



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 VI - MINUTA DO INSTRUMENTO DE PARCERIA SOLUÇÃO INTEGRADA PARA CIBERSEGURANÇA

1. DEFINIÇÕES

1.1. Aplicam-se a este Instrumento e aos demais anexos o glossário comum do item 1.1 do Edital e as definições técnicas complementares desta cláusula, sem ampliação do público-alvo ou do objeto.

1.2. **CLIENTE:** órgão ou entidade integrante da Administração Pública direta ou indireta, incluindo consórcio público com personalidade de direito público, destinatário de implementação identificada em instrumento executivo. Não abrange serviços sociais autônomos nem consórcios de direito privado ou outros entes privados não integrantes da Administração Pública. O instrumento executivo definirá a base jurídica da relação, o escopo, as responsabilidades, os recursos, os prazos, a medição, o aceite e as condições econômicas.

1.3. **PARCEIRA:** pessoa jurídica de direito privado selecionada no Chamamento Público correspondente e signatária deste Instrumento, responsável pelas obrigações técnicas, operacionais, documentais, funcionais, comerciais, de licenciamento, suporte, segurança, sustentação, transição e demais encargos atribuídos.

1.4. **PARTES:** o InPACTA e a PARCEIRA, reciprocamente considerados.

1.5. **SOLUÇÃO INTEGRADA PARA CIBERSEGURANÇA:** iniciativa institucional destinada à prevenção, identificação, monitoramento, análise, validação e mitigação contínua de ameaças e riscos cibernéticos no ambiente do CLIENTE, mediante plataformas interoperáveis, serviços técnicos especializados, governança, inteligência, automação, relatórios, evidências e sustentação continuada.

1.6. **SOLUÇÃO INTEGRADA:** ecossistema único, modular, escalável e interoperável composto pelos cinco módulos definidos no ANEXO I – ESPECIFICAÇÃO DO OBJETO, incluindo implantação, parametrização, integração, operação assistida,

suporte, manutenção, atualização, treinamento, relatórios e continuidade.

1.7. EVIDÊNCIAS DIGITAIS: logs, trilhas de auditoria, relatórios, indicadores, capturas de tela, arquivos exportados, painéis, registros de sistema, alertas, tickets, recomendações, validações, eventos e demais elementos aptos a comprovar fato técnico-operacional relevante.

1.8. INFORMAÇÕES SIGILOSAS: informações técnicas, operacionais, comerciais, institucionais, estratégicas, documentais ou digitais fornecidas, acessadas ou produzidas no contexto da parceria, inclusive dados de arquitetura, ativos, vulnerabilidades, credenciais, logs, incidentes, evidências, indicadores, relatórios, superfícies de ataque, inteligência de ameaças e dados pessoais.

1.9. ORDEM DE SERVIÇO: instrumento operacional de acionamento, detalhamento, autorização, execução, acompanhamento e validação de entrega específica vinculada ao objeto.

1.10. PROVA DE CONCEITO – PoC: procedimento objetivo de demonstração, teste, validação e registro técnico da solução ou de parte dela, conforme roteiro, critérios e evidências definidos nos documentos do procedimento.

1.11. SUPORTE ESPECIALIZADO: suporte técnico prestado pela PARCEIRA para diagnóstico, correção, atualização, integração, restabelecimento, orientação técnica, documentação, evidências de atendimento, solução, contorno e encerramento técnico.

1.12. DADOS OPERACIONAIS: registros, metadados, eventos, logs, indicadores, relatórios, inventários, evidências, históricos, métricas, painéis e demais dados produzidos, coletados, processados ou disponibilizados pela solução.

1.13. 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.

1.14. EVENTO DE SEGURANÇA: ocorrência observável com possível relevância para a segurança.

1.15. ALERTA DE SEGURANÇA: evento ou conjunto de eventos selecionado para triagem por regra, correlação, comportamento, indicador ou contexto de risco.

1.16. INCIDENTE DE SEGURANÇA: ocorrência confirmada ou provável capaz de comprometer confidencialidade, integridade, disponibilidade, autenticidade ou continuidade.

1.17. VULNERABILIDADE: fragilidade técnica, operacional ou de configuração que possa ser explorada ou contribuir para a materialização de risco.

1.18. ACHADO DE SEGURANÇA: resultado de varredura, pentest, CTEM, BAS, CTI, SOC, TPRM ou analista digital, acompanhado das evidências disponíveis.

1.19. EVIDÊNCIA TÉCNICA: registro verificável que sustente alerta, achado,

vulnerabilidade, incidente ou conclusão técnica.

1.20. IOC: artefato técnico associado a atividade maliciosa ou potencial comprometimento.

1.21. TTPs: padrões de comportamento utilizados por agentes de ameaça em operações cibernéticas.

1.22. TERCEIRO MONITORADO: fornecedor, prestador, parceiro ou organização cuja exposição possa representar risco ao CLIENTE.

1.23. OPERAÇÃO ASSISTIDA: etapa posterior à implantação destinada à estabilização, à correção de falhas e ao apoio aos usuários.

2. OBJETO

2.1. O objeto deste Instrumento é a associação de esforços entre as PARTES, em regime de cooperação técnica, operacional, institucional e comercial, para disponibilização, implantação, parametrização, integração, operação assistida, suporte técnico, sustentação, atualização, evolução e continuidade da solução integrada, definida na cláusula 1.6, no âmbito da SOLUÇÃO INTEGRADA PARA CIBERSEGURANÇA, conforme o Edital, o ANEXO I – ESPECIFICAÇÃO DO OBJETO, os demais Anexos, a proposta técnica aprovada e os instrumentos executivos formalizados.

2.2. 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.

2.3. O escopo compreende, no mínimo: I – Módulo 1: segurança ofensiva autorizada, gestão de vulnerabilidades, hardening e SOC 24x7; II – Módulo 2: gestão contínua da exposição a ameaças e simulação de violação e ataque – CTEM/BAS; III – Módulo 3: gerenciamento de risco cibernético de terceiros – TPRM; IV – Módulo 4: inteligência de ameaças cibernéticas – CTI; e V – Módulo 5: analistas cibernéticos digitais baseados em inteligência artificial.

2.4. Integram o escopo a implantação, configuração, integração, licenciamento, treinamento, operação assistida, suporte, manutenção, relatórios, evidências, governança, portabilidade e encerramento assistido necessários ao funcionamento integral.

2.5. 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.

2.6. O Módulo 1 será prestado de forma contínua, com SOC em regime 24x7x365 e ciclos mensais de gestão de vulnerabilidades, testes de intrusão autorizados e recomendações de hardening. Retestes e validações de correções ocorrerão sob demanda, observado o mínimo bimestral, após comunicação de remediação e conforme criticidade, disponibilidade do ambiente e regras de engajamento.

2.7. Nenhum módulo, licença, integração, serviço ou entrega poderá ser tratado isoladamente quando sua operação depender do ecossistema principal, cabendo à PARCEIRA assegurar o fluxo integrado de identificação, validação, inteligência, monitoramento, priorização, resposta e reporte.

2.8. Qualquer exploração controlada, teste intrusivo, validação de credencial ou ação capaz de alterar, bloquear, isolar, excluir, revogar ou impactar ativos dependerá de autorização da entidade responsável pelo ambiente, ressalvado playbook expressamente aprovado. 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.

2.9. Toda funcionalidade declarada deverá possuir documentação, forma objetiva de comprovação, evidência técnica e possibilidade de validação prática, quando aplicável.

3. NATUREZA ASSOCIATIVA DA PARCERIA

3.1. O presente Instrumento possui natureza associativa, técnico-institucional, operacional e não societária, celebrado em regime de cooperação para estruturação, disponibilização, operação, evolução e inserção institucional da oportunidade de negócio relativa à SOLUÇÃO INTEGRADA PARA CIBERSEGURANÇA.

3.2. A parceria não implica constituição de pessoa jurídica distinta, sociedade, consórcio societário, solidariedade empresarial automática, vínculo trabalhista entre as equipes das PARTES ou transferência de direitos não prevista expressamente.

3.3. A assinatura não garante resultado comercial, volume mínimo de CLIENTES, demanda mínima, receita mínima, exclusividade de mercado ou contratação automática da solução.

3.4. A ausência de garantia comercial não afasta a obrigação da PARCEIRA de cumprir os resultados técnicos, operacionais, documentais, de segurança, suporte,

licenciamento, transição e continuidade assumidos nos instrumentos aplicáveis.

3.5. A execução financeira, quando houver, dependerá de instrumento específico que estabeleça a obrigação correspondente.

4. REGIME JURÍDICO, FUNDAMENTAÇÃO E VINCULAÇÃO

4.1. Este Instrumento observará a Regulamentação DIR_EXEC/InPACTA nº 001/2025 e o respectivo Regulamento Interno de Parcerias para Oportunidades de Negócios, a Lei Complementar Municipal nº 1.503/2025, a Lei nº 13.303/2016 na extensão adaptada prevista nos arts. 1º e 2º do Regulamento, os preceitos de Direito Privado, a Lei nº 13.709/2018 e a legislação anticorrupção aplicável. A Lei nº 14.133/2021 não constitui regime subsidiário automático desta parceria.

4.2. Integram este Instrumento, independentemente de transcrição, o Edital, o ANEXO I – ESPECIFICAÇÃO DO OBJETO, o ANEXO II – QUALIFICAÇÃO DAS PROPOSTAS, os Anexos III, IV e V relativos à qualificação e à PoC, o ANEXO VII – CHECKLIST DE APRESENTAÇÃO DA PROPOSTA, a proposta técnica aprovada, a matriz de licenciamento, os planos operacionais e as ordens de serviço. A matriz de riscos definitiva, aprovada e anexada antes da assinatura, integra o contrato nos termos do art. 27, § 2º, do Regulamento.

4.3. Os documentos integrantes vinculam as PARTES quanto ao objeto, requisitos, comprovações, critérios de dimensionamento por cliente, licenciamento, PoC, execução, medição, aceite e transição.

4.4. Em matéria técnica específica, prevalecerá o requisito mais aderente ao objeto constante do ANEXO I, sem prejuízo da coerência com o Edital e a proposta aprovada.

4.5. A proposta técnica aprovada não poderá reduzir, restringir, condicionar, substituir ou excluir obrigação mínima prevista no Edital, nos Anexos ou neste Instrumento.

4.6. Em caso de divergência técnica, prevalecerá o ANEXO I; matérias jurídicas, administrativas, econômico-financeiras e procedimentais observarão o Edital, este Instrumento e os instrumentos específicos aplicáveis.

5. CONDIÇÕES PRÉVIAS À FORMALIZAÇÃO, REGULARIDADE E

MANUTENÇÃO DAS CONDIÇÕES DE QUALIFICAÇÃO

5.1. A formalização ficará condicionada à homologação do procedimento, à regularidade documental da PARCEIRA e à apresentação das certidões, declarações e comprovações exigidas no Edital e no ANEXO II. Antes da assinatura, a Procuradoria Jurídica conferirá por checklist as certidões válidas e os extratos

dados das consultas ao CEIS, CNEP e cadastros complementares previstos no Edital, inclusive quanto aos terceiros relevantes. A assinatura também depende da deliberação do Conselho de Administração e da aprovação do Plano de Negócio Detalhado. Antes da assunção de obrigações operacionais permanentes, deverá estar documentado o dimensionamento da capacidade interna do InPACTA.

5.2. A PARCEIRA deverá manter durante a vigência as condições de qualificação, regularidade e ausência de impedimentos exigidas no procedimento.

5.3. A documentação técnica da solução deverá permanecer compatível com os produtos, edições, módulos, licenças, integrações, equipe e serviços efetivamente disponibilizados.

5.4. Alteração relevante das condições declaradas deverá ser comunicada formalmente ao InPACTA.

5.5. A seleção e a homologação da PARCEIRA decorrem exclusivamente do Valor Técnico-Institucional – VTI, da PoC, da integridade e da análise jurídica, sem proposta, qualificação ou validação econômico-financeira. Condições financeiras de eventual implementação futura não alteram nem revalidam a classificação.

5.6. O instrumento definitivo conterá condição resolutiva para a perda superveniente de condição de qualificação exigida no procedimento, observadas a apuração, a comunicação escrita, a defesa e a decisão motivada previstas nas cláusulas 31 e 34. A aplicação não dispensa as medidas de continuidade, portabilidade e transição.

6. VIGÊNCIA, PRAZO DE EXECUÇÃO E PRORROGAÇÃO MOTIVADA

6.1. A vigência inicial, o marco de início e os períodos de execução serão definidos no instrumento definitivo após aprovação do Plano de Trabalho Técnico-Institucional e da análise jurídica, sem adoção automática de prazo extraído de regime jurídico diverso. Eventual obrigação financeira dependerá de instrumento específico posterior e não condicionará a seleção. O Plano de Negócio Detalhado, aprovado pela instância competente antes da assinatura definitiva, fixará vigência, prorrogação, reajuste, remuneração e forma de repasse, sem modificar a ordem do VTI.

6.2. Cada implementação deverá distinguir os prazos de diagnóstico, implantação, integração, operação assistida, serviços recorrentes, transição e encerramento, com marcos, dependências e critérios de aceite próprios.

6.3. A natureza continuada de determinadas capacidades de cibersegurança não cria, por si só, prazo máximo, renovação automática, garantia de demanda ou obrigação de permanência.

6.4. A duração deverá ser motivada pela necessidade institucional, pelo ciclo tecnológico, pelo licenciamento, pela implantação, pela segurança, pelo

desempenho, pela obsolescência, pela sustentabilidade econômica e pelas condições de transição.

6.5. Eventual prorrogação dependerá de previsão no instrumento definitivo, manifestação técnica, econômica e jurídica e autorização da autoridade competente, sem direito adquirido da PARCEIRA.

6.6. A análise de eventual prorrogação deverá demonstrar, no mínimo:

- I – a permanência do interesse institucional e da demanda efetivamente formalizada;
- II – o desempenho satisfatório e o cumprimento das obrigações, dos níveis de serviço e dos resultados;
- III – a compatibilidade do escopo, das capacidades, do licenciamento e dos recursos com os instrumentos executivos vigentes;
- IV – a sustentabilidade econômica e a compatibilidade das condições com referências contemporâneas de mercado;
- V – a disponibilidade dos recursos e das aprovações exigidas para o período;
- VI – a manutenção da segurança, da proteção de dados, da continuidade e da portabilidade;
- VII – a atualização tecnológica e a inexistência de obsolescência ou descontinuidade impeditiva;
- VIII – a adequação da matriz de riscos e das responsabilidades;
- IX – a inexistência de renovação automática ou garantia de demanda; e
- X – a autorização expressa da autoridade competente.

6.7. A previsão de vigência ou prorrogação não obriga o InPACTA ou qualquer CLIENTE a acionar serviços, manter volumes ou celebrar instrumentos executivos.

6.8. Alterações de prazo, escopo ou condições dependerão de instrumento formal, motivação e preservação da coerência com o Plano de Negócio Detalhado e com as implementações vigentes.

6.9. Índice, data-base, periodicidade e método de atualização econômica somente poderão ser aplicados se definidos no modelo econômico aprovado e reproduzidos no instrumento correspondente.

6.10. Não se presume a adoção de IPCA, reajuste anual ou mecanismo equivalente. A solução aprovada deverá guardar pertinência com a estrutura real de custos e com o regime jurídico aplicável.

6.11. Revisão ou recomposição econômica dependerá dos pressupostos, da documentação, da análise e da aprovação previstos no instrumento aplicável, vedada a duplicidade de remuneração.

7. OBRIGAÇÕES COMUNS DAS PARTES

- 7.1. Atuar com cooperação, boa-fé, transparência, integridade e lealdade institucional.
- 7.2. Observar o Edital, os Anexos, a proposta aprovada, os planos, as ordens de serviço e os instrumentos específicos.
- 7.3. Preservar rastreabilidade de decisões, comunicações, entregas, ocorrências, validações, aceites, recusas e medidas corretivas.
- 7.4. Observar confidencialidade, segurança da informação, proteção de dados e finalidade dos acessos.
- 7.5. Comunicar fatos que possam afetar execução, continuidade, segurança, licenciamento, dados, evidências ou disponibilidade.
- 7.6. Responder por seus atos, omissões, pessoal e terceiros mobilizados, nos limites das obrigações assumidas.
- 7.7. Cooperar para que a execução preserve a continuidade dos serviços públicos, sem transferência à PARCEIRA das decisões administrativas e técnicas reservadas ao InPACTA, ao CLIENTE ou ao responsável pelo ambiente.

8. OBRIGAÇÕES EXCLUSIVAS DA PARCEIRA

- 8.1. Disponibilizar, implantar, parametrizar, integrar, manter, suportar e evoluir a solução em conformidade com o objeto.
- 8.2. Assegurar compatibilidade, interoperabilidade e responsabilidade técnica unificada dos cinco módulos, inclusive quando houver fabricantes, provedores, integradores ou subcontratados.
- 8.3. Manter licenças, acessos, APIs, conectores, armazenamento, suporte e direitos suficientes ao escopo e aos entregáveis efetivamente autorizados em cada instrumento executivo, com dimensionamento documentado antes da execução.
- 8.4. Executar o SOC 24x7x365 e os ciclos mensais do Módulo 1, comunicando imediatamente vulnerabilidades críticas, indícios de exploração ativa, incidentes ou riscos urgentes.
- 8.5. Manter CTEM/BAS, TPRM, CTI e analistas digitais com as funcionalidades e condições técnicas do ANEXO I, conforme dimensionamento e licenciamento definidos para cada cliente.
- 8.6. Emitir relatórios técnicos e executivos, alertas, recomendações, evidências, trilhas de auditoria e registros de atendimento.
- 8.7. Adotar controles de segurança, sigilo, proteção de dados, segregação de acesso, rastreabilidade, retenção e descarte governado.
- 8.8. Prestar suporte, manutenção corretiva, preventiva, adaptativa e evolutiva, atualizações, patches e correções necessários à continuidade.

8.9. Capacitar os usuários indicados, manter documentação atualizada e transferir conhecimento.

8.10. Corrigir falhas e não conformidades sob sua responsabilidade e executar transição, portabilidade e encerramento assistido.

8.11. Não realizar ação intrusiva ou de impacto sem autorização e respeitar as regras de engajamento aprovadas.

8.12. Manter supervisão humana sobre resultados e ações de inteligência artificial conforme o ANEXO I.

8.13. Executar, no Módulo 1, a identificação, validação, classificação, priorização, recomendação de tratamento, acompanhamento e reteste dos achados, com relatórios mensais de vulnerabilidades, impacto e risco, evolução das correções, painel de acompanhamento e relatório formal do SOC, sem prejuízo de comunicações imediatas para riscos críticos e incidentes relevantes.

8.14. No CTEM/BAS, manter descoberta e inventário dinâmicos da superfície externa, monitoramento contínuo, validações controladas e não invasivas, evidências, painéis, notificações, exportações e integração aos fluxos de tratamento, com escopo dimensionado por cliente e observância das regras de engajamento.

8.15. No TPRM, disponibilizar plataforma SaaS com interface web e API RESTful para cadastramento, classificação, monitoramento e avaliação de terceiros, com acessos autorizados, perfis administrativos, questionários de conformidade, avaliação de exposição, alertas e relatórios de risco. A abrangência e os recursos serão dimensionados no instrumento executivo de cada cliente.

8.16. No CTI, disponibilizar acessos, monitoramentos, consultas, objetos, marcas, mapeamentos e apoio a solicitações de remoção com as funcionalidades do item 7.13 do ANEXO I e o dimensionamento previsto na cláusula 2.5 deste Instrumento, com inteligência contextualizada, evidências, trilha de auditoria, monitoramento, investigação, panorama de ameaças, inteligência técnica, atores de ameaça, proteção de identidade e de marca, IOCs e mapeamento de infraestrutura maliciosa.

8.17. Pesquisas direcionadas, análises especiais, RFIs, inclusão de novas fontes, sandbox e apoio a takedown somente serão executados quando previstos ou formalmente acionados, com escopo, prazo, entregáveis, viabilidade, legalidade, segurança e condições aplicáveis definidos no instrumento correspondente.

8.18. Nos analistas digitais baseados em inteligência artificial, manter caráter assistivo, indicação de fontes, confiança e limitações sempre que possível, trilha de auditoria, controles contra manipulação e injeção de comandos, avaliação periódica de precisão e supervisão humana para decisões críticas e ações de impacto.

8.19. Manter interface web segura, gestão de usuários, perfis e grupos, autenticação multifator, segregação de funções, menor privilégio, referência temporal sincronizada,

trilhas de auditoria e interface, documentação operacional e suporte em língua portuguesa.

8.20. Disponibilizar APIs, conectores e mecanismos documentados de integração, com autenticação segura, tratamento de erros, registros e controle de versão, sem cobrança adicional pelo consumo ordinário necessário à execução regular quando não houver previsão expressa em sentido diverso.

8.21. 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.

8.22. Não utilizar produto ou versão sem suporte ativo quando isso comprometer segurança ou continuidade e comunicar previamente descontinuidade, fim de suporte, mudança de licenciamento ou outro impacto relevante.

9. OBRIGAÇÕES EXCLUSIVAS DO InPACTA E DO CLIENTE

9.1. Compete ao InPACTA exercer a governança institucional da parceria, designar responsáveis, emitir instrumentos de acionamento, acompanhar a execução e validar entregas.

9.2. Compete ao CLIENTE, quando aplicável, indicar pontos focais, ativos, terceiros, domínios, contas, marcas, usuários, prioridades e demais elementos do escopo autorizado.

9.3. O InPACTA e o CLIENTE deverão fornecer informações, acessos, inventários, janelas, autorizações e condições sob sua responsabilidade necessários à execução.

9.4. Caberá ao responsável pelo ambiente decidir sobre contenções, bloqueios, correções, exploração controlada, validação de credenciais e demais ações de impacto.

9.5. O InPACTA e o CLIENTE deverão analisar entregáveis, comunicar inconsistências e preservar credenciais e informações conforme os controles definidos.

9.6. A implementação de correções, alterações de configuração, bloqueios, isolamento, revogação de credenciais e demais medidas de remediação permanecerá sob decisão e responsabilidade do titular do ambiente, cabendo à PARCEIRA recomendar, apoiar, acompanhar e validar tecnicamente nos limites autorizados.

10. MATRIZ DE RESPONSABILIDADES OPERACIONAIS

10.1. A execução observará matriz de responsabilidades compatível com o ANEXO I, a proposta, os planos operacionais e as ordens de serviço.

10.2. Compete ao InPACTA a governança, o acionamento, o acompanhamento, a fiscalização, a análise de medições e a validação institucional.

10.3. Compete à PARCEIRA o fornecimento, a sustentação, a integração, a operação técnica, o suporte, a manutenção, a documentação, os relatórios, a segurança e a transição da solução.

10.4. Compete ao CLIENTE autorizar acessos e testes em seu ambiente, indicar escopo e prioridades, decidir sobre ações sob sua competência e apoiar a validação das entregas.

10.5. A matriz detalhada poderá ser complementada por plano ou ordem de serviço, sem afastar a responsabilidade técnica unificada da PARCEIRA.

10.6. O fluxo operacional deverá contemplar identificação, triagem, classificação, comunicação, recomendação, decisão do responsável pelo ambiente, acompanhamento, reteste e encerramento rastreável.

11. ATENDIMENTO INSTITUCIONAL E SUPORTE ESPECIALIZADO DA PARCEIRA

11.1. O atendimento institucional fará o registro, a triagem, o acompanhamento, a comunicação e o escalonamento das demandas conforme a governança definida.

11.2. A PARCEIRA prestará suporte especializado, incluindo diagnóstico, correção, atualização, integração, restabelecimento, orientação, evidências, análise de causa e encerramento técnico.

11.3. A PARCEIRA manterá base de conhecimento, matriz de escalonamento, procedimentos, contatos, histórico e registros compatíveis com o plano de suporte.

11.4. O atendimento institucional não reduz a obrigação da PARCEIRA de manter disponibilidade, suporte, segurança e cumprimento dos níveis de serviço.

11.5. Eventos críticos observarão atendimento contínuo e escalonamento técnico e gerencial, conforme a matriz de SLA aprovada, sem prejuízo da comunicação imediata prevista no ANEXO I.

12. ACOMPANHAMENTO OPERACIONAL E DE SEGURANÇA

12.1. O acompanhamento operacional abrangerá painéis, indicadores, alertas, eventos, disponibilidade, vulnerabilidades, exposições, riscos de terceiros, inteligência, incidentes, relatórios, evidências, tendências e anomalias disponibilizados pela solução.

12.2. A PARCEIRA deverá disponibilizar dados, painéis, indicadores, logs, alertas, integrações, evidências e trilhas necessários ao acompanhamento proativo e auditável.

12.3. Os dados e indicadores deverão informar origem, periodicidade, critério de cálculo, limitações e forma de extração quando aplicável.

12.4. Eventos relevantes poderão originar chamados, verificações, incidentes, planos corretivos, notificações, glosas ou outras providências cabíveis.

12.5. O acompanhamento do SOC será contínuo, em regime 24x7x365, a partir das fontes de logs, alertas e telemetrias integradas e autorizadas no escopo contratado.

13. CRONOGRAMA, PLANO DE TRABALHO TÉCNICO-INSTITUCIONAL, PLANOS OPERACIONAIS E ORDENS DE SERVIÇO

13.1. O cronograma abrangerá estruturação, validação, formalização, implantação, integração, operação assistida, suporte, manutenção, evolução, governança e transição.

13.2. O plano de implantação deverá indicar etapas, dependências, responsáveis, acessos, integrações, testes, treinamento, marcos, riscos, critérios de aceite e reversão.

13.3. Cada instrumento executivo ou ordem de serviço indicará, no mínimo, CLIENTE, diagnóstico, escopo, componentes, unidades e quantidades efetivas ou critérios de determinação, capacidade, recursos, responsáveis, prazos, entregáveis, condições econômicas, medição, critérios de aceite, requisitos de segurança, evidências e forma de homologação.

13.4. Nenhuma ordem de serviço poderá reduzir requisito funcional obrigatório nem criar garantia geral de consumo. O dimensionamento, o licenciamento, as responsabilidades, a segurança, a interoperabilidade, a continuidade e a remuneração deverão corresponder ao escopo efetivamente autorizado para o cliente.

13.5. Após a ordem de início, será realizada reunião de abertura para alinhamento de escopo, responsáveis, canais, cronograma, riscos, acessos e regras de engajamento.

13.6. A implantação compreenderá levantamento, inventário, configuração, integração, testes, homologação, documentação e entrada controlada em produção, seguida de operação assistida.

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

14. FUNCIONALIDADES SOB DEMANDA E MOBILIZAÇÃO DE EQUIPE

14.1. Pesquisas direcionadas, análises de inteligência, relatórios especiais, RFIs, inclusão de novas fontes, mecanismos de coleta especializados e ambiente sandbox poderão ser acionados nos limites e condições previstos no ANEXO I e em instrumento próprio.

14.2. A mobilização de equipe ou recurso sob demanda será responsabilidade da PARCEIRA e observará escopo, perfil, qualificação, segurança, prazo, documentação, teste, aceite, viabilidade técnica, legalidade e sustentação definidos no acionamento.

14.3. A mobilização não poderá justificar atraso, perda de qualidade, falha de integração, deficiência de segurança ou descumprimento do instrumento.

14.4. O acionamento sob demanda deverá preservar o núcleo do objeto e não poderá criar cobrança adicional sem previsão no instrumento aplicável.

15. PROVA DE CONCEITO, VALIDAÇÃO TÉCNICA E ACEITE

15.1. A PoC, quando realizada, validará objetivamente requisitos técnicos, funcionais, operacionais, de integração e segurança, conforme roteiro e matriz próprios.

15.2. A aprovação na PoC não exonera a PARCEIRA de manter o atendimento aos requisitos durante implantação, operação, suporte, auditoria e fiscalização.

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

15.4. O aceite dependerá de evidências, documentação, testes, licenciamento, integrações, atendimento ao escopo dimensionado no instrumento executivo de cada cliente, estabilidade e correção das pendências impeditivas.

15.5. Testes utilizarão ambiente controlado e não poderão provocar indisponibilidade, alteração indevida ou interação não autorizada.

15.6. O resultado será registrado em ata, termo ou relatório técnico com requisitos, testes, evidências, ocorrências, ressalvas e conclusão.

15.7. O aceite provisório não afasta a correção de falhas identificadas na operação assistida, e o aceite definitivo dependerá da correção das pendências impeditivas e da estabilidade da solução.

15.8. Dados reais, credenciais, vulnerabilidades e evidências somente poderão ser utilizados em testes ou demonstrações mediante autorização e controles adequados.

16. INTEGRIDADE, ANTICORRUPÇÃO, NEPOTISMO E CONFLITO DE INTERESSES

- 16.1. As PARTES conduzirão a parceria com ética, integridade, transparência, boa-fé, prevenção à fraude, combate à corrupção e respeito à competitividade.
- 16.2. A PARCEIRA observará os normativos de integridade e conduta do InPACTA formalmente disponibilizados e a legislação anticorrupção aplicável.
- 16.3. É vedado oferecer ou aceitar vantagem indevida, fraudar o procedimento, ocultar interesses, manipular preços ou praticar ato ilícito relacionado à parceria.
- 16.4. Conflito de interesses, vínculo relevante ou situação superveniente deverá ser comunicado para avaliação e tratamento.
- 16.5. A violação sujeitará o responsável às consequências previstas nos instrumentos e na legislação aplicável, assegurados os procedimentos cabíveis.

17. AVALIAÇÃO DE INTEGRIDADE E TRANSAÇÕES COM PARTES

RELACIONADAS

- 17.1. O InPACTA poderá avaliar a integridade da PARCEIRA antes da assinatura, prorrogação, repasse, acionamento de maior risco ou quando houver fato relevante.
- 17.2. A avaliação poderá abranger beneficiários finais, vínculos societários, administradores, controladores, subcontratados, terceiros relevantes, conflitos de interesses e relações com agentes públicos.
- 17.3. A PARCEIRA fornecerá as informações e adotará as medidas de mitigação solicitadas no prazo formalmente definido pelo InPACTA.
- 17.4. Omissão relevante, declaração falsa ou ocultação de conflito poderá ensejar as medidas do instrumento cabíveis.

18. COMPARTILHAMENTO DE RESULTADOS, RECEITAS E CONDIÇÕES DE REPASSE

- 18.1. Receitas, pagamentos ou repasses eventualmente decorrentes de implementação futura serão disciplinados exclusivamente por instrumento específico com o CLIENTE, ordem de serviço ou documento equivalente. As diretrizes de compartilhamento de riscos e resultados dos itens 29.4 a 29.7 do Edital integram a modelagem da parceria, sem efeito de pontuação. Os parâmetros de remuneração e de eventual participação institucional serão aprovados no Plano de Negócio Detalhado antes da assinatura definitiva e concretizados no instrumento executivo.
- 18.2. Este Instrumento não gera obrigação financeira imediata entre as PARTES sem previsão expressa em instrumento específico.
- 18.3. Valores estimados não representam garantia de demanda, receita, margem, volume ou direito automático a repasse.

18.4. Percentuais, base de cálculo, tributos, glosas, prazos, documentos fiscais, faturamento e condições de repasse deverão constar do instrumento econômico-financeiro aplicável. O Plano de Negócio Detalhado identificará a natureza da receita institucional, o teto ou faixa e a base de cálculo da eventual participação do InPACTA, com motivação dos encargos e sem presumir valores ainda não aprovados. Deverão ser demonstrados os encargos efetivos do Instituto e o nexo entre esses encargos e sua receita, vedada duplicidade de remuneração pelo mesmo encargo. Os parâmetros essenciais aprovados serão publicados, na extensão compatível com o sigilo comercial legítimo.

ELEMENTO	DEFINIÇÃO
Modelo de pagamento	Definido no instrumento específico de cada implementação antes de qualquer obrigação financeira, sem efeito sobre a seleção ou o VTI.
Base de cálculo	Composição, unidades, tributos, riscos, glosas e eventual compartilhamento de resultados expressamente aprovados, sem duplicidade de remuneração.
Prazo e faturamento	Prazo, documento fiscal, medição, aceite e condição de repasse ou pagamento definidos no instrumento aplicável.

18.5. O repasse, quando devido, observará o recebimento correspondente, a regularidade da PARCEIRA, a conformidade fiscal, a medição e as glosas aplicáveis.

18.6. Antes de cada instrumento executivo, serão juntadas pesquisa de preços por módulo e cenário, memória de cálculo e justificativa de compatibilidade com o mercado. O instrumento fixará prazo de revisão periódica e dever de a PARCEIRA comunicar condições mais favoráveis concedidas a cliente comparável, estendendo-as quando demonstrada equivalência de escopo, escala, tributos e riscos. O teto ou preço de referência será calculado segundo o método validado antes da publicação do Edital, previsto nos itens 16.4.1 e 16.4.2 do Plano, sem substituição por negociação bilateral livre. A produção de efeitos financeiros dependerá também da base jurídica e da análise cabível do respectivo CLIENTE.

18.7. A garantia de execução, por seguro-garantia ou meio equivalente, será motivada e dimensionada em cada instrumento executivo, antes do início de suas obrigações, sem compor a qualificação, a pontuação ou o desempate da seleção. Os planos de continuidade e transição permanecerão exigíveis desde a proposta, com verificação das medidas concretas de continuidade em caso de recuperação judicial.

18.8. O InPACTA não prestará fiança, aval ou garantia de obrigações dos CLIENTES nem se obrigará de favor. A inadimplência de CLIENTE não gera garantia automática

do Instituto em benefício da PARCEIRA. Esta disposição não afasta as obrigações próprias expressamente assumidas pelo InPACTA ou a responsabilidade por seus atos.

19. ESTRATÉGIA DE ALAVANCAGEM INSTITUCIONAL, TÉCNICA E

COMERCIAL

19.1. As PARTES poderão realizar demonstrações, PoC, pilotos, ambientes demonstrativos, estudos de caso, apresentações e outras ações de estruturação, validação ou expansão da solução.

19.2. Cada iniciativa deverá ser justificada e delimitada quanto a objetivo, custos, responsabilidades, prazo, medição, encerramento, uso de marca, dados, ambientes e evidências.

19.3. A iniciativa não gera direito automático a contratação, repasse, ressarcimento, exclusividade ou continuidade sem instrumento expresso.

19.4. Dados reais, credenciais, vulnerabilidades e evidências de CLIENTES somente poderão ser utilizados com autorização e controles adequados.

20. MATRIZ DE RISCOS

20.1. A matriz de riscos definitiva deverá ser aprovada e anexada ao instrumento antes da assinatura, dele constituindo parte integrante, nos termos do art. 27, § 2º, do Regulamento. As PARTES observarão essa matriz e suas complementações formalizadas. A alocação mínima seguirá o item 29.4 do Edital, com detalhamento das dependências, medidas de prevenção, gatilhos de atuação e responsáveis nos instrumentos executivos.

20.2. A matriz abrangerá, quando aplicável, riscos técnicos, operacionais, jurídicos, financeiros, de integridade, segurança, proteção de dados, licenciamento, disponibilidade, suporte, implantação, terceiros e continuidade.

20.3. A alocação de risco implicará o dever de prevenção, mitigação, resposta e comunicação pela PARTE responsável.

20.4. Eventos supervenientes serão tratados de forma motivada, proporcional e compatível com a continuidade e o regime aplicável.

21. PROPRIEDADE INTELECTUAL, COCRIAÇÃO, USO DE MARCA E ATIVOS INTANGÍVEIS

21.1. Permanecem com seus titulares os direitos preexistentes sobre plataformas,

códigos, bases, metodologias, modelos, algoritmos, playbooks e tecnologias.

21.2. Resultados cocriados, customizações e ativos desenvolvidos serão disciplinados no instrumento que os autorizar, com definição de titularidade, uso, manutenção, portabilidade e confidencialidade.

21.3. O CLIENTE terá direito de acesso, fiscalização, extração e portabilidade dos dados, relatórios e evidências produzidos em seu contexto, observados sigilo, segurança e licenciamento.

21.4. O uso de nomes, marcas, sinais, imagens ou casos de uso dependerá de autorização e finalidade definida.

22. LICENCIAMENTO, MÓDULOS E DIREITOS DE USO

22.1. A matriz de licenciamento identificará produtos, edições, métricas, critérios de dimensionamento por cliente, usuários, ativos, integrações, APIs, armazenamento, suporte e direitos incluídos.

22.2. O licenciamento será suficiente ao funcionamento integral e aos entregáveis do ANEXO I, conforme o escopo e o dimensionamento definidos no instrumento executivo de cada cliente.

22.3. Não será admitida dependência de licença, módulo ou conector essencial omitido da proposta.

22.4. Atualizações corretivas, patches, versões e renovações necessários à continuidade estarão abrangidos durante a vigência conforme a proposta e os instrumentos aplicáveis.

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

22.6. A matriz de licenciamento deverá identificar produtos, edições, métricas, critérios de dimensionamento por cliente, usuários, ativos, integrações, APIs, armazenamento, suporte e direitos incluídos, e sua comprovação ocorrerá por documentação oficial ou outro meio verificável.

23. SEGURANÇA DA INFORMAÇÃO, PROTEÇÃO DE DADOS E CONFIDENCIALIDADE

23.1. A PARCEIRA adotará medidas técnicas, administrativas e organizacionais para proteger confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade e resiliência.

23.2. As plataformas deverão disponibilizar autenticação multifator, e os acessos observarão menor privilégio, segregação de funções, necessidade de conhecimento

e trilha de auditoria.

23.3. Dados, credenciais, evidências, relatórios e comunicações sensíveis serão protegidos em trânsito e, quando aplicável, em repouso.

23.4. As PARTES manterão sigilo sobre informações não ostensivas acessadas ou produzidas, inclusive após o encerramento enquanto persistir sua natureza protegida.

23.5. Incidentes, suspeitas de vazamento, acesso indevido ou indisponibilidade relevante serão comunicados formalmente, com contenção, análise, mitigação, evidências e atualizações pertinentes.

23.6. Subcontratados observarão obrigações equivalentes de segurança, sigilo e proteção de dados.

23.7. A PARCEIRA manterá gestão de vulnerabilidades e atualização dos componentes que utilizar na prestação dos serviços.

23.8. Incidentes que afetem a solução, os dados ou a continuidade serão comunicados formalmente, com informações e atualizações relevantes, preservadas as evidências e a cooperação para contenção e mitigação.

23.9. Após a homologação, as PARTES firmarão Termo de Confidencialidade, conforme o art. 29 do Regulamento, sem prejuízo das obrigações de sigilo já aplicáveis à seleção e à PoC. O termo não afastará a publicidade legalmente exigida do contrato, de seus aditivos e dos atos de controle.

24. TRATAMENTO E PROTEÇÃO DE DADOS PESSOAIS

24.1. O tratamento de dados pessoais observará a Lei nº 13.709/2018, a finalidade parceira, necessidade, adequação, segurança, prevenção, rastreabilidade e retenção limitada.

24.2. As funções e responsabilidades das PARTES no tratamento serão definidas conforme a operação efetivamente realizada e os instrumentos aplicáveis.

24.3. Dados pessoais, credenciais expostas e conteúdos sensíveis terão acesso restrito às finalidades autorizadas.

24.4. Solicitações de titulares, incidentes e determinações da autoridade competente serão tratados de forma cooperativa, conforme as responsabilidades de cada PARTE.

24.5. Encerrada a finalidade e observadas retenções aplicáveis, os dados serão devolvidos, eliminados ou tornados inacessíveis de forma segura.

24.6. Antes do tratamento, os instrumentos aplicáveis deverão definir, conforme a operação efetivamente realizada, as funções das PARTES, as finalidades, os acessos autorizados, as medidas de segurança, a retenção e o fluxo de atendimento a incidentes e direitos dos titulares. Como diretriz, o CLIENTE atuará como

controlador dos dados de seus sistemas e das finalidades de segurança por ele definidas; a PARCEIRA atuará como operadora ou suboperadora na execução de instruções documentadas. O papel do InPACTA será definido por operação, distinguindo a atuação sob instruções do CLIENTE das finalidades próprias de governança e cumprimento de obrigações. Antes de qualquer tratamento, o instrumento executivo confirmará esses papéis segundo as atividades efetivas, exigirá o registro das operações e preverá relatório de impacto à proteção de dados nas implantações de risco elevado e nas demais hipóteses exigíveis.

24.7. É vedado à PARCEIRA e aos terceiros por ela utilizados reutilizar dados, evidências ou telemetria dos CLIENTES para treinamento de modelos de inteligência artificial ou para finalidades próprias alheias à execução autorizada.

25. ARMAZENAMENTO, RETENÇÃO, BACKUP, PORTABILIDADE E CONTINUIDADE

25.1. A solução manterá armazenamento compatível com históricos, evidências, alertas, investigações, relatórios e auditoria.

25.2. A política de retenção será documentada e coerente com finalidade, criticidade, obrigações e determinações do responsável pelos dados.

25.3. Expurgo e descarte serão governados, rastreáveis e seguros.

25.4. A PARCEIRA manterá backup, contingência, recuperação e testes de restauração dos componentes sob sua responsabilidade.

25.5. O plano de continuidade contemplará indisponibilidade, perda de conectividade, comprometimento de credenciais e incidentes.

25.6. Dados, logs e históricos necessários permanecerão acessíveis durante a vigência e serão disponibilizados na transição.

25.7. Retenções específicas determinadas pelo responsável pelos dados serão documentadas e observadas, sem prejuízo do expurgo seguro ao término da finalidade.

26. SUPORTE, MANUTENÇÃO, SLA E IMR

26.1. A PARCEIRA manterá central de atendimento com registro, classificação, acompanhamento, escalonamento, comunicação e encerramento.

26.2. O parâmetro documentado para ocorrências críticas é início da investigação em até 2 horas, relatório preliminar em até 24 horas e regime 24x7x365. Os níveis de serviço das demais criticidades, os marcos de contagem, as exclusões e as consequências serão definidos no instrumento executivo de cada implementação antes do início da operação.

CRITICIDADE	INÍCIO DA INVESTIGAÇÃO	RELATÓRIO PRELIMINAR	REGIME
Crítica	Até 2 horas	Até 24 horas	24x7x365
Alta	Conforme instrumento executivo	Conforme instrumento executivo	Conforme criticidade e cobertura aprovadas
Média	Conforme instrumento executivo	Conforme instrumento executivo	Conforme criticidade e cobertura aprovadas
Baixa	Conforme instrumento executivo	Conforme instrumento executivo	Conforme criticidade e cobertura aprovadas

26.3. Ocorrências serão classificadas segundo impacto, urgência, risco e alternativa operacional. Nenhum prazo ainda não definido produzirá obrigação, glosa ou sanção até sua aprovação e formalização no instrumento executivo aplicável.

26.4. O suporte compreenderá diagnóstico, orientação, correção, atualização, restauração, análise de causa e documentação.

26.5. A manutenção preservará compatibilidade, segurança, histórico, integrações e continuidade.

26.6. O desempenho será acompanhado por disponibilidade, prazos, qualidade, efetividade, reincidência e pendências, conforme IMR quando adotado.

27. CAPACITAÇÃO E TRANSFERÊNCIA DE CONHECIMENTO

27.1. A PARCEIRA apresentará plano de capacitação compatível com os perfis indicados.

27.2. A capacitação abrangerá plataformas, alertas, indicadores, casos, relatórios, acessos, integrações, segurança e escalonamento.

27.3. Serão fornecidos materiais, guias, manuais e registros das capacitações.

27.4. Atualizações relevantes serão acompanhadas de orientação complementar.

27.5. A transferência de conhecimento ocorrerá durante a execução e será reforçada na transição.

28. RELATÓRIOS, EVIDÊNCIAS E GOVERNANÇA DOCUMENTAL

28.1. A PARCEIRA disponibilizará alertas, notificações, atendimentos, evidências, recomendações e pendências durante a execução.

28.2. Mensalmente, apresentará relatório técnico e executivo consolidado com indicadores, riscos, vulnerabilidades, exposições, inteligência, incidentes, ações e recomendações.

28.3. Incidente relevante gerará comunicação imediata e, quando aplicável, relatório com linha do tempo, evidências, análise e medidas.

28.4. Relatórios e indicadores deverão ser rastreáveis aos registros de origem e permitir fiscalização, priorização, avaliação de desempenho e prestação de contas.

28.5. Reuniões de governança serão registradas com participantes, decisões, responsáveis, prazos, riscos e plano de ação.

28.6. Os indicadores acompanharão, conforme aplicável, volume, criticidade, tendência, recorrência, tratamento, disponibilidade, SLA e efetividade, com rastreabilidade às evidências de origem.

29. ALTERAÇÕES, EVOLUÇÕES, SUBSTITUIÇÕES E GOVERNANÇA DE MUDANÇAS

29.1. Mudanças relevantes de arquitetura, integração, versão, retenção, licenciamento, segurança ou operação seguirão processo documentado de avaliação, autorização, teste, reversão e comunicação.

29.2. Substituição de produto, módulo ou componente dependerá de comprovação de equivalência ou superioridade e preservará funcionalidades, integração, segurança, desempenho, histórico e direitos.

29.3. Não serão admitidas alterações que reduzam requisitos obrigatórios, o escopo efetivamente pactuado no instrumento executivo, o licenciamento, a interoperabilidade ou a responsabilidade técnica.

29.4. Atualizações serão planejadas e executadas de modo a reduzir risco de indisponibilidade e perda de dados.

29.5. Substituições por obsolescência, descontinuidade ou fim de suporte dependerão de comprovação de equivalência ou superioridade e não poderão reduzir funcionalidades, integrações, segurança, desempenho, histórico ou direitos.

30. MEDIÇÃO, FISCALIZAÇÃO, GLOSAS E NÃO CONFORMIDADES

30.1. A fiscalização acompanhará disponibilidade, atendimento, prazos, incidentes, relatórios, qualidade, integrações, segurança, evidências e cumprimento das obrigações.

30.2. A medição utilizará os entregáveis, indicadores, SLA, IMR, registros e critérios constantes dos instrumentos aplicáveis.

30.3. Não conformidades serão registradas com descrição, evidência, criticidade, responsável, prazo e condição de encerramento.

30.4. Glosas e demais consequências observarão previsão documental, proporcionalidade, motivação e os procedimentos cabíveis.

30.5. A fiscalização não exclui nem reduz a responsabilidade da PARCEIRA por falhas, vícios, omissões ou danos.

30.6. Medição, aceite, glosa e pagamento ou repasse, quando aplicáveis, deverão manter coerência com os entregáveis, o dimensionamento de cada instrumento executivo, o licenciamento, os indicadores e as evidências previstos nos documentos integrantes.

31. DESCUMPRIMENTO, INFRAÇÕES E SANÇÕES

31.1. O descumprimento de obrigações técnicas, operacionais, de segurança, confidencialidade, suporte, prazo, qualidade, licenciamento, continuidade ou proteção de dados poderá ensejar as consequências previstas no Edital, neste Instrumento, nos instrumentos específicos e na legislação aplicável. Antes da assinatura, o instrumento definitivo deverá tipificar os descumprimentos e as sanções cabíveis, graduando objetivamente suas consequências segundo a gravidade, o impacto, a reincidência e a proporcionalidade, com bases de cálculo, valores ou percentuais quando aplicáveis, sem importação automática de penalidades de outro regime.

31.2. A aplicação de medida observará a natureza, a gravidade, o impacto, a reincidência, as circunstâncias, a cooperação e os procedimentos de defesa cabíveis. O instrumento definitivo fixará, antes da assinatura, os prazos de defesa e de recurso cabíveis, as autoridades responsáveis e o procedimento de apuração. A comunicação será escrita, com identificação dos fatos, das evidências e da consequência proposta, acesso aos elementos pertinentes e decisão motivada, assegurados contraditório e ampla defesa.

31.3. A correção da irregularidade não afasta, por si só, a apuração de consequências decorrentes do período de descumprimento.

31.4. Sanção ou rescisão não afasta confidencialidade, segurança, portabilidade, transição, prestação de contas e responsabilização cabíveis.

32. RESPONSABILIDADE POR VÍCIOS, DANOS E DIREITO DE REGRESSO

32.1. Cada PARTE responderá pelos danos decorrentes de seus atos, omissões,

descumprimentos e riscos assumidos, conforme o regime aplicável.

32.2. A PARCEIRA responderá por vícios, falhas, incompatibilidades, vulnerabilidades introduzidas, perda de dados ou indisponibilidade atribuíveis aos componentes e serviços sob sua responsabilidade.

32.3. A utilização de fabricantes, provedores, integradores ou terceiros não afasta a responsabilidade da PARCEIRA perante o InPACTA e o CLIENTE.

32.4. O direito de regresso será preservado quando uma PARTE suportar prejuízo imputável à outra ou a terceiro sob responsabilidade desta.

33. SUBCONTRATAÇÃO, TERCEIROS E PROFISSIONAIS MOBILIZADOS

33.1. A subcontratação somente será admitida nos limites do Edital e dos instrumentos aplicáveis, sem transferência da responsabilidade principal da PARCEIRA.

33.2. A PARCEIRA assegurará que terceiros observem requisitos de qualificação, segurança, sigilo, proteção de dados, integridade, acesso e continuidade equivalentes.

33.3. A PARCEIRA manterá identificação e governança dos terceiros relevantes, inclusive fabricantes, licenciadores, provedores e suboperadores.

33.4. Restrições do instrumento entre a PARCEIRA e terceiros não poderão ser opostas para justificar descumprimento perante o InPACTA ou o CLIENTE.

34. RESCISÃO, EXTINÇÃO E ENCERRAMENTO

34.1. O Instrumento poderá ser encerrado nas hipóteses previstas nos instrumentos aplicáveis, mediante motivação e observância dos procedimentos cabíveis. A perda superveniente de condição de qualificação observará a condição resolutiva do item 5.6 e o procedimento de defesa da cláusula 31.

34.2. O encerramento considerará gravidade, possibilidade de correção, continuidade dos serviços, segurança, proteção de dados, interesse institucional e riscos aos CLIENTES.

34.3. A extinção não prejudica obrigações de confidencialidade, responsabilização, prestação de contas, devolução de ativos, portabilidade, retenção e transição.

34.4. As PARTES cooperarão para evitar interrupção abrupta, perda de evidências, exposição de dados ou comprometimento de controles de segurança.

35. TRANSIÇÃO, PORTABILIDADE E ENCERRAMENTO ASSISTIDO

35.1. A PARCEIRA executará plano de transição destinado a preservar continuidade,

portabilidade, histórico, segurança e rastreabilidade.

35.2. A transição incluirá inventários, configurações, casos, alertas, evidências, indicadores, relatórios, auditoria, integrações, matriz de licenciamento, registros de suporte e documentação.

35.3. Dados serão fornecidos em formatos estruturados, abertos ou amplamente utilizados, acompanhados da documentação necessária.

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

35.5. Após o encerramento e observadas retenções aplicáveis, cópias remanescentes serão eliminadas ou tornadas inacessíveis de forma segura.

36. COMUNICAÇÕES E REGISTRO DE OCORRÊNCIAS

36.1. Comunicações formais, notificações, ordens de serviço, ocorrências, defesas, manifestações, glosas, aceites e decisões serão realizadas por escrito em canal institucional definido.

36.2. Reuniões relevantes serão reduzidas a termo, ata, relatório ou registro eletrônico equivalente.

36.3. As PARTES manterão atualizados seus representantes, pontos focais, endereços e canais formais.

36.4. Comunicações críticas de segurança utilizarão os canais e fluxos de escalonamento aprovados, sem prejuízo do registro formal.

37. GESTÃO E FISCALIZAÇÃO CONTRATUAL

37.1. O InPACTA designará representantes para acompanhar e fiscalizar a execução da parceria.

37.2. A gestão verificará obrigações, recursos, equipe, licenças, suporte, segurança, documentação, entregáveis, SLA, IMR e demais elementos necessários.

37.3. Os representantes poderão solicitar esclarecimentos, evidências, correções, planos de ação e demais providências previstas nos instrumentos.

37.4. A fiscalização não exclui nem reduz a responsabilidade da PARCEIRA.

38. RESOLUÇÃO DE CONTROVÉRSIAS

38.1. As PARTES buscarão solução consensual por comunicação formal, reunião técnica, negociação institucional ou outro mecanismo adequado.

38.2. Persistindo o impasse, serão adotados os meios de solução admitidos pelo regime aplicável e definidos no instrumento definitivo. A escolha do mecanismo será

expressa no contrato antes da assinatura, conforme o art. 30 do Regulamento, vedada a permanência de remissão genérica no instrumento assinado.

38.3. Fica eleito o foro da Comarca de Maringá/PR, sem prejuízo de competência legal de observância obrigatória.

39. DISPOSIÇÕES GERAIS

39.1. A legislação brasileira regerá este Instrumento.

39.2. Os casos omissos serão resolvidos à luz do Edital, dos Anexos, da proposta aprovada, do Regulamento DIR_EXEC/InPACTA nº 001/2025, da Lei nº 13.303/2016 na extensão adaptada nele prevista, dos demais normativos internos aplicáveis, dos preceitos de Direito Privado e da legislação material incidente.

39.3. A tolerância quanto ao descumprimento não constituirá novação, renúncia ou alteração tácita.

39.4. A invalidade de uma disposição não prejudicará as demais, devendo-se preservar a finalidade do instrumento quando juridicamente possível.

39.5. Em conflito entre documentos, a interpretação preservará integridade do objeto, segurança, continuidade e coerência entre proposta, PoC, execução, medição, aceite e transição, prevalecendo o requisito técnico específico do ANEXO I quando mais aderente ao objeto.

39.6. A PARCEIRA não poderá opor limitação assumida com terceiro para deixar de cumprir obrigação perante o InPACTA ou o CLIENTE.

39.7. Cessão ou transferência de direitos e obrigações dependerá de consentimento e formalização, ressalvadas hipóteses admitidas.

39.8. Permanecem válidas após o término as obrigações de segurança, confidencialidade, integridade, rastreabilidade, transição, portabilidade e colaboração necessárias à proteção do interesse público e à continuidade da SOLUÇÃO INTEGRADA PARA CIBERSEGURANÇA.

39.9. O contrato e seus aditivos serão publicados no sítio institucional do InPACTA, nos termos do art. 29, §§ 4º e 5º, do Regulamento. Eventuais restrições deverão individualizar e justificar as informações legitimamente sigilosas, sem ocultar atos sujeitos à publicidade e ao controle.

Maringá/PR, data da assinatura eletrônica.

INSTITUTO DE PROJETOS AVANÇADOS PARA CIDADES, TECNOLOGIA E
ADMINISTRAÇÃO – InPACTA

Representante legal

PARCEIRA

Representante legal

Procuradoria Jurídica do InPACTA

Testemunha 1 – Nome: _____ CPF: _____

Testemunha 2 – Nome: _____ CPF: _____



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 **9823992** e o código CRC **C2213374**.

Referência: Processo nº 43.04.00000186/2026.88

SEI nº 9823992