços publicamente acessíveis.

8.10.3. A solução deverá gerar relatórios consolidados contendo o resultado da validação de cada credencial, indicando seu status, nível de risco, evidências disponíveis, data da última verificação e demais informações relevantes para apoio à investigação.

8.11. SEGURANÇA, SUPERVISÃO E RASTREABILIDADE

8.11.1. Resultados de IA deverão indicar, sempre que possível, fontes, confiança, limitações e evidências.

8.11.2. A solução deverá manter trilha de auditoria de consultas, respostas, dados acessados, recomendações, aprovações e ações.

8.11.3. Conteúdos e comandos provenientes de fontes externas deverão ser tratados como não confiáveis, com controles contra manipulação e injeção de comandos.

8.11.4. Os analistas digitais não poderão alterar controles, executar código, bloquear ativos ou excluir informações sem autorização humana e mecanismo previamente aprovado.

8.11.5. A PARCEIRA deverá avaliar periodicamente com precisão, utilidade, falsos positivos e desempenho dos analistas digitais.

8.12. DIMENSIONAMENTO POR CLIENTE DOS ANALISTAS DIGITAIS

8.12.1. Os analistas digitais deverão constituir perfis configuráveis da mesma solução, compartilhando a plataforma, a base de inteligência, os controles de segurança, a trilha de auditoria e as integrações, sem exigir produtos isolados para

cada perfil. A tabela descreve funções e critérios de dimensionamento. Perfis efetivamente ativados, simultaneidade, acessos, recursos e licenciamento serão definidos no instrumento executivo de cada cliente, sem quantitativos prefixados na parceria.

ELEMENTO	CRITÉRIO DE DIMENSIONAMENTO	APLICAÇÃO RECOMENDADA	SITUAÇÃO
Perfis configuráveis de analista digital	Perfis configuráveis conforme as funções e o escopo autorizado.	Perfis para apoio operacional ao SOC e para investigação governamental, configurados na mesma solução, com supervisão humana.	A configuração efetiva, a simultaneidade e a unidade de licenciamento serão fixadas no instrumento executivo de cada cliente.
Usuários nomeados	Acessos dimensionados por cliente, com segregação de funções.	Perfis de administração, operação técnica, gestão ou auditoria, conforme as atribuições autorizadas.	Os acessos e sua inclusão no licenciamento serão definidos no instrumento executivo, sem quantidade geral prefixada.
Regime de operação	24x7x365	Monitoramento e processamento contínuos, observados a supervisão humana e os fluxos de autorização.	Cobertura, disponibilidade e suporte serão definidos no instrumento executivo, preservado o regime de operação previsto.
Consultas e investigações	Compatível com o escopo contratado	Consultas, briefings, investigações e relatórios compatíveis com o escopo autorizado para a SOLUÇÃO INTEGRADA PARA Cibersegurança .	Demanda variável, condicionada ao acionamento, às franquias e aos limites expressamente definidos no instrumento executivo.

9. REQUISITOS TRANSVERSAIS DAS PLATAFORMAS E DOS SERVIÇOS

9.1. As plataformas deverão possuir interface web segura, gestão de usuários, perfis e grupos, autenticação multifator, segregação de funções e trilhas de auditoria.

9.2. Deverão disponibilizar pesquisa, filtros, dashboards, alertas, notificações, casos, relatórios e exportações compatíveis com cada módulo.

9.3. Os registros deverão utilizar referência temporal sincronizada e permitir correlação entre origem, usuário, ativo, alerta, evidência, ação e resultado.

9.4. A solução deverá disponibilizar APIs, conectores ou mecanismos documentados de integração.

9.5. Administração, consulta, investigação e exportação deverão observar menor privilégio, necessidade de conhecimento e rastreabilidade.

9.6. A PARCEIRA deverá monitorar disponibilidade e saúde dos componentes, registrando falhas e ações corretivas.

9.7. Interface, documentação operacional e suporte deverão estar disponíveis em língua portuguesa.

10. LICENCIAMENTO, MÓDULOS E DIREITOS DE USO

10.1. A INTERESSADA deverá apresentar matriz de licenciamento com produtos, edições, métricas, direitos de uso, dependências, suporte, APIs, conectores e critérios de expansão. O dimensionamento de usuários, ativos, recursos e armazenamento será definido por cliente, sem pacote volumétrico prefixado para a parceria.

10.2. O licenciamento deverá assegurar as funcionalidades, integrações, entregáveis e níveis de serviço previstos. Os direitos de uso e os recursos necessários a cada implementação serão dimensionados e formalizados antes de sua execução.

10.3. Não será admitida dependência de licença, módulo ou conector essencial não identificado na proposta.

10.4. Atualizações corretivas, patches e versões necessárias à continuidade deverão estar abrangidos durante a vigência.

10.5. O consumo ordinário de APIs e integrações necessário à execução regular não poderá gerar cobrança adicional não prevista.

10.6. A PARCEIRA responderá pela validade, suficiência e renovação das licenças, inclusive de terceiros.

10.7. A comprovação deverá ocorrer por documentação oficial ou outro meio verificável.

11. SEGURANÇA DA INFORMAÇÃO, PROTEÇÃO DE DADOS E

CONFORMIDADE

11.1. A solução deverá adotar controles de confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade e resiliência compatíveis com os riscos.

11.2. Deverá utilizar autenticação, autorização, gestão de sessão, segregação de funções, menor privilégio e revisão de acessos.

11.3. Dados, credenciais, evidências, relatórios e comunicações sensíveis deverão ser protegidos contra acesso, alteração ou divulgação não autorizados, mediante criptografia em trânsito e, quando armazenados, em repouso, além de controles de acesso compatíveis.

11.4. A PARCEIRA deverá manter gestão de vulnerabilidades e atualização dos componentes utilizados.

11.5. Incidentes de segurança que afetem a solução, os dados tratados ou a continuidade dos serviços deverão ser comunicados formalmente à InPACTA, no prazo de 24 horas, com indicação do impacto identificado, das medidas adotadas e das atualizações relevantes.

11.6. O tratamento de dados pessoais deverá observar os princípios da finalidade, necessidade, segurança, prevenção e limitação da conservação, em conformidade com a legislação aplicável.

11.7. Credenciais expostas, dados vazados e conteúdos sensíveis deverão ter acesso restrito aos usuários autorizados e às finalidades previstas na contratação.

11.8. Subcontratados deverão observar obrigações equivalentes de segurança, sigilo e proteção de dados, sem prejuízo da responsabilidade da PARCEIRA.

12. ARMAZENAMENTO, RETENÇÃO, BACKUP E CONTINUIDADE

12.1. A solução deverá manter armazenamento compatível com históricos, evidências, alertas, investigações, relatórios e auditoria.

12.2. A política de retenção deverá ser documentada e coerente com finalidade, criticidade e obrigações contratuais.

12.3. Expurgo e descarte deverão ser governados, rastreáveis e seguros, preservadas retenções determinadas pela InPACTA.

12.4. A PARCEIRA deverá manter backup, contingência, recuperação e testes de restauração dos componentes sob sua responsabilidade.

12.5. O plano de continuidade deverá contemplar indisponibilidade, perda de conectividade, comprometimento de credenciais e incidentes.

12.6. Dados, logs e históricos mínimos deverão permanecer acessíveis durante a

vigência e ser disponibilizados na transição.

13. INTEGRAÇÃO, ESCALABILIDADE E GOVERNANÇA

13.1. A arquitetura deverá ser modular, escalável e interoperável, permitindo ampliação sem perda de funcionalidades ou histórico.

13.2. A PARCEIRA deverá correlacionar informações, achados e evidências dos módulos para aprimorar detecção, priorização e tratamento.

13.3. CTI deverá subsidiar SOC e vulnerabilidades; CTEM/BAS deverá apoiar risco; e riscos de terceiros deverão integrar as análises pertinentes.

13.4. Integrações deverão possuir documentação, autenticação segura, tratamento de erros, registros e controle de versão.

13.5. Mudanças relevantes de arquitetura, integração, retenção ou licenciamento deverão seguir governança de mudanças.

13.6. A solução deverá evitar bases paralelas não governadas e dependências que prejudiquem rastreabilidade, portabilidade ou continuidade.

14. IMPLANTAÇÃO, CONFIGURAÇÃO, INTEGRAÇÃO E ACEITE

14.1. Reunião de abertura. Após a emissão da Ordem de Início, deverá ser realizada reunião de abertura para alinhamento do escopo, responsáveis, canais de comunicação, cronograma, riscos e acessos necessários.

14.2. Plano de implantação. A PARCEIRA deverá apresentar plano de implantação contendo etapas, dependências, integrações, testes, treinamento, marcos, critérios de aceite e procedimentos de reversão.

14.3. Gestão de acessos. Os acessos necessários à implantação e à operação deverão observar o princípio do menor privilégio e limitar-se ao estritamente necessário.

14.4. Execução da implantação. A implantação compreenderá, no mínimo, levantamento inicial, inventário, configuração, integração, testes, homologação, documentação e entrada controlada em produção.

14.5. Operação assistida. Após a ativação, deverá ocorrer período de operação assistida para estabilização da solução, correção de falhas e apoio aos usuários da InPACTA.

14.6. Aceite. O aceite poderá ocorrer por módulo ou etapa concluída, preservada a validação final do ecossistema integrado.

15. SUPORTE, MANUTENÇÃO, SLA E OPERAÇÃO ASSISTIDA

15.1. A PARCEIRA deverá disponibilizar canal de atendimento para recebimento, registro, acompanhamento, encaminhamento e encerramento de solicitações, incidentes, alertas, falhas e demais ocorrências relacionadas à solução.

15.2. As ocorrências deverão ser registradas de forma rastreável, contendo informações suficientes para sua identificação, classificação, acompanhamento das providências adotadas e encerramento.

15.3. A PARCEIRA deverá classificar as ocorrências, no mínimo, segundo sua criticidade, considerando o impacto operacional, a urgência, o risco cibernético e os ativos ou serviços envolvidos.

15.4. Os prazos de atendimento deverão ser compatíveis com a criticidade da ocorrência, observada, no mínimo, a seguinte referência:

CRITICIDADE	ATENDIMENTO INICIAL	ACOMPANHAMENTO
Crítica	Prioritário, em regime contínuo	Até a estabilização ou encaminhamento da ocorrência
Alta	Em prazo compatível com a urgência	Até a definição das providências necessárias
Média	Em prazo razoável	Conforme a necessidade de tratamento
Baixa	Conforme programação e prioridade	Conforme a necessidade de tratamento

15.5. As ocorrências críticas deverão receber tratamento prioritário, com escalonamento técnico ou gerencial quando necessário.

15.6. O suporte poderá compreender, conforme a natureza da ocorrência, diagnóstico, orientação técnica, recomendação de providências, tratamento de falhas, atualização, restauração, análise de causa e registro das ações realizadas.

15.7. As atividades de manutenção deverão buscar preservar a segurança, a continuidade dos serviços, a compatibilidade da solução, a integridade dos registros e o funcionamento das integrações aplicáveis.

15.8. Quando a solução de uma ocorrência depender de autorização, ação, acesso ou providência da InPACTA, de fornecedor ou de terceiro, a PARCEIRA deverá comunicar a situação, indicar as medidas recomendadas e acompanhar a ocorrência no âmbito de sua responsabilidade.

15.9. O desempenho dos serviços poderá ser acompanhado pela InPACTA com base em registros de atendimento, cumprimento dos prazos acordados, disponibilidade, qualidade do suporte, reincidência de ocorrências e pendências identificadas.

16. CAPACITAÇÃO TÉCNICO-OPERACIONAL E TRANSFERÊNCIA DE

CONHECIMENTO

16.1. A PARCEIRA deverá realizar ações de capacitação técnico-operacional compatíveis com a solução fornecida e com os perfis dos usuários, gestores e profissionais indicados pela InPACTA.

16.2. A capacitação deverá abranger, conforme aplicável, a utilização das plataformas, a consulta e o tratamento de alertas, indicadores, relatórios, fluxos de atendimento, procedimentos de escalonamento, perfis de acesso e integrações relacionadas à solução.

16.3. A PARCEIRA deverá disponibilizar materiais de apoio compatíveis com as ações realizadas, tais como guias, manuais, orientações, apresentações ou outros registros necessários à adequada utilização da solução.

16.4. As atualizações, alterações ou funcionalidades relevantes introduzidas na solução deverão ser acompanhadas, quando necessário, de orientação complementar à InPACTA.

16.5. A transferência de conhecimento deverá ocorrer de forma contínua durante a execução da parceria, especialmente por meio das interações de suporte, reuniões técnicas, orientações operacionais e disponibilização de documentação aplicável.

16.6. Ao término do contrato ou em caso de transição, a PARCEIRA deverá prestar apoio razoável à transferência dos conhecimentos, documentos, registros e informações necessários à continuidade da operação pela InPACTA ou por quem esta indicar.

17. QUALIFICAÇÃO TÉCNICA, EQUIPE E CAPACIDADE OPERACIONAL

17.1. A interessada deverá demonstrar capacidade técnica compatível com o objeto, especialmente para implantação, integração, operação e suporte de serviços contínuos de cibersegurança, incluindo, conforme aplicável, monitoramento de segurança, gestão de vulnerabilidades, hardening, inteligência de ameaças cibernéticas, gestão contínua de exposição, simulação de violações e ataques, risco de terceiros e integrações com ferramentas da InPACTA.

17.2. A comprovação técnico-operacional deverá ocorrer mediante atestado(s) emitido(s) por pessoa jurídica de direito público ou privado, em nome da interessada, que permitam verificar autenticidade, objeto, período de execução, escopo, quantitativos quando aplicáveis, complexidade, suporte, níveis de serviço e evidências de aceite ou execução satisfatória.

17.3. A compatibilidade da experiência será examinada pela correlação entre objeto, ambientes, complexidade, continuidade, integração e resultados comprovados, sem adotar um volume geral de ativos como mínimo de atestado. A capacidade funcional

e a metodologia de dimensionamento por cliente serão comprovadas nos termos das matrizes, sem presumir que a retirada de quantitativos dispensa evidência material.

17.4. Os atestados deverão demonstrar experiência objetiva em serviços compatíveis com o núcleo técnico-operacional do objeto, incluindo, conforme aplicável, descoberta e monitoramento de ativos externos, identificação e tratamento de vulnerabilidades ou exposições, geração de alertas, análise de riscos, relatórios técnicos, acompanhamento de providências e retestes, não sendo suficiente documentação genérica.

17.5. A interessada deverá dispor de equipe técnica com capacidade compatível para implantação, integração, administração, operação, suporte e manutenção dos serviços e plataformas ofertados, abrangendo, conforme aplicável, gestão de cibersegurança, tratamento de alertas e incidentes, vulnerabilidades, hardening, CTI, gestão de exposição, risco de terceiros e integrações de segurança. A equipe considerada na pontuação deverá guardar proporcionalidade com a equipe efetivamente alocada na execução, preservadas a capacidade e as responsabilidades demonstradas.

17.6. Para fins de qualificação técnica da proposta, a interessada deverá apresentar declaração de atendimento aos requisitos técnicos deste Anexo, acompanhada de documentação técnica suficiente para subsidiar a análise da solução ofertada.

17.7. A comprovação complementar de adoção, maturidade ou reconhecimento de mercado da solução CTI observará os itens 7.12.1 a 7.12.3, admitidas fontes independentes e evidências equivalentes, sem constituir requisito eliminatório autônomo.

17.7.1. A ausência de reconhecimento por instituição específica não impedirá a qualificação quando os requisitos técnicos, funcionais, operacionais e de segurança forem comprovados pelos meios previstos neste Anexo. A evidência de reconhecimento de mercado será identificada como RF-C-028 no Anexo III, de natureza complementar e peso zero.

17.7.2. O relatório SOC 2 Tipo II ou mecanismo equivalente de avaliação independente constitui demonstração contratual posterior dos controles de segurança e proteção de dados, a ser apresentada antes do início do tratamento de informações de inteligência cibernética em produção. Na seleção, sua apresentação é complementar, admitida equivalência, sem barreira de participação ou efeito eliminatório autônomo.

17.7.3. O RCO-004 fica suprimido da avaliação, inclusive quanto à exigência de escala de adoção e aos seus 7 pontos. Permanecem 10 requisitos operacionais ativos, dos quais 3 eliminatórios, com pesos brutos que somam 93 pontos. A nota operacional será normalizada para a escala de 0 a 100 pela fórmula $NO = (\text{soma dos$

pontos operacionais validados / 93) × 100, com corte de 70 pontos normalizados e contribuição de até 25 pontos ao VTI. Os demais pesos relativos e os requisitos eliminatórios ficam preservados.

17.7.4. A apuração documental da nota funcional, a normalização do atendimento obtido por configuração ou integração e o tratamento dos resultados processuais da PoC observarão os itens 19.1.1, 19.1.2 e 19.6.1 a 19.8 do Edital, os itens 6.7.1 a 6.7.3 do Anexo II e o item 7.6 do Anexo V. O meio de implementação não reduz a nota quando o atendimento integral estiver efetivamente comprovado.

17.8. As soluções ofertadas serão submetidas à Prova de Conceito – PoC, de caráter eliminatório, conforme o Anexo específico, devendo atender integralmente aos requisitos obrigatórios e alcançar a pontuação mínima exigida.

17.8.1. O não atendimento de requisito obrigatório ou a não obtenção da pontuação mínima implicará a não qualificação técnica da proposta.

17.8.2. A PoC não acrescentará pontos ao VTI nem constituirá critério autônomo de desempate. A evidência que infirmar materialmente pontuação documental ensejará revisão motivada dos pontos afetados, com manifestação, recursos e reapuração da NF e da ordem do VTI, conforme o item 25.6 e seus subitens do Edital. Permanecem o atendimento integral dos eliminatórios e o corte de 70 pontos. A perda de pontos em requisito exclusivamente pontuável não cria eliminação autônoma. A convocação sucessiva observará a ordem vigente e o item 26.3.1 do Edital.

18. DOCUMENTAÇÃO TÉCNICA E COMPROVAÇÕES OBRIGATÓRIAS

18.1. A interessada deverá apresentar matriz de atendimento que relacione cada requisito técnico previsto neste Anexo ao módulo, serviço ou componente ofertado, à evidência apresentada e à respectiva forma de validação.

18.2. A interessada deverá apresentar documentação técnica suficiente para comprovar o atendimento aos requisitos da solução ofertada, incluindo, conforme aplicável:

18.2.1. datasheets, manuais, guias técnicos, documentos de arquitetura, especificações técnicas, white papers, portais oficiais ou documentação equivalente emitida pelo fabricante, desenvolvedor, provedor ou responsável pela solução;

18.2.2. identificação dos módulos, serviços, licenças, subscrições, conectores, integrações e demais componentes necessários ao funcionamento integral da solução, incluindo produto, versão, capacidade, vigência e métrica de licenciamento, quando aplicável;

18.2.3. documentação de integração por API, conectores, webhooks, protocolos ou mecanismos equivalentes, quando previstos fluxos com ferramentas ou sistemas da

InPACTA; e

18.2.4. documentação relativa aos requisitos de segurança da solução, incluindo, quando aplicável, autenticação, perfis de acesso, registros de auditoria, criptografia, proteção de dados, atualização e tratamento de vulnerabilidades.

18.3. A comprovação de requisito essencial não poderá fundamentar-se exclusivamente em material publicitário, apresentação comercial, declaração genérica, mera reprodução textual dos requisitos ou promessa de desenvolvimento futuro, devendo estar amparada por documentação técnica oficial ou por evidência técnica verificável.

18.4. Toda funcionalidade ou requisito declarado deverá possuir forma objetiva de comprovação e validação, conforme a matriz de atendimento, mediante documentação técnica, demonstração funcional, Prova de Conceito – PoC, aceite técnico ou verificação durante a execução da parceria, quando aplicável.

18.5. Eventuais divergências, omissões ou inconsistências identificadas na documentação poderão ser objeto de diligência pela InPACTA, sem que isso implique substituição indevida da solução originalmente ofertada ou alteração de suas características essenciais.

19. PROVA DE CONCEITO, TESTES E VALIDAÇÃO TÉCNICA

19.1. A Prova de Conceito – PoC verificará, de forma objetiva, padronizada, rastreável e documentada, os requisitos técnicos, funcionais, operacionais, de integração e segurança expressamente previstos na matriz funcional constante do Anexo III, observados os procedimentos operacionais da PoC previstos no Anexo V. O roteiro aprovado e divulgado com o Edital identificará requisitos e subitens, procedimentos, massa representativa, evidências e critérios, distinguindo a demonstração da execução contratual, sem exigência nova na convocação.

19.1.1. A matriz funcional constante do Anexo III deverá identificar, para cada requisito avaliado, sua classificação como eliminatório, pontuável ou complementar, a evidência esperada, a forma de validação, a pontuação aplicável e a consequência decorrente de seu não atendimento.

19.1.2. Em caso de divergência entre o roteiro, a matriz e os demais documentos relacionados à PoC, prevalecerão os critérios e as regras expressamente estabelecidos na matriz funcional constante do Anexo III, observada a prevalência técnica do Anexo I e o caráter procedimental do Anexo V. Os efeitos procedimentais da revisão de pontuação observarão o item 25.6 do Edital e o item 17.8.2 deste Anexo, sem alteração dos pesos ou dos cortes.

19.1.3. O não atendimento de requisito obrigatório implicará reprovação na PoC,

independentemente da pontuação obtida nos demais critérios, observados os critérios do Anexo III e os procedimentos definidos no Anexo V.

19.2. Não será admitida substituição de módulo essencial, promessa de desenvolvimento ou integração posterior para requisito obrigatório.

19.3. A autodeclaração apenas organizará informações; caberá à Comissão Técnica validar cada requisito.

19.4. Apresentações comerciais, vídeos, folders ou declarações genéricas não serão suficientes isoladamente.

19.5. A PoC deverá utilizar ambiente controlado, vedado o uso de dados reais sem autorização.

19.5.1. A autorização deverá ser prévia, expressa e escrita, emitida pelo titular ou responsável competente pelo sistema, com escopo, janela e regras de engajamento delimitados. A validação de credenciais expostas fica restrita aos sistemas expressamente autorizados, vedada a interação com ambientes de terceiros não autorizados. As regras de engajamento integrarão o roteiro aprovado e a autorização do titular será juntada aos autos antes de cada sessão que envolva esses testes.

19.6. Os testes não poderão provocar indisponibilidade, alteração indevida ou interação não autorizada.

19.7. A Comissão elaborará relatório circunstanciado com solução, módulos, requisitos, evidências, diligências e conclusão. Havendo revisão de pontuação, serão preservados os registros anteriores e indicados os pontos afetados, a motivação, a decisão e a ordem recalculada.

20. TRANSIÇÃO, PORTABILIDADE E ENCERRAMENTO

20.1. A PARCEIRA deverá executar plano de transição destinado a preservar continuidade, portabilidade, histórico e segurança.

20.2. A transição incluirá inventários, configurações, casos, alertas, evidências, indicadores, relatórios, auditoria, integrações e documentação.

20.3. Os dados serão fornecidos em formatos estruturados, abertos ou amplamente utilizados, acompanhados de documentação.

20.4. A PARCEIRA apoiará transferência de conhecimento, revogação de credenciais e desativação segura de integrações.

20.5. Após o encerramento e observadas retenções aplicáveis, cópias remanescentes deverão ser eliminadas ou tornadas inacessíveis.

21. CRITÉRIOS GERAIS DE ACEITE DA SOLUÇÃO

21.1. O aceite da solução dependerá da verificação objetiva de aderência ao objeto,

aos requisitos técnicos e funcionais, à documentação apresentada, aos resultados da PoC, quando aplicável, e aos critérios definidos no contrato.

21.2. O aceite deverá considerar, no mínimo:

21.2.1. funcionamento dos módulos, serviços, licenças, integrações, acessos e demais componentes contratados;

21.2.2. atendimento aos critérios de dimensionamento por cliente, capacidades, entregáveis e parâmetros previstos;

21.2.3. conformidade dos relatórios, registros, documentação técnica, operacional e de integração exigidos;

21.2.4. realização das etapas aplicáveis de implantação, configuração, testes, homologação, capacitação e operação assistida;

21.2.5. correção ou tratamento das pendências e não conformidades identificadas; e

21.2.6. inexistência de falha crítica ou pendência impeditiva à utilização adequada da solução.

21.3. O aceite poderá ocorrer por módulo, serviço, etapa, entrega, ordem de serviço ou período de medição, desde que mantida a rastreabilidade entre escopo, execução, evidências, validação e faturamento.

21.4. As pendências deverão ser registradas com descrição, criticidade, responsável, prazo para tratamento e condição de encerramento.

21.5. O aceite provisório não afasta a obrigação de correção das pendências identificadas durante a operação assistida.

21.6. O aceite definitivo dependerá da correção das pendências impeditivas e da comprovação do atendimento aos requisitos aplicáveis.

21.7. Declarações de atendimento ou apresentações comerciais não substituirão evidências, documentação, testes, demonstrações ou outros meios objetivos de verificação.

22. RELATÓRIOS, INDICADORES E GOVERNANÇA DOS RESULTADOS

22.1. A PARCEIRA deverá disponibilizar, durante a execução da parceria, alertas, notificações, registros de atendimento, evidências, recomendações e informações sobre pendências relacionadas aos serviços prestados.

22.2. Mensalmente, a PARCEIRA deverá apresentar relatório técnico e executivo consolidado, contendo, conforme aplicável, indicadores, riscos, vulnerabilidades, exposições, informações de inteligência, incidentes, ações realizadas, pendências e recomendações.

22.3. A identificação de incidente relevante deverá ser comunicada à InPACTA com a prioridade compatível com sua criticidade, com base no SLA, devendo ser

apresentado, quando aplicável, relatório técnico contendo linha do tempo, evidências disponíveis, análise realizada, medidas adotadas e recomendações.

22.4. Os indicadores deverão permitir o acompanhamento, no mínimo, de volume, criticidade, tendência, recorrência, tratamento, disponibilidade, cumprimento de níveis de serviço e efetividade das ações adotadas.

22.5. As reuniões de governança deverão registrar participantes, temas tratados, decisões, responsáveis, prazos, riscos, pendências e plano de ação, quando aplicável.

22.6. Os relatórios, indicadores, alertas e registros apresentados deverão ser rastreáveis às respectivas fontes, registros operacionais e evidências que lhes deram origem.

23. SUSTENTABILIDADE TECNOLÓGICA, OBSOLESCÊNCIA E CICLO DE SUPORTE

23.1. Não poderão ser utilizados produtos ou versões sem suporte ativo quando isso comprometer segurança ou continuidade.

23.2. A PARCEIRA deverá comunicar descontinuidade, fim de suporte, mudança de licenciamento ou impacto relevante.

23.3. Substituições deverão preservar ou ampliar funcionalidades, integrações, segurança, desempenho, histórico e direitos.

23.4. Atualizações deverão ser planejadas, testadas e documentadas.

23.5. A PARCEIRA manterá capacidade de correção, atualização, suporte e continuidade durante a vigência.

24. OBRIGAÇÕES TÉCNICAS ESSENCIAIS

24.1. Constituem obrigações da PARCEIRA:

I – disponibilizar, manter e operar serviços, plataformas, módulos e funcionalidades;

II – implantar, parametrizar, integrar, atualizar, suportar e operar assistidamente;

III – emitir relatórios, alertas, notificações, evidências e entregáveis;

IV – comunicar eventos críticos, incidentes e vulnerabilidades prioritárias;

V – manter sigilo, segurança, proteção de dados e rastreabilidade;

VI – capacitar a equipe indicada;

VII – manter equipe, licenças, suporte e capacidade operacional;

VIII – corrigir falhas e não conformidades sob sua responsabilidade;

IX – cooperar com a fiscalização; e

X – executar transição, portabilidade e encerramento assistido.

24.2. Constituem obrigações técnicas da InPACTA:

- I – designar gestores, fiscais e pontos focais;
- II – fornecer informações, acessos, inventários e autorizações necessários;
- III – acompanhar a execução, analisar entregáveis e comunicar inconsistências;
- IV – decidir sobre alterações, contenções, bloqueios e correções sob sua competência; e
- V – comunicar limitações ou dependências que afetem a execução.

25. DIRETRIZ FINAL DE INTEGRIDADE

25.1. Os documentos e instrumentos da contratação deverão manter coerência entre objeto, requisitos, critérios de dimensionamento por cliente, licenciamento, proposta, PoC, entregáveis, níveis de serviço, medição, aceite, pagamento e obrigações das partes.

25.2. Não será admitido tratamento isolado de requisitos ou componentes que comprometa a integração da solução, a interoperabilidade, a segurança, a rastreabilidade, a continuidade dos serviços ou a responsabilidade da PARCEIRA pelo objeto.

25.3. Toda funcionalidade declarada deverá possuir comprovação documental, forma objetiva de validação e correspondência com a solução efetivamente ofertada e disponibilizada.

25.4. Inconsistências materiais entre proposta, documentação, atestados, licenças, demonstrações, PoC e execução da parceria deverão ser registradas, avaliadas e tratadas pela PARCEIRA, sem prejuízo das medidas cabíveis pela InPACTA.

25.5. Soluções, componentes ou funcionalidades equivalentes ou superiores poderão ser admitidos desde que comprovem integralmente o atendimento aos requisitos exigidos e não contrariem requisitos específicos de caráter obrigatório previstos neste Anexo.

Maringá/PR, 09 de outubro de 2026.



Documento assinado eletronicamente por **Cristiane Regina de Camargo Hasegawa**, **Diretor(a)-Presidente do INPACTA**, em 09/10/2026, às 18:03, conforme horário oficial de Brasília, com fundamento na [Medida Provisória nº 2200-2, de 24 de agosto de 2001](#) e [Decreto Municipal nº 871, de 7 de julho de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.maringa.pr.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **9823696** e o código CRC **B1CBB152**.

