

ANEXO I-A

GESTÃO DE SERVIÇOS

1. FINALIDADE

Este anexo de Gestão dos Serviços define os padrões de desempenho, responsabilidades e expectativas para os serviços de Threat Intelligence fornecidos pela empresa ao CONTRATANTE. O objetivo é garantir a entrega de serviços confiáveis, oportunos e de alta qualidade para proteger o Contratante contra fraudes e ameaças cibernéticas.

2. ESCOPO DA GESTÃO DOS SERVIÇOS

- 2.1. Monitoramento contínuo de marca e executivos em redes sociais, dark web, deep web e outros canais, com alertas sobre ameaças como difamação, phishing direcionado e uso indevido de propriedade intelectual.
- 2.2. Classificação e priorização de riscos com base em frameworks reconhecidos, considerando probabilidade, impacto e criticidade.
- 2.3. Utilização de inteligência artificial (IA) para detecção e classificação de ameaças, com emprego de aprendizado de máquina (ML) e processamento de linguagem natural (PLN) para detectar, classificar e prever ameaças, com alta precisão e baixa taxa de falsos positivos.
- 2.4. Detecção e interrupção de campanhas maliciosas (ex.: phishing, DDoS, desinformação), com ações proativas para interrupção (ex.: takedown de domínios).
- 2.5. Compartilhamento de Indicadores de Compromisso (IoCs) em formatos padronizados e integração com redes de compartilhamento de inteligência.
- 2.6. Integração com sistemas SIEM e SOAR da Contratante, com suporte a automação de respostas.

3. ENTREGAS

- 3.1. Relatórios periódicos contendo análises contextualizadas, priorização de riscos e recomendações práticas para mitigação.
- 3.2. Contribuição comprovada para a redução de riscos de fraude e ataques cibernéticos, com foco em prevenção e resposta antecipada.
- 3.3. Envio de alertas em tempo real para ameaças críticas, com classificação por criticidade.
- 3.4. Integração eficiente com sistemas de segurança existentes.
- 3.5. Derrubada (takedown) de sites e perfis falsos relacionados a marcas e personalidades do Banco.
- 3.6. Aprimoramento contínuo da visibilidade e resposta a riscos reputacionais e ataques direcionados à marca e aos executivos, com foco em detecção antecipada e mitigação.

4. CARACTERÍSTICAS GERAIS DO SERVIÇO

- 4.1. A CONTRATADA deverá ser capaz de monitorar, gerar alertas e permitir o acesso das informações coletadas pelo CONTRATANTE em regime de 24x7 (24 horas por dia, 7 dias por semana), inclusive finais de semana e feriados.
- 4.2. A CONTRATADA deve disponibilizar equipe técnica para relacionamento com o Banco no ambiente remoto, horário comercial em regime de 8x5 (8 horas por dia, 5 dias por semana), capaz de executar, no mínimo, as seguintes atividades sob demanda:
 - 4.2.1. Realização de buscas por assuntos de interesse dentro do contexto de inteligência cibernética e de potenciais ameaças direcionadas ao Banco;

- 4.2.2. Configuração e parametrização para coleta dos assuntos de interesse do Banco dentro do contexto de inteligência cibernética de forma a direcionar as informações coletadas;
- 4.2.3. Criação de buscas pré-configuradas direcionadas para contextos distintos em busca de potenciais ameaças ao Banco;
- 4.2.4. Criação de alertas automáticos nos assuntos de interesse do Banco no contexto de inteligência cibernética;
- 4.2.5. Elaboração de relatórios de inteligência sobre ameaças de interesse do Banco;
- 4.2.6. Interação com Grupos maliciosos (Threat Actors) no intuito de adquirir informações pertinentes às ameaças;
- 4.2.7. Interação com a equipe técnica do Banco;
- 4.2.8. Repasse de informações sobre pessoas envolvidas em atividades contra o sistema financeiro, com ênfase no Banco, (ex.: funcionários, clientes vítimas, terceirizados, contratados);
- 4.2.9. Repasse de informações referentes a comercialização online ilegal de itens financeiros com ênfase aos produtos relacionados ao Banco.
- 4.3. A CONTRATADA deverá integrar a CTI com a solução de SIEM/SOAR do Banco;
- 4.4. A CONTRATADA deverá copiar a equipe do BNB nas solicitações de *takedown* realizadas via e-mail; também deverá dar visibilidade ao time do BNB para os demais pedidos de *takedown* que não sejam realizados via e-mail.
- 4.5. No encerramento do contrato (Transição Contratual) a CONTRATADA se obriga a fornecer backup das informações que foram geradas para os Eventos de Exceção ao longo de toda a execução contratual, em formato como JSON, HTML, PDF, CSV, Planilha eletrônica e DOCX, ou em outros formatos aderentes com o intuito de que se possa reutilizar essa base histórica de informações, inclusive em eventual nova contratação.

5. MÉTRICAS DE DESEMPENHO E NÍVEIS DE SERVIÇO

5.1. Disponibilidade do Serviço

- 5.1.1. Métrica: O serviço de Threat Intelligence (incluindo plataformas, feeds de inteligência e suporte) deve estar disponível 99,9% do tempo, medido mensalmente.
- 5.1.2. Exceções: Manutenções programadas (com notificação prévia de 72 horas) não contam como indisponibilidade, limitado à 5% no mês.
- 5.1.3. Medição: Calculada como:
$$[(\text{Total de minutos no mês} - \text{Minutos de indisponibilidade}) / \text{Total de minutos no mês}] \times 100.$$
- 5.1.4. Redutor: redução de 2% do valor mensal por cada 0,1% abaixo de 99,9%, até o limite de 25% do valor mensal.

5.2. Tempo de Resposta a Incidentes Críticos

- 5.2.1. Definição: Incidentes críticos incluem campanhas maliciosas ativas (ex.: phishing direcionado, ransomware) ou vazamentos de dados na dark web.
- 5.2.2. Métrica A: Alerta inicial: <10 minutos após a detecção.
- 5.2.3. Métrica B: Resposta inicial (confirmação e plano de mitigação): <30 minutos após o alerta.
- 5.2.4. Métrica C: Ação de mitigação (ex.: takedown, bloqueio de IPs): <2 horas após a resposta inicial, quando aplicável.
- 5.2.5. Medição: Tempo entre detecção e notificação (A), Tempo entre o alerta inicial e a resposta inicial (B), tempo entre a ação de mitigação e resposta inicial (C).

5.2.6. Redutor: Redução de 5% do valor mensal por cada hora de atraso nas métricas A, B ou C, limitada a 50% do valor mensal.

5.3. Efetividade de Takedown:

5.3.1. Definição: Taxa de sucesso de takedown de domínios, links ou perfis maliciosos efetivamente removidos.

5.3.2. Métrica (A) >= taxa de sucesso de takedown 95%.

5.3.3. Métrica (B) <= 10min tempo entre detecção e solicitação de remoção.

5.3.4. Medição: Total de remoção de takedown/Total de detecção de incidentes*100 (A), Tempo entre a detecção do incidente e o envio de remoção (B).

5.3.5. Redutor: Redução de 3% do valor mensal por cada 1% abaixo de 95% (A) ou 10 minuto de atraso na métricas (B), limitada a 50% do valor mensal do serviço de takedown.

5.4. Tempo de Resposta a Ameaças Não Críticas

5.4.1. Definição: Ameaças não críticas incluem menções suspeitas à marca, perfis falsos ou IoCs de baixa prioridade.

5.4.2. Métrica (A): Alertas: <1 hora após a detecção.

5.4.3. Métrica (B): Resposta inicial: <4 horas após o alerta.

5.4.4. Medição: Tempo entre detecção e notificação (A), Tempo entre o alerta inicial e a resposta inicial (B).

5.4.5. Redutor: Redução de 2% do valor mensal por cada alertas fora do prazo, até o limite de 25% do valor mensal.

5.5. Precisão na Classificação de Ameaças

5.5.1. Métrica: Taxa de falsos positivos <5% nas classificações de ameaças.

5.5.2. Medição: Calculada como:

$$\left[\frac{\text{Número de falsos positivos}}{\text{Total de alertas emitidos}} \right] \times 100$$
, com base em validação conjunta entre Contratante e Fornecedor.

5.5.3. Redutor: Redutor de 3% do valor mensal por cada 1% acima de 5%, até o limite de 25% do valor mensal.

5.6. Frequência e Qualidade de Relatórios

5.6.1. Métrica (A): Relatórios semanais: Entregues toda segunda-feira até 12:00 (horário local do Contratante).

5.6.2. Métrica (B): Relatórios mensais detalhados: Entregues até o 5º dia útil do mês.

5.6.3. Medição: Conformidade com prazos e completude do conteúdo, avaliada pelo Contratante.

5.6.4. Redutor: Redutor de 1% do valor mensal por relatório atrasado ou incompleto, limitado a 25% do valor mensal.

5.7. Compartilhamento de IoCs

5.7.1. Métrica (A): IoCs fornecidos em tempo real (<15 minutos após validação).

5.7.2. Métrica (B): 95% dos IoCs devem ser acionáveis e validados.

5.7.3. Medição: Tempo de entrega acima da métrica (A) e taxa de IoCs úteis (B), verificada pelo Contratante.

5.7.4. Redutor: Redutor de 2% do valor mensal por cada IoCs com tempo de entrega acima da métrica (A) ou por cada 1% abaixo do percentual da métrica (B) até o limite de 25% do valor mensal.

5.8. Integração com SIEM/SOAR

5.8.1. Métrica (A): Taxa de falhas de integração (ex.: erros de API, logs perdidos) <1%.

5.8.2. Métrica (B): Suporte a respostas automatizadas via SOAR em <1 minuto para eventos críticos.

5.8.3. Medição: Testes de integração e monitoramento contínuo.

5.8.4. Redutor: redução de 5% do valor mensal para cada 1% superior de taxa de falha de integração (A) ou para cada minuto superior do suporte a respostas automatizadas (B) acima da métrica, até 25% do valor mensal.

5.9. A parcela mensal terá o limite de redução de 75% do total quando somados os redutores.

6. RESPONSABILIDADES

6.1. A CONTRATADA deve designar um especialista técnico de ponto de contato para comunicação com o Banco, durante toda a vigência do contrato.

6.2. A CONTRATADA deve comunicar sobre mudanças em sistemas ou políticas que possam afetar o serviço.

6.3. A CONTRATADA deve realizar Monitoramento contínuo e entrega periódica de Relatórios.

6.4. A CONTRATADA deve realizar reuniões:

6.4.1. Semanal: Revisão de incidentes e alertas.

6.4.2. Mensal: Análise de desempenho do SLA e tendências de ameaças.

6.5. Relatórios de Conformidade: A CONTRATADA fornecerá um relatório mensal detalhando o cumprimento de cada métrica, incluindo justificativas para descumprimentos.

ANEXO I-B**ESPECIFICAÇÕES E CARACTERÍSTICAS TÉCNICAS DOS SERVIÇOS****1. FINALIDADE**

Este anexo descreve como deverão ser prestados os serviços relacionados a contratação de empresa especializada em Inteligência de Ameaças Cibernéticas (*Cyber Threat Intelligence - CTI*) e prevenção a fraudes, conforme descrito a seguir.

- 1.1. Para a contratação do serviço de CTI, a quantidade estimada e os respectivos ativos de informação a serem monitorados são os seguintes:

Tópico	Descrição	Ativos	Quantidade
1	Monitoração da surface web, deep web, e dark web	Pessoas de Interesse	20
2	Monitoração da surface web, deep web, e dark web	Produtos/Marcas	20
3	Sites e contas fraudulentas	Takedown por Ano	180
4	Monitoração de fontes de informações	Domínios/Subdomínios	25
5	Monitoração de vazamento de informações	Nomes de Empresas Fornecedoras	25

- 1.2. Para fins de contagem do limite de pedidos de *takedown* (tópico 3), serão considerados apenas os casos em que a remoção do conteúdo for comprovadamente realizada pela CONTRATADA.
- 1.3. O quantitativo estimado de *takedown* corresponde ao período de 12 meses, sendo zerado anualmente na data de aniversário do contrato.

2. REQUISITOS GERAIS

- 2.1. Os serviços deverão ser prestados fora das dependências do Banco do Nordeste.
- 2.2. O serviço de CTI deverá prover uma console de acesso para que o Banco e as equipes do seu SOC (serviços de SOC e SIEM não fazem parte do escopo desta contratação) possam consultar as informações de inteligência de ameaças cibernéticas.
- 2.3. Todos os custos envolvidos na prestação dos serviços, tais como: alocação de pessoas, aluguel, energia, computadores, softwares e demais custos serão de inteira responsabilidade da CONTRATADA.
- 2.4. Além dos ativos de TIC, o serviço deve monitorar e reportar indicativos de uma listagem de serviços de tecnologias e softwares que são utilizadas pelo Banco do Nordeste.
- 2.5. O serviço deve monitorar as BINs de cartões informados pelo Banco, verificando se o padrão corresponde a um número de cartão válido.
- 2.6. O serviço deve monitorar e reportar indicativos de ameaças a usuários do domínio @bnb.gov.br, inclusive as credenciais vazadas do Banco.
- 2.7. Para efeito de reporte, o serviço de CTI irá gerar eventos em, pelo menos, 3 categorias:

Eventos de Informação: Estes eventos não requerem qualquer ação. Este grupo de eventos deve ser utilizado quando não há risco cibernético aos ativos de TIC e de informação monitorados, por exemplo, uma menção simples em uma rede social contendo o nome dos ativos de TIC e de informação do CONTRATANTE;

Eventos de Aviso: Este grupo de eventos deve ser utilizado quando existe algum comportamento que represente risco cibernético em relação aos ativos de TIC e de informação monitorados, por exemplo, uma menção na internet, deep ou dark web, ou qualquer outro meio monitorado, com contexto de ameaças e/ou ataques cibernéticos direcionados contra o BNB;

Eventos de Exceção: Estes eventos são aqueles que sugerem que os princípios da PSIBC (confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade, privilégio mínimo, necessidade de conhecer, proteção de dados pessoais e proteção da privacidade), foram impactados negativamente. São exemplos desses eventos: detecção de um vazamento de dados do CONTRATANTE e venda de informações atreladas aos ativos de informação monitorados em canais de fraude.

- 2.8. O BNB deverá fornecer previamente à CONTRATADA responsável pelo serviço de CTI a lista de ativos de informação a serem monitorados.
- 2.9. A lista de ativos de informação pode ser alterada, caso seja necessário, para atender às demandas de segurança cibernética da instituição, sendo sempre comunicadas à CONTRATADA para devida atualização do monitoramento.
- 2.10. Caso a CONTRATADA identifique a ausência de insumos necessários para a geração dos Eventos, será responsabilidade da CONTRATADA a correção e/ou habilitação de tal insumo. O BNB, sempre que solicitado, repassará para a CONTRATADA as informações necessárias para aprimorar este processo.
- 2.11. O serviço deverá ser acessível, através de API e Console, com as seguintes características:
 - 2.11.1. Devem ser disponibilizados, no mínimo, 10 (dez) usuários com acessos simultâneos;
 - 2.11.2. Deve ter a autenticação integrada com Microsoft Entra ID (Antigo Azure AD) do BNB.
 - 2.11.3. Não deve ser instalado na infraestrutura de TIC do BNB;
- 2.12. O serviço deverá disponibilizar a console via interface web, por meio de URL segura (HTTPS), TLS v 1.2 e cifras fortes além de configuração de HSTS.
- 2.13. Da Confidencialidade, Integridade e Disponibilidade dos dados de CTI, a CONTRATADA deverá:
 - 2.13.1. Implementar os controles necessários para que apenas os seus profissionais, bem como os usuários e grupos criados por esta instituição, tenham acesso às pesquisas realizadas e aos dados armazenados;
 - 2.13.2. Se responsabilizar pela guarda das informações coletadas por período a ser definido pelo BNB, não menor que 12 (doze) meses;
 - 2.13.3. Realizar cópia de segurança dos dados coletados em razão dos ativos de informação monitorados, de forma a permitir ao menos a restauração das pesquisas realizadas e de seus

resultados. Observação: Essas informações, quando solicitadas pelo BNB, devem ser repassadas nos formatos HTML, PDF, CSV, Planilha eletrônica e DOCX.

2.13.4. Disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, contexto, metadados e tipo da fonte.

2.13.5. Gerar e armazenar trilhas de auditoria que permitam o rastreamento de ações efetuadas em todas as contas de usuários. Os registros de logs devem conter, no mínimo, a data e hora do evento, origem de acesso, usuário, hostname do equipamento e ação/pesquisa efetuada.

3. SOBRE A CONSOLE DO CTI

3.1. Não limitar quantidade de recursos pesquisados;

3.2. Prover pesquisa direcionada através da monitoração de palavras pré-selecionadas fornecidas;

3.3. Possuir modelos de filtro de informações pré-configurados, personalizados de acordo com comportamentos conhecidos dos usuários na utilização das diferentes fontes de informação monitoradas.

3.4. Possibilitar salvar os resultados das pesquisas já realizadas e apresentar os dados filtrados em painéis com as principais fontes identificadas na busca.

3.5. Permitir a navegação com clicks nos tipos de informações de interesse do painel, com apresentação das informações relacionadas.

3.6. Prover um campo de descrição em que os analistas de segurança cibernética do BNB, ou da CONTRATADA, possam contextualizar as informações associadas aos eventos. Este recurso deve facilitar o consumo das informações de CTI pelas equipes de segurança cibernética, a exemplo das equipes do serviço de CSOC;

3.7. Permitir a pesquisa de informações nos seguintes contextos:

3.7.1. Ameaças cibernéticas;

3.7.2. Resposta a incidentes;

3.7.3. Prevenção de perdas de dados;

3.7.4. Proteção de Marca e Executivos;

3.7.5. Risco de Terceiros;

3.7.6. Fraude;

3.7.7. Quaisquer outras fontes disponíveis, ou que venham a se tornar disponíveis.

3.8. Apresentar a descoberta de páginas web de "phishing", utilizando o nome dos recursos pesquisados, a marca, identidade visual, domínios e ativos de informação que serão protegidas;

3.9. Apresentar a verificação de sites suspeitos de phishing para domínios solicitados pelo CONTRATANTE, ou que tenham sido levantados pela CONTRATADA. Para essa verificação deve-se utilizar, entre outras, as seguintes entidades reguladoras: ICANN (Internet Corporation for Assigned Names and Numbers) e Registro.Br (Registro de Domínios para a Internet do Brasil);

3.10. Apresentar a detecção de domínios recentemente registrados que possam oferecer riscos e serem utilizados de forma maliciosa contra o BNB como, por exemplo:

3.10.1. Variações comuns de nomes;

- 3.10.2. Permutações de caracteres; e
- 3.10.3. Desvio de URL (typosquatting);
- 3.10.4. Domínios exatos em diferentes TLDs.
- 3.11. Nos domínios monitorados a solução deve:
 - 3.11.1. Identificar a emissão de certificados;
 - 3.11.2. Identificar a criação de domínios de recursos monitorados;
- 3.12. Identificar a desfiguração de sítio (detecção via código-fonte ou OCR);
- 3.13. Identificar a indisponibilidade de domínios (>5 min);
- 3.14. Identificar diretórios sensíveis e possíveis exposições de dados;
- 3.15. Identificar anomalias no registro de URL, timestamp, categoria, snapshot e código-fonte;
- 3.16. A solução deve realizar consulta Whois de forma automática nos Bots que realizam coletas de domínios.
- 3.17. Os resultados das pesquisas no Console de CTI devem, no mínimo:
 - 3.17.1. Retornar os seguintes campos: contexto pesquisado, data da menção e/ou exposição, data e hora de criação do alerta, idioma, endereço (web/deep web/dark web) e conteúdo original completo;
 - 3.17.2. Permitir que as pesquisas sejam salvas para posterior verificação.
 - 3.17.3. Permitir que os resultados exibidos sejam ordenados conforme o interesse do usuário sendo ordenáveis por data e hora da ocorrência mais recente para a mais antiga, e por tema, ameaça, entre outros;
 - 3.17.4. Permitir a atualização automática do resultado de pesquisas anteriormente realizadas com alertas visuais dessas atualizações;
 - 3.17.5. Disponibilizar as informações das pesquisas por, no mínimo: intervalo de data, contexto, metadados e tipo da fonte;
 - 3.17.6. Possuir interface de fácil visualização para demonstrar os resultados das buscas por cada categoria de fonte realizada, (fontes abertas, fóruns, blogs, redes sociais, aplicativos de mensagens instantâneas, deep web e dark web);
 - 3.17.7. Disponibilizar uma tela com informações consolidadas para visualização das pesquisas realizadas e alertas cadastrados;
 - 3.17.8. Permitir exportar qualquer pesquisa realizada de forma manual ou automática para os seguintes formatos: HTML, PDF, CSV, Planilha eletrônica e DOCX;
- 3.18. Este Serviço de INTELIGÊNCIA DE AMEAÇAS CIBERNÉTICAS deve:
 - 3.18.1. Monitorar ameaças contidas na internet aberta, deep web e dark web, em temas que possam ameaçar pessoas de interesse, ativos de informação e sistemas de TIC do BNB, do ponto de vista da segurança cibernética. O monitoramento nestes 3 ambientes compreende, mas não se limita, às mídias como: domínios, sites, blogs, vlogs, fóruns, chats de mensagens e redes sociais;

- 3.18.2. Monitorar as lojas de aplicativos Apple Store e Google Play com o objetivo de detectar aplicativos maliciosos que estejam relacionados com o BNB. É de responsabilidade da CONTRATADA providenciar a remoção de aplicações falsas e maliciosas através de parcerias com as lojas de aplicativos, quando solicitado pelo BNB;
- 3.18.3. Monitorar fontes de informações como Shodan, BinaryEdge, Zone-H, Bases de CVE, entre outras, bem como sites que compartilhem informações sobre TTPs utilizados para ataques como phishing, ransomware, entre outros;
- 3.18.4. Monitorar listagem detalhada de serviços vulneráveis (DNS, NTP, FTP, SMB, etc.), vulnerabilidades clássicas (HeartBleed, Poodle, Logjam, etc.), Google Dorks para descoberta, registro com CVE, CWE, payload, geolocalização, provedor, protocolo, severidade (CVSS);
- 3.18.5. Monitorar ameaças cibernéticas contidas nas redes sociais em temas que possam ameaçar pessoas de interesse, ativos de informação e sistemas de TIC do BNB, do ponto de vista da segurança cibernética. As redes sociais, compreendem, mas não se limitam à: Twitter, Facebook, Youtube, Instagram, TikTok, LinkedIn, WhatsApp, Discord, Telegram, Pastebin, Ghostbin, Scribd, Reclame Aqui, Apple Store, 4Shared, Google Play, Vimeo e Github, Gitlab e feeds RSS;
- 3.18.6. Monitorar ameaças representadas por domínios suspeitos ou fraudulentos e em seguida realizar o takedown desses domínios. A CONTRATADA se obriga a realizar todo o processo para retirada do ar desses sites que contenham phishing ou sites que disparem spam utilizando-se do nome, da marca ou da imagem do BNB, mesmo que similar, (com intuito de confundir e aplicar fraudes ou golpes nos usuários dos serviços prestados pelo BNB). A CONTRATADA deve prover serviço de monitoramento de domínios nacionais e internacionais, incluindo Top-Level Domain (TLDs) e Generic Top-Level Domain (gTLDs) e Country Code Top-Level Domain (ccTLD), que verifique a utilização do uso indevido das marcas do BNB no nome do domínio ou na URL, a empresa que administra o registro do domínio, e os dados do proprietário do domínio. A CONTRATADA deverá emitir um alerta, atualizado conforme andamento do atendimento, para acompanhamento do processo de takedown de cada ocorrência.
- 3.18.7. Fruto do monitoramento do item anterior, pode ser necessário remover perfis falsos, desde que estejam relacionados com os ativos de informação monitorados. Será obrigação da CONTRATADA estabelecer parcerias com as principais redes sociais para os procedimentos de desativação desses perfis falsos, quando solicitado pelo BNB;
- 3.18.8. Monitorar ameaças, ataques e vulnerabilidades contidas em aplicativos de mensagens, como por exemplo WhatsApp e Telegram, em temas que possam ameaçar pessoas de interesse, ativos de informação e sistemas de TIC do BNB, do ponto de vista da segurança cibernética;
- 3.19. A solução deve fornecer um painel de visualização que contemple, no mínimo:
 - 3.19.1. Visualização de eventos relacionados às palavras-chaves;

- 3.19.2. Realização de buscas nos dados incluindo buscas avançadas com critérios e entidades diferentes;
 - 3.19.3. Navegação com clicks nos tipos de informações de interesse do painel, com apresentação das informações relacionadas.
 - 3.19.4. Apresentação dos dados buscados em painéis com as principais fontes identificadas na busca;
- 3.20. A solução deve possuir um *dashboard* para análise dos dados coletados com, no mínimo:
- 3.20.1. Gráfico com a quantidade de informações de acordo com palavras ou termos buscados;
 - 3.20.2. Divisão dos dados por tipo de dado encontrado (imagem, texto, áudio etc.);
 - 3.20.3. Principais perfis;
 - 3.20.4. Principais fontes de dados;
 - 3.20.5. Principais grupos.
- 3.21. A solução deve permitir configuração de alertas diretamente via interface de gerenciamento.
- 3.22. A solução deve permitir, através da interface de gerenciamento, que se realizem testes de funcionamento dos alertas configurados, bem como também deve permitir a configuração de envio de alertas, no mínimo, via e-mail e SMS.
- 3.23. A solução deve permitir a configuração de alertas baseados em:
- 3.23.1. consultas/pesquisas salvas;
 - 3.23.2. CPF vazado/exposto;
 - 3.23.3. citações de pessoas importantes (VIP);
 - 3.23.4. credenciais de domínios cadastrados;
 - 3.23.5. cartão de crédito vazados.
- 3.24. A solução deve permitir filtrar os resultados da busca por data de recebimento da credencial vazada e por tipo de vazamento.
- 3.25. A solução deve permitir filtrar os resultados da busca por credenciais internas ou por credenciais de terceiros em domínios institucionais.
- 3.26. A solução deve fornecer busca direta por IP com honeyscore, de exploits integrada à base (ExploitDB/Metasploit).
- 3.27. A solução deve fornecer filtros personalizados que possibilitem a consulta de incidentes por campos diversos, tais como, URL, IP, data, status, assunto e remetente.
- 3.27.1. A solução deve disponibilizar mecanismo para busca das informações, permitindo buscas por intervalo de data, metadados específicos, fontes de informação, palavras-chaves, bem como por perfis específicos, usando nome/apelido, número de telefone ou e-mail, com no mínimo os seguintes campos: fonte; nome; apelido; telefone; e grupos.
- 3.28. A solução deve disponibilizar, através de interface web, busca utilizando mecanismos como: proximidade, lógica *fuzzy* (difusa), lógica binária, expressões regulares (regex), operadores lógicos ("AND", "OR" e "NOT") e caracteres *wildcard* (coringa).

- 3.29. A solução deve permitir a ordenação dos resultados por data da postagem mais recente para a mais antiga.
- 3.30. A solução deve permitir salvar o resultado da pesquisa.
- 3.31. A solução deve possuir um painel de visualização de todas as pesquisas salvas, possibilitando a execução dessas pesquisas salvas.
- 3.32. A solução deve possuir mecanismo que permita que buscas criadas possam ser salvas para uso posterior.
- 3.33. A solução deve permitir a criação/alteração/exclusão de variáveis na plataforma, possibilitando gerenciamento de termos ou buscas dentro dessa variável.
- 3.34. A ferramenta deve permitir o drill-down das pesquisas utilizando filtros inclusivos e exclusivos;

4. MONITORAMENTO DE MARCA, PRODUTOS E EXECUTIVOS

O monitoramento de marca, produtos e executivos envolve rastrear menções *online* (em redes sociais, fóruns, dark web, etc.) para identificar ameaças como campanhas de difamação, vazamentos de dados ou tentativas de phishing direcionadas. Ferramentas como Brandwatch, Recorded Future ou soluções baseadas em OSINT (Open-Source Intelligence). IA deve ser utilizada para analisar os eventos de forma contextual, detectando anomalias em tempo real e classificando-as por prioridade, com o objetivo de proteger a reputação e identificar ataques direcionados a executivos do Banco (ex.: spear phishing). A seguir os requisitos para monitoramento de marca, produtos e executivos:

- 4.1. Monitorar menções à marca em tempo real em redes sociais, fóruns, blogs e mídia tradicional.
- 4.2. Rastrear a dark web e deep web para identificar vazamentos de dados ou credenciais relacionadas à marca ou executivos.
- 4.3. Detectar campanhas de difamação ou desinformação contra a marca ou executivos.
- 4.4. Identificar atividades voltadas para tentativas de phishing direcionado (spear phishing) contra executivos.
- 4.5. Monitorar perfis falsos ou não autorizados que imitem a marca ou executivos em plataformas digitais.
- 4.6. Fornecer alertas em tempo real sobre menções sensíveis ou ameaças à reputação.
- 4.7. Analisar contextualmente menções públicas que expressem sentimentos ou tendências negativas, classificando-as conforme o conteúdo transmitido (uso de palavras ofensivas, ameaças, dentre outros).
- 4.8. Rastrear uso indevido de logotipos, marcas registradas ou propriedade intelectual.
- 4.9. Monitorar marketplaces ilícitos para detectar vendas de dados roubados relacionados à marca.
- 4.10. Fornecer relatórios detalhados sobre atividades suspeitas envolvendo executivos (ex.: doxxing).
- 4.11. Utilizar ferramentas de OSINT (Open-Source Intelligence) para coleta de dados públicos.
- 4.12. Identificar tentativas de engenharia social direcionadas a executivos ou funcionários-chave.

- 4.13. Monitorar plataformas de mensagens instantâneas (ex.: Telegram, Discord) para ameaças à marca.
- 4.14. Garantir anonimato nas operações de monitoramento para proteger o contratante.
- 4.15. Fornecer painéis interativos para visualização de dados de monitoramento de marca.

5. CLASSIFICAÇÃO E PRIORIZAÇÃO DE RISCOS

A solução deve providenciar a classificação de riscos com base em probabilidade, impacto e criticidade dos ativos envolvidos. A priorização dos riscos pode ser automatizada com IA, que analisa dados históricos e contexto (ex.: vulnerabilidades críticas em sistemas expostos).

- 5.1. Utilizar frameworks reconhecidos (ex.: MITRE ATT&CK, NIST) para classificação de riscos.
- 5.2. Utilizar ferramentas (ex.: RiskLens ou métodos qualitativos/quantitativos) para priorizar os riscos.
- 5.3. Avaliar riscos com base em probabilidade, impacto e criticidade dos ativos.
- 5.4. Priorizar ameaças com base em contexto organizacional (ex.: setor, localização, tamanho).
- 5.5. Fornecer scores de risco quantitativos e qualitativos para cada ameaça identificada.
- 5.6. Atualizar a priorização de riscos em tempo real com base em novos dados de inteligência.
- 5.7. Identificar riscos específicos para fraudes financeiras, como BEC (Business Email Compromise).
- 5.8. Classificar ameaças por tipo (ex.: malware, phishing, insider threats).
- 5.9. Integrar dados de inteligência interna do contratante na avaliação de riscos.
- 5.10. Fornecer relatórios de riscos com recomendações acionáveis para mitigação.
- 5.11. Priorizar riscos com base em vulnerabilidades conhecidas em sistemas do contratante.
- 5.12. Garantir transparência na metodologia de classificação de riscos.
- 5.13. Oferecer suporte para revisão periódica da matriz de riscos.
- 5.14. Identificar riscos emergentes com base em tendências globais de cibersegurança.
- 5.15. Fornecer análise de impacto potencial de fraudes em operações e reputação.

6. UTILIZAÇÃO DE IA PARA CLASSIFICAÇÃO DE AMEAÇAS

- 6.1. Utilizar modelos de aprendizado de máquina (ML) para detectar padrões de ameaças em tempo real.
- 6.2. Empregar processamento de linguagem natural (PLN) para analisar comunicações maliciosas (ex.: e-mails de phishing).
- 6.3. Treinar modelos de IA com dados históricos de fraudes relevantes ao setor do contratante.
- 6.4. Reduzir falsos positivos por meio de algoritmos de IA otimizados.
- 6.5. Fornecer explicabilidade (explainable AI) para decisões de classificação de ameaças.
- 6.6. Atualizar continuamente os modelos de IA com novos dados de inteligência.
- 6.7. Utilizar IA para correlacionar dados de fontes díspares (ex.: logs, OSINT, dark web).
- 6.8. Implementar IA para prever campanhas de fraude com base em tendências.

- 6.9. Garantir que os modelos de IA sejam auditáveis e conformes com regulamentações.
- 6.10. Fornecer relatórios sobre a eficácia da IA na detecção de ameaças.
- 6.11. Utilizar IA para identificar ameaças de baixa visibilidade (ex.: ataques de cadeia de suprimentos).
- 6.12. Integrar IA com ferramentas de visualização para facilitar a análise de ameaças.
- 6.13. Garantir que os dados usados para treinar IA respeitem privacidade e conformidade.
- 6.14. Oferecer personalização de algoritmos de IA para atender às necessidades específicas do contratante.

7. REQUISITOS DE DETECÇÃO E INTERRUPTÃO DE CAMPANHAS MALICIOSAS

- 7.1. Detectar campanhas de phishing em tempo real, incluindo e-mails e sites falsos.
- 7.2. Identificar atividades voltadas para ataques de DDoS e tentativas de interrupção de serviços.
- 7.3. Rastrear campanhas de desinformação ou propaganda maliciosa contra a marca.
- 7.4. Detectar atividades voltadas para malware personalizado usado em fraudes ou ataques direcionados.
- 7.5. Monitorar atividades de botnets que afetem o contratante ou seus clientes.
- 7.6. Identificar atividades voltadas para tentativas de fraude financeira, como transferências não autorizadas.
- 7.7. Fornecer mecanismos para interromper campanhas via takedown de domínios maliciosos.
- 7.8. Colaborar com provedores de serviços (ex.: ISPs, registradores de domínio) para mitigar ataques.
- 7.9. Detectar atividades voltadas para o uso de credenciais vazadas em tentativas de login ou fraudes.
- 7.10. Identificar atividades voltadas para ataques de engenharia social em tempo real (ex.: chamadas fraudulentas).
- 7.11. Fornecer alertas imediatos sobre campanhas maliciosas em andamento.
- 7.12. Analisar padrões de ataque para antecipar próximas fases de campanhas.
- 7.13. Detectar atividades voltadas para campanhas de ransomware antes da execução completa.
- 7.14. Monitorar atividades de grupos APT (Ameaças Persistentes Avançadas) relevantes.
- 7.15. Analisar atividades maliciosas utilizando:
 - 7.15.1. Honeypots global e honeypots internos;
 - 7.15.2. Cobertura de múltiplos protocolos e portas (HTTP, SSH, RDP, SCADA, IoT, etc.);
 - 7.15.3. Integração via API;
 - 7.15.4. IA/LLM para interação realista;
 - 7.15.5. Registro detalhado de ataques e TTPs.
- 7.16. Fornecer relatórios pós-incidente com análise de campanhas detectadas.
- 7.17. Garantir resposta rápida (em minutos) para ameaças críticas.
- 7.18. Detectar atividades voltadas para tentativas de exploração de vulnerabilidades zero-day.
- 7.19. Oferecer suporte para mitigação de campanhas em múltiplos canais (ex.: e-mail, web, redes sociais).

8. REQUISITOS DE COMPARTILHAMENTO DE IOCS (INDICADORES DE COMPROMISSO)

- 8.1. Fornecer IoCs em formatos padronizados (ex.: STIX/TAXII, CSV, JSON).
- 8.2. Compartilhar IoCs em tempo real com a equipe de segurança do contratante.
- 8.3. Garantir que IoCs sejam específicos, acionáveis e contextualizados.
- 8.4. Incluir IoCs como hashes de malware, URLs maliciosas, IPs e domínios.
- 8.5. Participar de redes de compartilhamento de inteligência (ex.: ISACs, FS-ISAC).
- 8.6. Fornecer IoCs com metadados, como nível de confiança e origem.
- 8.7. Garantir que IoCs sejam compatíveis com ferramentas de segurança do contratante.
- 8.8. Atualizar IoCs regularmente com base em novas descobertas.
- 8.9. Proteger IoCs compartilhados contra acesso não autorizado.
- 8.10. Fornecer relatórios sobre a utilização e eficácia dos IoCs compartilhados.
- 8.11. Integrar IoCs com feeds de inteligência de ameaças globais.
- 8.12. Garantir que IoCs sejam validados antes do compartilhamento.
- 8.13. Oferecer suporte para personalização de IoCs com base em necessidades específicas.
- 8.14. Fornecer documentação detalhada sobre o uso de IoCs fornecidos.
- 8.15. Garantir conformidade com regulamentações ao compartilhar IoCs sensíveis.

9. REQUISITOS DE INTEGRAÇÃO COM SIEM/SOAR

- 9.1. Integrar-se com sistemas SIEM populares (ex.: Splunk, QRadar, ArcSight).
- 9.2. Suportar plataformas SOAR (ex.: Palo Alto Cortex XSOAR, ServiceNow).
- 9.3. Fornecer APIs RESTful para integração com ferramentas de segurança existentes.
- 9.4. Garantir compatibilidade com formatos de log como CEF ou Syslog.
- 9.5. Suportar automação de respostas a incidentes via integração com SOAR.
- 9.6. Fornecer playbooks pré-configurados para respostas a fraudes comuns.
- 9.7. Garantir baixa latência na integração de dados com SIEM/SOAR.
- 9.8. Oferecer suporte técnico para configuração inicial de integrações.
- 9.9. Fornecer documentação detalhada sobre APIs e integração.
- 9.10. Garantir que dados enviados ao SIEM/SOAR sejam criptografados.

ANEXO I-C**DISPONIBILIZAÇÃO DOS SERVIÇOS****1. FINALIDADE**

Este anexo descreve as etapas, cronograma, responsabilidades e entregáveis necessários para a implementação dos serviços de *Threat Intelligence* contratados. O objetivo é garantir que o serviço esteja totalmente operacional dentro do prazo acordado, integrado com os sistemas do contratante e alinhado com os requisitos especificados, incluindo monitoramento de marca e executivos, classificação de riscos, utilização de IA, detecção de campanhas maliciosas, compartilhamento de IoCs e integração com SIEM/SOAR.

2. CRONOGRAMA DE DISPONIBILIZAÇÃO DOS SERVIÇOS DA SOLUÇÃO

2.1. O Contratado deverá considerar o cronograma de eventos e prazos abaixo apresentados, para a disponibilização dos serviços da solução. Os prazos informados são considerados como máximos, não impedindo, pois, que sejam cumpridos em prazos menores.

Nº	Evento	Responsável	Prazo
1	Assinatura do Contrato	Banco e Contratado	Imediatamente após a convocação pelo Banco.
2	Planejamento e coleta de informações	Contratado	Até 5 (cinco) dias úteis após o evento 1.
3	Entrega da versão inicial do Plano de disponibilização	Contratado	Até 2 (dois) dias úteis após o evento 2.
4	Entrega da versão final do Plano de disponibilização	Contratado	Até 3 (três) dias úteis após o evento 3.
5	Configuração da solução	Contratado	Até 10 (dez) dias úteis após o evento 3.
6	Integração com sistemas	Contratado	Até 10 (dez) dias úteis após o evento 5.
7	Testes e Validação	Banco e Contratado	Até 10 (dez) dias úteis após o evento 6.
8	Treinamento e Transição	Contratado	Até 10 (dez) dias úteis após o evento 5, em período a ser acordado com o Banco
9	Emissão do Termo de Aceitação Definitivo (TAD)	Banco	Até 3 (três) dias úteis após os eventos 7, condicionada ao aceite do evento 8.

2.2. Todos os termos de aceitação, a serem entregues pelo Banco, estão condicionados à prévia entrega dos componentes e realização das atividades, em conformidade com os requisitos do Edital, e dentro dos prazos estabelecidos.

3. REQUISITOS GERAIS

- 3.1. O CONTRATADO é responsável pelo planejamento, alocação de recursos e definição do cronograma de instalação;
- 3.2. O CONTRATADO deverá documentar os processos de configuração e integração;
- 3.3. Todas as atividades relacionadas à disponibilização da solução serão executadas remotas, através do Microsoft TEAMS e a critério do Banco as reuniões podem ser gravadas;
- 3.4. Em caso de atrasos nas entregas, o Banco poderá solicitar a execução das atividades relacionadas à disponibilização da solução na modalidade presencial, nas instalações do Centro Administrativo

Presidente Getúlio Vargas (CAPGV), do Banco do Nordeste do Brasil, situado à avenida Dr. Silas Munguba 5700, bairro Passaré, CEP. 60743-015, em Fortaleza – CE;

- 3.5. O Contratado deverá criar e manter atualizados documentação das atividades, processos, testes, homologação, entrega e conferência, encontros de trabalho, compromissos e prazos, incluindo planos de trabalho, planos de contingência e atas, de modo a compor uma documentação final da disponibilização a ser entregue ao Banco, no final do processo. Toda a documentação gerada no escopo do projeto deverá ser entregue no idioma português.
- 3.6. O Banco se reserva o direito de redefinir, a qualquer momento da disponibilização, quaisquer fases, ações, prazos e recursos envolvidos, objetivando a garantia de atendimento dos parâmetros de qualidade, segurança, mitigação de riscos e atendimento de prazos, cabendo ao Contratado adequar-se às modificações propostas, refazendo atividades e documentação, caso necessário, desde que essas não extrapolem o escopo dos serviços aqui descritos.
- 3.7. O Contratado será responsável pela execução de quaisquer procedimentos de diagnóstico de problemas relacionados aos serviços de disponibilização dos componentes objetos do Edital. Caso o diagnóstico aponte para problemas não relacionados aos componentes da solução, o Banco deverá adotar as medidas necessárias para saná-los, desde que devidamente comprovados pelo Contratado, e sempre a critério do Banco.
- 3.8. Será de inteira responsabilidade e a expensas do Contratado, sem nenhum custo adicional para o Banco, as atividades de:
 - Disponibilização da solução, incluindo o apoio e suporte técnico e logístico eventualmente necessários ao seu adequado funcionamento;
 - Alocação de profissionais qualificados e todas as obrigações trabalhistas relacionadas;
 - Todos os ônus relativos a transporte, alimentação e hospedagem de profissionais, transporte e instalação de equipamentos, ligações telefônicas para suporte técnico, montagem física dos equipamentos que compõem a solução, disponibilização de ferramentas e insumos diversos, requeridos durante qualquer das fases de disponibilização;
 - Configuração lógica dos componentes, análise técnica de forma a viabilizar, integralmente, os testes a serem realizados, como parte da homologação e o adequado funcionamento em ambiente de produção;
 - Atividades de concepção, projeto, planejamento, implementação, suporte técnico, assistência técnica e apoio logístico, eventualmente necessários à adequada disponibilização da solução;
 - Demonstração de todas as características técnicas e funcionalidades previstas na contratação, durante a fase de homologação de funcionalidades da solução.
- 3.9. O Contratado deverá possuir experiência e estar qualificado a prestar adequadamente os serviços de disponibilização, mediante comprovação nos termos do Edital.
- 3.10. Dentre os profissionais alocados, o Contratado deverá indicar um Gerente de Projetos, funcionário ou contratado da empresa, que será o líder e responsável pela entrega dos serviços e pela disponibilização da solução, e 2 (dois) Especialistas Técnicos, funcionários ou contratados da empresa, que serão responsáveis pela disponibilização da solução de modo a garantir a qualidade dos resultados e o atendimento aos requisitos e prazos estipulados no Edital.
- 3.11. O Gerente de Projetos deverá possuir certificação PMP – Project Management Professional do PMI – Project Management Institute ou possuir MBA – Master of Business Administration em Gerência de Projetos. Os documentos de certificação devem ser apresentados por ocasião da assinatura do Contrato, na versão original ou por qualquer processo de cópia autenticada em Cartório.
- 3.12. O Gerente de Projetos deverá possuir experiência com documentação oficial comprobatória, em projeto(s) de cliente(s) de grande porte, relacionados à disponibilização de soluções de CTI. A referida experiência deverá ser comprovada mediante apresentação de documento(s) timbrado(s), emitido(s) por cliente(s), até 5 (cinco) dias úteis após a assinatura do contrato, contemplando a descrição geral dos serviços prestados, datas inicial e final de execução dos serviços, área responsável por parte do cliente, nome e telefone para contato por parte do cliente e avaliação sucinta

dos resultados, quanto ao cumprimento dos objetivos do projeto, com destaque para o gerenciamento do mesmo.

- 3.13. Os especialistas da equipe técnica deverão possuir experiência, no mínimo de 2 (dois) anos, com documentação oficial comprobatória, em projeto(s) de cliente(s) de grande porte, relacionados à disponibilização de soluções de CTI. A referida experiência deverá ser comprovada mediante apresentação de documento(s) timbrado(s), emitido(s) por cliente(s), até 5 (cinco) dias úteis após a assinatura do contrato, contemplando a descrição geral dos serviços prestados, datas inicial e final de execução dos serviços, área responsável por parte do cliente, nome e telefone para contato por parte do cliente e avaliação sucinta dos resultados, quanto ao cumprimento dos objetivos do projeto, com destaque para o gerenciamento do mesmo.
- 3.14. Será obrigatória a realização de reuniões de acompanhamento, com frequência semanal, durante todo o período de execução da disponibilização da solução, desde a assinatura do contrato até a emissão do TAD (Termo de Aceitação Definitiva), para tratar de assuntos técnicos e gerenciais do projeto. Tais encontros contarão com a presença dos seguintes profissionais:
- Gerente de Projetos (Contratado);
 - Representante da equipe técnica (Contratado);
 - Gerente de Projetos (Banco);
 - Representante da equipe técnica (Banco).
- 3.14.1. A critério do Banco, e de acordo com o andamento das atividades do projeto, a frequência das reuniões de acompanhamento poderá ser alterada.
- 3.15. Os profissionais do Contratado deverão ter alçada para deliberar sobre as questões gerenciais e técnicas discutidas nos encontros, após aprovação prévia de representantes do Banco.
- 3.16. O quadro de profissionais a serem alocados, pelo Contratado, deverá atender às demandas por serviços de apoio e suporte técnico às atividades de configuração, integração, desenvolvimento e à própria disponibilização dos componentes da solução.
- 3.17. O Contratado deverá indicar, por ocasião da assinatura do Contrato, a composição da equipe de especialistas, funcionários ou contratados da empresa, responsáveis pela disponibilização dos componentes da solução.
- 3.18. O Contratado deverá manter atualizada toda a documentação gerada pelo projeto e disponibilizá-la ao Banco, sempre que requerida.

4. ESCOPO DA DISPONIBILIZAÇÃO

- 4.1. Planejamento e coleta de informações contextuais do contratante (ex.: ativos críticos, marca, executivos).

4.1.1. Plano de Gerenciamento do Projeto

- 4.1.1.1. O Contratado deverá apresentar, ao Banco, em reunião própria, quando da entrega da versão inicial do Plano de Disponibilização, documentos de gerenciamento do projeto, com as informações necessárias para fornecer subsídios que possibilitem controle efetivo do projeto, a serem validados pelo Banco. São eles:

- Plano de Gerenciamento do Escopo;
- Plano de Gerenciamento do Cronograma;
- Plano de Gerenciamento de Recursos Humanos;
- Plano de Gerenciamento das Comunicações;
- Plano de Gerenciamento de Riscos;
- Plano de Gerenciamento da Qualidade;
- Declaração detalhada do escopo do projeto;
- EAP – Estrutura Analítica do Projeto;
- Lista de Riscos e Plano de Resposta aos Riscos do Projeto;
- Cronograma do Projeto;

- Relatório de Desempenho e Status do Projeto;
- Formulário de Requisição de Mudanças;
- Ata de Reuniões.

4.1.2. Plano de Disponibilização da solução:

4.1.2.1. O Plano de Disponibilização da solução deverá consolidar as informações e descrever os procedimentos e prazos necessários para a execução das atividades de disponibilização dos serviços. Deverá ser composto, no mínimo, pelos seguintes documentos:

- Descrição detalhada das atividades de integração que serão efetuadas e a metodologia a ser utilizada na implementação da integração;
- Descrição detalhada dos ativos críticos do Banco com domínios, marcas registradas, IPs, dentre outros identificados na fase de planejamento.
- Descrição detalhada dos executivos a serem monitorados do Banco, devendo ser integrado ao MeuRH para atualização automática dos executivos, em caso de alteração pelo Banco.
- Descrição detalhada dos requisitos de conformidade com LGPD e regulamentos do BACEN.
- Visão genérica do processo de gerenciamento dos componentes disponibilizados na solução.

4.2. Configuração das ferramentas e plataformas de Threat Intelligence, incluindo monitoramento de marca e executivos, classificação de riscos, utilização de IA, detecção de campanhas maliciosas, compartilhamento de IoCs, alertas, relatórios, painéis e dashboards.

4.3. Treinamento da equipe do contratante.

4.4. Testes e validação da solução.

4.5. Transição para operação contínua com monitoramento e suporte.

5. FASES DA DISPONIBILIZAÇÃO

5.1. Fase 1: Planejamento e coleta das informações

5.1.1. **Duração:** 5 dias úteis

5.1.2. **Objetivo:** Definir escopo detalhado, coletar informações e alinhar expectativas.

5.1.3. Atividades:

5.1.3.1. Reunião de kick-off com as equipes do contratante e do fornecedor.

5.1.3.2. Coleta de informações sobre:

5.1.3.2.1. Infraestrutura de TI (ex.: sistemas SIEM/SOAR, firewalls).

5.1.3.2.2. Ativos críticos (ex.: domínios, marcas registradas, IPs).

5.1.3.2.3. Executivos a serem monitorados (ex.: CEO, CFO).

5.1.3.2.4. Requisitos de conformidade (ex.: LGPD, GDPR).

5.1.3.3. Definição de pontos de contato e canais de comunicação.

5.1.3.4. Elaboração do plano detalhado de disponibilização (com cronograma ajustado).

5.1.3.5. Assinatura de NDA (Non-Disclosure Agreement), se ainda não realizado.

5.1.4. Responsabilidades:

5.1.4.1. CONTRATADO: Liderar a reunião de kick-off, fornecer questionário de coleta de dados.

5.1.4.2. CONTRATANTE: Nomear ponto de contato, fornecer informações solicitadas.

5.1.5. Entregáveis:

5.1.5.1. Plano de Gerenciamento do Projeto.

5.1.5.2. Questionário preenchido com informações do contratante.

5.1.5.3. Plano detalhado de disponibilização.

5.2. Fase 2: Configuração da solução

5.2.1. **Duração:** 10 dias úteis

5.2.2. **Objetivo:** Configurar as ferramentas de Threat Intelligence.

5.2.3. Atividades:

- 5.2.3.1. Configuração da plataforma de Threat Intelligence (ex.: acesso ao portal, feeds de inteligência).
- 5.2.3.2. Configuração de monitoramento:
 - 5.2.3.2.1. Cadastro de palavras-chave da marca e perfis de executivos.
 - 5.2.3.2.2. Definição de fontes de dados (ex.: X, dark web, fóruns).
- 5.2.3.3. Personalização de modelos de IA:
 - 5.2.3.3.1. Ajuste de algoritmos para reduzir falsos positivos (<5%).
 - 5.2.3.3.2. Incorporação de dados históricos do contratante, se disponíveis.
- 5.2.3.4. Configuração de alertas, relatórios, painéis e dashboards (ex.: frequência, destinatários, formato).
- 5.2.4. **Responsabilidades:**
 - 5.2.4.1. CONTRATADO: Configurar ferramentas, realizar integrações, documentar processos.
 - 5.2.4.2. CONTRATANTE: Fornecer acesso a sistemas (ex.: credenciais de API), validar configurações.
- 5.2.5. **Entregáveis:**
 - 5.2.5.1. Relatório de configuração (detalhando ferramentas e integrações).
 - 5.2.5.2. Documentação técnica (ex.: endpoints de API, formatos de IoCs).
 - 5.2.5.3. Playbooks SOAR iniciais (mínimo de 3, ex.: phishing, malware, vazamento de dados).
- 5.3. **Fase 3: Integração com sistemas**
 - 5.3.1. **Duração:** 10 dias úteis
 - 5.3.2. **Objetivo:** Configurar as integrações com os sistemas de SIEM/SOAR do contratante.
 - 5.3.3. **Atividades:**
 - 5.3.3.1. Integração com SIEM/SOAR:
 - 5.3.3.1.1. Configuração de APIs RESTful para envio de logs e IoCs.
 - 5.3.3.1.2. Testes de compatibilidade com formatos (ex.: STIX/TAXII, CEF, Syslog).
 - 5.3.3.1.3. Criação de playbooks SOAR para respostas automatizadas (ex.: bloqueio de IPs maliciosos).
 - 5.3.3.2. Integração com MEURH:
 - 5.3.3.2.1. Configuração de integração com MEURH para atualização automática dos executivos, em caso de alteração pelo Banco;
 - 5.3.4. **Responsabilidades:**
 - 5.3.4.1. CONTRATADO: Configurar ferramentas, realizar integrações, documentar processos.
 - 5.3.4.2. CONTRATANTE: Fornecer acesso a sistemas (ex.: credenciais de API), validar configurações.
 - 5.3.5. **Entregáveis:**
 - 5.3.5.1. Relatório de configuração (detalhando ferramentas e integrações).
 - 5.3.5.2. Playbooks SOAR iniciais (mínimo de 3, ex.: phishing, malware, vazamento de dados).
 - 5.3.5.3. Integração bem-sucedida com SIEM/SOAR (100% dos eventos registrados).
- 5.4. **Fase 4: Testes e Validação**
 - 5.4.1. **Duração:** 10 dias úteis
 - 5.4.2. **Objetivo:** Validar a eficácia do serviço por meio de testes e simulações.
 - 5.4.3. **Atividades:**
 - 5.4.3.1. Execução de simulações:
 - 5.4.3.1.1. Simulação de cenários reais (ex.: campanha de phishing, perfil falso no X, vazamento de dados na dark web).
 - 5.4.3.1.2. Teste de detecção de ameaças (ex.: tempo de alerta, precisão da IA).
 - 5.4.3.1.3. Validação de interrupção de campanhas (ex.: takedown de domínio falso).
 - 5.4.3.2. Testes de integração:
 - 5.4.3.2.1. Verificação de envio de IoCs ao SIEM (ex.: 100% dos eventos registrados).
 - 5.4.3.2.2. Teste de automação SOAR (ex.: bloqueio automático de IPs).
 - 5.4.3.3. Validação de relatórios:
 - 5.4.3.3.1. Geração de relatório de teste (semanal e pós-incidente).
 - 5.4.3.3.2. Feedback do contratante sobre formato e conteúdo.
 - 5.4.3.4. Ajustes com base nos resultados das simulações (ex.: redução de falsos positivos, ajuste de alertas).

5.4.4. Responsabilidades:

- 5.4.4.1. CONTRATADO: Conduzir simulações, realizar testes, ajustar configurações.
- 5.4.4.2. CONTRATANTE: Participar das simulações, fornecer feedback, validar resultados.

5.4.5. Entregáveis:

- 5.4.5.1. Relatório das simulações (resultados, métricas, lições aprendidas).
- 5.4.5.2. Relatórios de teste (ex.: semanal, pós-incidente).
- 5.4.5.3. Evidências de integração (ex.: logs do SIEM com IoCs).
- 5.4.5.4. Solução validada com taxa de falsos positivos <5% e detecção de >95% das ameaças simuladas.

5.5. Fase 5: Treinamento e Transição

5.5.1. **Duração:** Durante o expediente, com carga horária diária de 4 (quatro) horas.

5.5.2. Local: Remota, através da ferramenta Microsoft Teams e gravação pelo BNB.

5.5.3. Carga horária: 20 horas.

5.5.4. **Objetivo:** Capacitar a equipe do contratante e iniciar a operação contínua.

5.5.5. Qualificação: O instrutor deverá possuir no mínimo 2 (dois) anos de experiência comprovada na solução,

5.5.6. Atividades:

5.5.6.1. Treinamento para a equipe do contratante:

- 5.5.6.1.1. Uso da plataforma de Threat Intelligence (ex.: navegação no portal, análise de alertas).
- 5.5.6.1.2. Interpretação de relatórios e IoCs.
- 5.5.6.1.3. Resposta a incidentes com base em playbooks SOAR.
- 5.5.6.1.4. Sessões práticas (ex.: análise de um alerta simulado).
- 5.5.6.1.5. Apresentação da solução e conceitos fundamentais;
- 5.5.6.1.6. Descrição das funcionalidades e navegação em cada módulo da ferramenta e seus modos de funcionamento;
- 5.5.6.1.7. Configuração de robôs / rotinas automatizadas;
- 5.5.6.1.8. Configuração de alertas;
- 5.5.6.1.9. Pesquisa simples e avançada;
- 5.5.6.1.10. Operação completa da solução;
- 5.5.6.1.11. Criação de ocorrências dentro da plataforma;
- 5.5.6.1.12. Exportação de dados;
- 5.5.6.1.13. Relatórios: criação, customização, geração e agendamento de relatórios.
- 5.5.6.1.14. Funções de filtragem de eventos e construção de métricas para relatórios.
- 5.5.6.1.15. Funções administrativas básicas: visão geral das configurações da ferramenta e de perfis de acesso, visão geral de monitoramento da ferramenta e solução de problemas, configurações de segurança.
- 5.5.6.1.16. Transferência de conhecimento:
- 5.5.6.1.17. Documentação de processos (ex.: como escalar alertas críticos).
- 5.5.6.1.18. Guia de usuário para a plataforma.

5.5.6.2. Início da operação contínua:

- 5.5.6.2.1. Monitoramento 24/7 ativado.
- 5.5.6.2.2. Suporte técnico disponível conforme SLA.

5.5.7. Responsabilidades:

- 5.5.7.1. CONTRATADO: Ministrando treinamento, fornecer documentação.
- 5.5.7.2. CONTRATANTE: Garantir participação da equipe, confirmar início da operação.

5.5.8. Entregáveis:

- 5.5.8.1. Material de treinamento (slides, vídeos, manuais).
- 5.5.8.2. Guia de usuário da plataforma.
- 5.5.8.3. Emissão de certificado aos participantes do treinamento.
- 5.5.8.4. Relatório de transição (confirmação de início da operação).

ANEXO I-D

RELATÓRIOS FINAIS

1. FINALIDADE

Este anexo define os tipos e modelos de relatórios de serviços que deverão ser fornecidos pelo CONTRATADO de acordo com a periodicidade exigida no contrato relativa aos serviços de *Threat Intelligence* e prevenção a fraudes.

2. ESCOPO DOS RELATÓRIOS

- 2.1. O CONTRATADO deverá disponibilizar semanalmente, através de página na Internet ou correio eletrônico, ao longo da vigência do contrato, relatório semanal de alertas com informações sobre todas as ameaças detectadas na semana, com alertas acionáveis e atualizações sobre monitoramento de marca, executivos e campanhas maliciosas, toda segunda-feira até 12:00 (horário local do Contratante).
- 2.2. O CONTRATADO deverá disponibilizar mensalmente, através de página na Internet ou correio eletrônico, ao longo da vigência do contrato, relatório mensal de análise detalhada das tendências de ameaças, desempenho do serviço e recomendações estratégicas para o contratante, até o quinto dia útil do mês subsequente ao mês de referência do relatório.
- 2.3. O CONTRATADO deverá disponibilizar relatório pós ocorrência de incidente, através de página na Internet ou correio eletrônico, ao longo da vigência do contrato, relatório pós-incidente para detalhar a análise de um incidente específico, incluindo cronologia, impacto, mitigação e lições aprendidas, até 5 dias após a resolução do incidente.
- 2.4. Todos os relatórios devem conter, no mínimo, as seguintes informações: resumo de ameaças, IoCs compartilhados, métricas de desempenho, recomendações acionáveis.
- 2.5. Os relatórios devem conter, no mínimo, a ocorrência dos seguintes eventos:
 - 2.5.1. Sites utilizados para realizar, ou tentar realizar, golpes e fraudes que envolvam ou remetam de qualquer forma aos ativos de informação monitorados;
 - 2.5.2. Anomalias nos registros "WhoIS" dos domínios monitorados;
 - 2.5.3. Serviços que devem ser somente de consumo interno, sistemas e páginas internas (intranet) relacionados ao CONTRATANTE e que estejam expostas na internet, podendo ou não ser exploradas para eventuais ataques cibernéticos;
 - 2.5.4. Vulnerabilidades dos domínios monitorados que foram tornadas públicas, mesmo que essa exposição esteja disponível apenas na deep e dark web;
 - 2.5.5. Identificação de possíveis intenções de ataques a sistemas, serviços, ativos de informação e pessoas de interesse do BNB que serão fornecidas ao CONTRATADO na fase de Inserção do Contratado;
 - 2.5.6. Intenções de ataque que tenham como objetivo os ativos monitorados, por exemplo SFN, PIX, Open Banking, entre outros;

- 2.5.7. Campanhas relevantes de “hacktivismo”, como por exemplos ataques crescentes cujos alvos são em sua maioria órgãos públicos ou de governo, ou ainda campanhas de ataques em que a vulnerabilidade explorada possa estar presente nas tecnologias implantadas no BNB;
- 2.5.8. Comercialização online de informações sensíveis, informações pessoais, entre outras, das pessoas de interesse ou vinculadas ao BNB;
- 2.5.9. Atividades fraudulentas relacionadas aos ativos monitorados (utilização indevida de nome e marca, por exemplo);
- 2.5.10. Endereços de correio eletrônico (e-mails) de domínios monitorados em listas de spam;
- 2.5.11. Credenciais de acesso aos ativos e Nuvem privada do BNB que estejam, ou não, à venda na web aberta, dark web e deep web;
- 2.5.12. Credenciais de correio eletrônico dos domínios monitorados que estejam, ou não, à venda na web aberta, dark web e deep web;
- 2.5.13. Códigos maliciosos (malwares) direcionados para os ativos e sistemas de informação monitorados;
- 2.5.14. Intenções diretas de ataques aos ativos e sistemas de informação monitorados;
- 2.5.15. Discussões online maliciosas que divulguem ou acompanhem informações dos ativos de informação monitorados;
- 2.5.16. Perfis falsos que utilizem os nomes e/ou fotos das pessoas de interesse do BNB;
- 2.5.17. Documentos ou informações confidenciais, sensíveis ou sigilosas vazadas dos ativos de informação monitorados;
- 2.5.18. Aplicações (dispositivos móveis, softwares e aplicações web) falsas que utilizem o nome, a marca ou identidade visual dos ativos de informação monitorados;
- 2.5.19. Desfiguração de páginas (defacement) hospedadas nos domínios monitorados.

3. RELATÓRIO SEMANAL DE ALERTAS

- 3.1. Propósito: Fornecer uma visão rápida das ameaças detectadas na semana, com alertas acionáveis e atualizações sobre monitoramento de marca, executivos e campanhas maliciosas.
- 3.2. Formato: PDF, 5-10 páginas, com gráficos e tabelas para visualização rápida.
- 3.3. Prazo: Entregue toda segunda-feira até 12:00.
- 3.4. Estrutura e Conteúdo:
 - 1. Resumo Executivo
 - Período: 16/06/2025 a 22/06/2025
 - Visão Geral:
 - 12 alertas emitidos (8 de prioridade média, 3 de alta, 1 crítica).
 - 2 tentativas de phishing direcionadas a executivos detectadas e mitigadas.
 - 1 perfil falso da marca identificado no X e removido.
 - Principais Ações: Takedown de um domínio malicioso e bloqueio de 5 IPs associados a uma campanha de malware.
 - 2. Monitoramento de Marca e Executivos

- Menções à Marca:
 - 1.200 menções em redes sociais (90% neutras, 8% positivas, 2% negativas).
 - Destaque: Postagem negativa no X com 10 mil visualizações, sugerindo fraude associada à marca (investigação em andamento).
- Atividades de Executivos:
 - Tentativa de spear phishing contra o CFO via e-mail falso, bloqueada em 8 minutos.
 - Perfil falso no LinkedIn imitando o CEO, reportado e removido em 24 horas.
- Gráfico: Tendência de menções à marca (linha do tempo com picos de atividade).

3. Ameaças Detectadas

- Resumo de Alertas:

ID Alerta	Tipo	Prioridade	Descrição	Status
A-2025-001	Phishing	Alta	E-mail falso solicitando transferência financeira	Mitigado
A-2025-002	Malware	Crítica	Download de arquivo malicioso via site clonado	Takedown concluído

- Campanhas Maliciosas:
 - Campanha de phishing usando domínio semelhante (ex.: contratante-fake.com), interrompida via takedown.
 - Botnet detectado enviando spam com menções à marca, IPs bloqueados.

4. IoCs Compartilhados

- Indicadores Fornecidos:
 - 10 URLs maliciosas, 15 IPs, 3 hashes de malware.
 - Formato: STIX 2.1, integrado ao Splunk do contratante.
- Eficácia: 80% dos IoCs aplicados em bloqueios automáticos via SIEM.

5. Métricas de Desempenho

- Tempo de Resposta:
 - Alertas críticos: Média de 7 minutos (SLA: <10 minutos).
 - Alertas não críticos: Média de 45 minutos (SLA: <1 hora).
- Taxa de Falsos Positivos: 3% (SLA: <5%).
- Gráfico: Tempo de resposta por prioridade (barras).

6. Recomendações

- Revisar políticas de autenticação de e-mail (DMARC) para reduzir phishing.
- Treinar executivos sobre identificação de perfis falsos em redes sociais.
- Monitorar domínios recém-registrados semelhantes à marca.

7. Contato

- Ponto de contato do fornecedor: [Nome, e-mail, telefone].
- Próxima reunião de revisão: 23/06/2025, 10:00.

4. RELATÓRIO MENSAL DE INTELIGÊNCIA

4.1. Propósito: Fornecer uma análise detalhada das tendências de ameaças, desempenho do serviço e recomendações estratégicas para o contratante.

4.2. Formato: PDF, 15-20 páginas, com visualizações detalhadas (gráficos, mapas de calor, tabelas).

4.3. Prazo: Entregue até o 5º dia útil do mês subsequente.

4.4. Estrutura e Conteúdo:

1. Resumo Executivo

- Período: Junho de 2025
- Destaques:
 - 48 alertas emitidos (35 mitigados, 13 em monitoramento).
 - Aumento de 20% em tentativas de phishing comparado a maio.
 - Identificação de uma campanha de desinformação no X, neutralizada.
- Impacto Evitado: Estimativa de prevenção de perdas de [valor, ex.: \$50.000] devido a fraudes financeiras.

2. Tendências de Ameaças

- Setor do Contratante: Aumento de ataques BEC (Business Email Compromise) no setor financeiro.
- Ameaças Globais: Crescimento de ransomware-as-a-service na dark web.
- Gráfico: Mapa de calor de ameaças por região (ex.: 60% originadas da Europa Oriental).
- IA Insights: Modelos de IA identificaram 15% mais ameaças de baixa visibilidade (ex.: credenciais vazadas) comparado ao mês anterior.

3. Monitoramento de Marca e Executivos

- Menções à Marca:
 - 25.000 menções totais (5% negativas, associadas a uma campanha de desinformação).
 - Ação: Colaboração com plataforma X para remoção de 10 posts falsos.
- Dark Web:
 - 3 vazamentos de credenciais corporativas detectados em marketplaces ilícitos.
 - Ação: Notificação imediata e troca de senhas.
- Executivos:
 - 5 tentativas de spear phishing contra 3 executivos.
 - Ação: Bloqueio de e-mails e treinamento reforçado.
- Tabela: Resumo de menções por canal (X, LinkedIn, dark web, etc.).

4. Classificação e Priorização de Riscos

- Matriz de Riscos:

Ameaça	Probabilidade	Impacto	Prioridade	Mitigação
Phishing	Alta	Alto	Crítica	Bloqueio de domínios
Vazamento de Dados	Média	Alto	Alta	Monitoramento contínuo

- Framework: MITRE ATT&CK usado para mapear 80% das ameaças.
- Gráfico: Distribuição de riscos por prioridade (pizza).

5. Desempenho do Serviço

- Disponibilidade: 99,95% (SLA: 99,9%).
- Tempo de Resposta:
 - Crítico: Média de 6 minutos.
 - Não crítico: Média de 50 minutos.
- Integração SIEM/SOAR: 98% dos eventos enviados ao Splunk processados sem erros.
- Tabela: Conformidade com SLAs (métricas vs. metas).

6. IoCs e Integração

- IoCs Compartilhados: 150 URLs, 200 IPs, 50 hashes de malware.
- Eficácia: 90% dos IoCs aplicados em regras de firewall/SIEM.
- Integração: Playbook SOAR para phishing implementado, reduzindo tempo de resposta em 30%.

7. Recomendações Estratégicas

- Investir em autenticação multifator (MFA) para executivos.
- Monitorar grupos APT específicos (ex.: FIN7) com base em tendências do setor.
- Realizar simulações de phishing internas trimestralmente.
- Registrar domínios defensivos (ex.: contratante-seguro.com).

8. Anexos

- Lista completa de IoCs (JSON/STIX).
- Log de alertas detalhado (CSV).
- Capturas de tela de perfis falsos removidos.

5. RELATÓRIO PÓS-INCIDENTE

5.1. Propósito: Detalhar a análise de um incidente específico, incluindo cronologia, impacto, mitigação e lições aprendidas.

5.2. Formato: PDF, 5-8 páginas, com linha do tempo e diagramas.

5.3. Prazo: Entregue até 5 dias após a resolução do incidente.

5.4. Estrutura e Conteúdo:

1. Resumo do Incidente

- ID do Incidente: INC-2025-007
- Data/Hora: 20/06/2025, 14:30
- Tipo: Campanha de phishing direcionada ao departamento financeiro.
- Impacto: Nenhum dado comprometido; tentativa bloqueada antes de execução.
- Prioridade: Crítica

2. Cronologia

- 14:30: E-mail falso detectado pelo sistema de IA, imitando o CEO.

- 14:35: Alerta emitido à equipe de segurança (SLA: <10 minutos).
- 14:45: Análise confirmou domínio malicioso (contratante-falso.com).
- 15:00: Domínio reportado para takedown; IPs associados bloqueados via firewall.
- 16:30: Takedown concluído; campanha interrompida.
- Gráfico: Linha do tempo do incidente (barras).

3. Análise Técnica

- Vetor de Ataque: E-mail com link para site falso solicitando credenciais.
- IoCs:
 - URL: hxxp://contratante-falso.com/login
 - IP: 192.168.1.100
 - Hash: [SHA-256 do anexo malicioso]
- Tática (MITRE ATT&CK): T1566.001 (Phishing: Spearphishing Attachment).
- Ator de Ameaça: Possível associação com grupo FIN8 (baseado em padrões).

4. Impacto

- Operacional: Nenhum impacto; tentativa bloqueada antes de interação.
- Financeiro: Prevenção de potencial perda de [valor, ex.: \$20.000].
- Reputacional: Nenhum impacto público identificado.

5. Ações de Mitigação

- Bloqueio de 10 IPs e 3 URLs associados.
- Atualização de regras no SIEM para detectar domínios semelhantes.
- Notificação aos funcionários sobre a tentativa de phishing.
- Compartilhamento de IoCs com FS-ISAC.

6. Lições Aprendidas

- Necessidade de reforçar treinamento anti-phishing para o departamento financeiro.
- Domínios defensivos podem prevenir ataques semelhantes.
- Ajustar sensibilidade do modelo de IA para detectar e-mails com erros ortográficos sutis.

ANEXO I-E**DECLARAÇÃO DE NÃO OCORRÊNCIA DE REGISTRO DE OPORTUNIDADE**

Ao Banco do Nordeste S/A,

Ref. Edital de Pregão Eletrônico nº. ____/2025

Objeto: Contratação dos serviços de inteligência de ameaças cibernéticas (*cyber threat intelligence - CTI*) para prevenção de fraudes e incidentes cibernéticos.

Prezados Senhores,

O (LICITANTE), (qualificação), por meio de seu representante legal, **DECLARA**, que para a apresentação de proposta ao referido Edital, **NÃO** houve ocorrência de “**Registro de Oportunidade**”, de modo a garantir o princípio constitucional da isonomia e a seleção da proposta mais vantajosa para a Administração Pública, conforme disposto na Instrução Normativa Nº 1 de 4 de abril de 2019 e n art. 31 da Lei nº 13.303, de 2016.

Local: _____

Data: ____/____/____

Representante Legal:

(ASSINATURA) _____

RG: _____

CPF: _____