

ANEXO B – PROVA DE CONCEITO

1. FINALIDADE

1.1. Caso seja exigida, a Prova de Conceito (PoC) será realizada pela licitante provisoriamente classificada em primeiro lugar, mediante convocação formal da Administração;

1.2. A Prova de Conceito (PoC) tem por objetivo verificar, de forma prática, objetiva e comprovável, a aderência da solução conforme requisitos mínimos estabelecidos no Termo de Referência e seus anexos;

1.3. A PoC, quando exigida, será convocada pela Administração mediante comunicação formal, devendo ser realizada no prazo máximo de **05 (cinco) dias úteis** contados da notificação. Todos os custos relacionados à preparação, execução, infraestrutura, licenças, mão de obra, ambiente demonstrativo, conectividade, equipamentos e demais elementos necessários correrão exclusivamente às expensas da licitante, sem ônus para o MPRJ;

1.4. A PoC poderá ser realizada de forma presencial ou remota, conforme definido pela **Gerência de Operações/MPRJ**, devendo permitir acompanhamento em tempo real pelos avaliadores designados. É vedada a utilização de vídeos pré-gravados, simulações editadas, ambientes fictícios ou recursos não pertencentes à solução ofertada na proposta comercial;

1.5. A PoC será avaliada pela **Gerência de Operações/MPRJ**, que emitirá parecer conclusivo com base no roteiro oficial de testes que integra este Anexo. Todos os requisitos constantes da tabela de validação são de atendimento **obrigatório**, aplicando-se critério de aceite **binário**:

1.5.1. ATENDE – requisito comprovadamente demonstrado, com evidência válida;

1.5.2. NÃO ATENDE – requisito não demonstrado, demonstrado de forma incompleta, com evidência inválida ou não demonstrado nos termos solicitados.

1.6. Não será considerado atendimento quando a demonstração não comprovar integralmente o requisito nos termos definidos neste Anexo. A ausência de evidências, falha de execução, incompatibilidade técnica ou demonstração incompleta resultará na marcação de “NÃO ATENDE”;

1.7. A não realização da PoC no prazo, a apresentação incompleta, a falta de evidências verificáveis ou a não comprovação de atendimento aos requisitos obrigatórios implicará:

1.7.1. implicará a desclassificação da licitante, assegurado o contraditório e a ampla defesa nos termos da legislação aplicável; e

1.7.2. Convocação da licitante subsequente, observada a ordem de classificação do certame.

1.8. Ao final da PoC, será lavrado **Termo de Resultado**, assinado pelos avaliadores oficiais, contendo:

1.8.1. Roteiro de testes aplicado;

1.8.2. Registro de evidências apresentadas;

1.8.3. Resultados obtidos para cada requisito (“ATENDE” / “NÃO ATENDE”);

1.8.4. Parecer conclusivo: **APROVADA** ou **REPROVADA**;

1.8.4.1. Não haverá atribuição de pontuação, percentual, gradação ou nota.

2. ROTEIRO DE TESTES – TABELA DE VALIDAÇÃO

2.1. Todos os itens abaixo são obrigatórios. O não atendimento de qualquer um deles resultará na reprovação da PoC.

Item	Requisito Avaliado	Evidência Apresentada (pela licitante)	Atende	Não atende
1. INFRAESTRUTURA DO SOC (SECURITY OPERATIONS CENTER)				
1.1.	Apresentar documentação comprobatória de operação do SOC em regime contínuo (24x7x365);		☐	☐
1.2.	Demonstrar, por meio de documentação técnica ou declaração formal, a existência de mecanismos de redundância e continuidade operacional		☐	☐
1.3.	Descrever os controles de segurança física e lógica adotados para proteção do ambiente operacional		☐	☐
1.4.	Apresentar visão geral da arquitetura da solução ofertada, evidenciando mecanismos de disponibilidade e resiliência		☐	☐
2. COMUNICAÇÃO E CONECTIVIDADE COM O MPRJ				
2.1.	Demonstrar que o acesso ao ambiente do MPRJ ocorre		☐	☐

	exclusivamente por centrais certificadas, sem VPN direta			
2.2.	Demonstrar canal 0800 nacional, atendimento humano e tempo real		☐	☐
2.3.	Exibir a solução ITSM utilizada, mostrando abertura, histórico e tratamento de chamados		☐	☐
2.4.	Demonstrar sala de crise virtual funcional, com conexão criptografada SSL		☐	☐
3. MONITORAMENTO, GESTÃO E RELATÓRIOS				
3.1.	Demonstrar a disponibilização diária, no primeiro horário útil, por meio de painel ou portal, de informações sobre a saúde do ambiente, contemplando, no mínimo, análise de risco, vulnerabilidades identificadas e categorizadas por risco, indicador de compliance, ameaças na Dark Web, análise e alertas de incidentes, incidentes identificados e bloqueados e eventuais impactos, conforme item 3.4.2 do Anexo A.		☐	☐
3.2.	Demonstrar dashboards gerenciais e técnicos utilizados mensalmente		☐	☐
3.3.	Exibir relatório mensal padrão contendo: incidentes, SLAs, vulnerabilidades, riscos e ações de melhoria		☐	☐
3.4.	Mostrar evidência de ferramentas de monitoramento contínuo e antecipação de incidentes		☐	☐
3.5.	Demonstrar mecanismo para realização de pesquisa de		☐	☐

	qualidade operacional trimestral.			
3.6.	Demonstrar processo de revisão periódica das políticas e processos do ambiente integrado de monitoramento e resposta a incidentes de segurança da informação, em conformidade com as melhores práticas do ITIL.		☐	☐
4. NÍVEIS MÍNIMOS DE SERVIÇO (NMS)				
4.1.	Demonstrar capacidade real de triagem de incidentes em ≤ 15 minutos		☐	☐
4.2.	Exibir mecanismos que garantem disponibilidade mínima de ≥ 99,7%		☐	☐
4.3.	Mostrar como são aplicadas glosas em casos de SLA descumprido		☐	☐
5. EQUIPE TÉCNICA E CAPACITAÇÃO				
5.1.	Demonstrar o processo de escalação funcional, mapeado e documentado, contemplando os níveis de atendimento N1, N2 e N3, bem como a matriz de escalação hierárquica e funcional, conforme item 5.1.2.2 do Anexo A		☐	☐
5.2.	Demonstrar trilhas de capacitação contínua e políticas de sigilo implementadas		☐	☐
5.3.	Provar a existência de Gerente Técnico de Conta (TAM), apresentando agenda e modelo de atuação quinzenal		☐	☐
6. SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE				
6.1.	Demonstrar solução que implemente política de gestão de riscos conforme frameworks		☐	☐

	reconhecidos e métodos quantitativos			
6.2.	Exibir gerenciamento de KRI, matriz de risco, relatórios analíticos e gráficos		☐	☐
6.3.	Demonstrar capacidade da solução para gestão e varredura de vulnerabilidades em ambientes corporativos de grande porte, com monitoramento contínuo de ativos e identificação de exposições de segurança		☐	☐
6.4.	Demonstrar base de conhecimento com, no mínimo, 35.000 CVEs e suporte ao padrão CVSS.		☐	☐
6.5.	Demonstrar suporte para adição de detecções personalizadas utilizando Open Vulnerability Assessment Language (OVAL).		☐	☐
6.6.	Demonstrar suporte à integração para autenticação por ferramentas de cofres de senha com, ao menos, dois dos seguintes fabricantes: Thycotic/Centrify, CyberArk e BeyondTrust.		☐	☐
6.7.	Exibir solução de patch management com catálogo de, no mínimo, 35.000 patches.		☐	☐
7. GESTÃO DE INFORMAÇÕES, DADOS PESSOAIS E LGPD				
7.1.	Demonstrar sistema de gestão de políticas com versionamento, publicação por URL e histórico		☐	☐
7.2.	Demonstrar funcionalidades da solução para atendimento a titulares de dados pessoais, incluindo gestão de solicitações e fluxo de tratamento		☐	☐
7.3.	Apresentar recursos disponíveis para gestão de consentimento e		☐	☐

	direitos dos titulares, quando aplicável			
7.4.	Mostrar capacidade de gerar e manter ROPA, DPIA/RIPD e inventário de dados pessoais		☐	☐
8. GESTÃO DE TERCEIROS E RISCOS RELACIONADOS				
8.1.	Demonstrar funcionalidades da solução para avaliação e acompanhamento de riscos relacionados a terceiros, quando aplicável ao escopo da contratação		☐	☐
8.2.	Exibir funcionalidades de classificação de fornecedores, riscos, scoring e ciclos de revisão		☐	☐
8.3.	Mostrar monitoramento de riscos ESG com fontes oficiais e automação de alertas		☐	☐
9. GESTÃO DE INCIDENTES, SUPERFÍCIE DE ATAQUES E AMEAÇAS				
9.1.	Demonstrar solução que monitore Deep Web, Dark Web e fontes públicas, com alertas em tempo real		☐	☐
9.2.	Demonstrar capacidade de monitoramento de múltiplas fontes de inteligência de ameaças		☐	☐
9.3.	Exibir monitoramento de superfície de ataque (domínios, IPs, vulnerabilidades expostas)		☐	☐
9.4.	Demonstrar cálculo automático de score de risco cibernético		☐	☐
9.5.	Demonstrar disponibilidade de APIs documentadas para integração com sistemas de segurança existentes.		☐	☐
9.6.	Demonstrar capacidade de integração com SIEM.		☐	☐

9.7.	Demonstrar capacidade de integração com SOAR.		☐	☐
10. CONTROLE DE SEGURANÇA E SEGMENTAÇÃO				
10.1	Demonstrar funcionalidades de controle e segmentação de rede que contribuam para redução da superfície de ataque e contenção de ameaças		☐	☐
10.2.	Exibir visibilidade de tráfego Leste-Oeste/Norte-Sul		☐	☐
10.3.	Demonstrar a utilização de Feeds de Ameaça (Threat Feeds), conforme requisitos do Anexo A.		☐	☐
10.4.	Demonstrar mecanismos de detecção de anomalias.		☐	☐
10.5.	Demonstrar funcionalidades para criação ou aplicação de políticas de segmentação ou microsegmentação, conforme requisitos do Anexo A.		☐	☐
11. CONTINUIDADE DO NÉGOCIO E AIN				
11.1.	Demonstrar metodologia aplicada à Análise de Impacto no Negócio (AIN)		☐	☐
11.2.	Exibir identificação de serviços críticos, tempos toleráveis e planos mínimos de restabelecimento		☐	☐

3. DECLARAÇÃO FINAL DO RESULTADO

☐ **APROVADA** – A solução demonstrou atendimento integral a todos os requisitos obrigatórios da PoC.

☐ **REPROVADA** – A solução **não atendeu** a um ou mais requisitos obrigatórios, sendo a licitante desclassificada.

Rio de Janeiro, _____ de _____ de 20____.

Servidor Responsável

Servidor Responsável