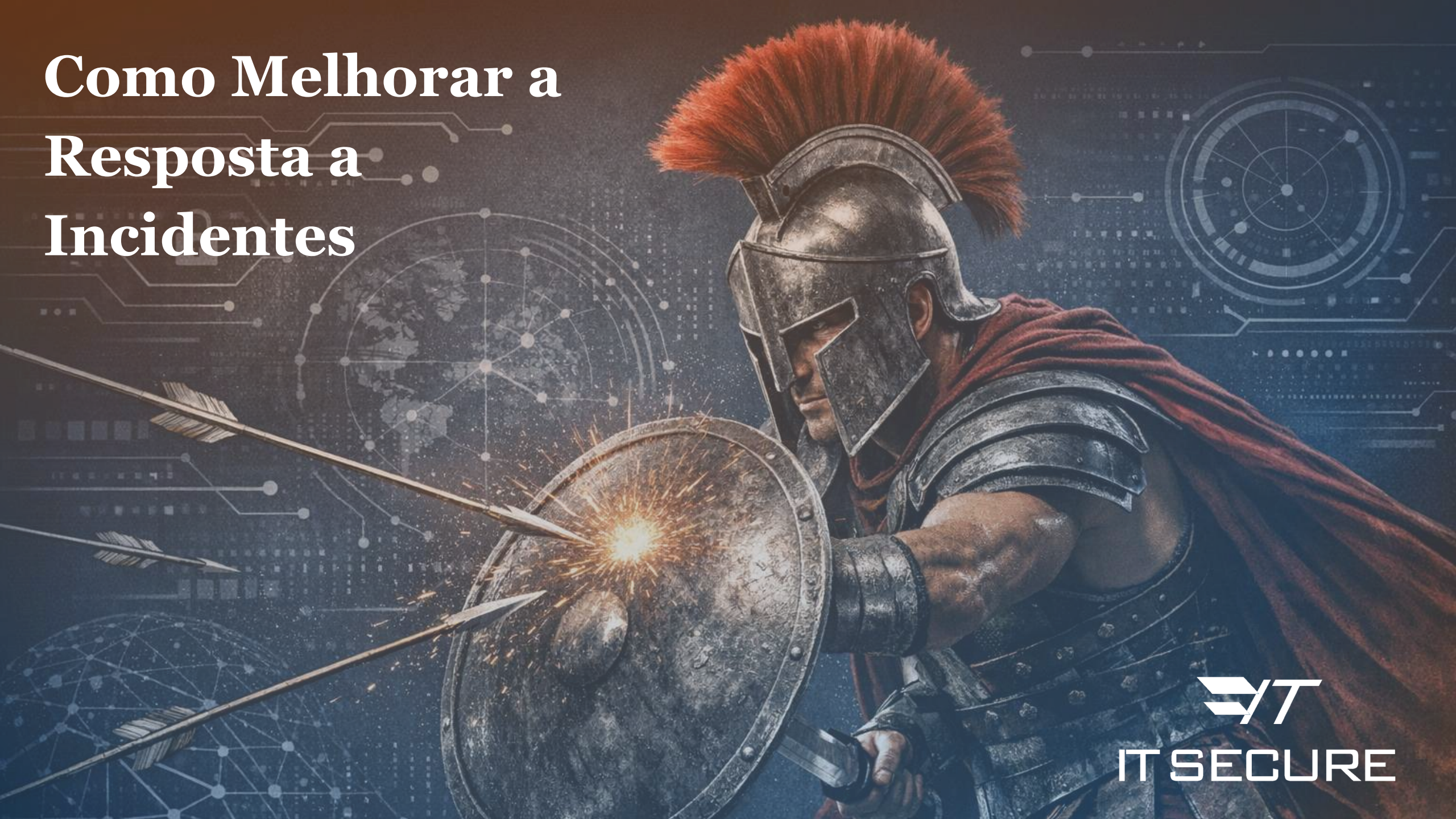
Como Melhorar a Resposta a Incidentes



IT SECURE

E-BOOK · IT SECURE CONSULTING · 2026

Como Melhorar a Resposta a Incidentes

Estrutura, Governança e Capacidade Operacional para a Alta Direção e o Conselho

Fundamentado em:

· NIST SP 800-61 Rev. 2 e 3

· ISO/IEC 27035-1 e 2

· CMU/CERT — Handbook for CSIRTs

· BACEN CMN 4.893 / 5.274 · LGPD / ANPD Res. 15/2024

· Decreto 9.637/2018 — PNSI · PL 2.338/2023 — IA

Carlos A. I. Bernardo | CISSP · MBA GRC · ISO 22301 LI

Rafael de Queiroz Batista | CDPSE · ISO 27701 LI · MSc FGV

IT SECURE

SUMÁRIO

O que você vai encontrar neste e-book

Incidente cibernético não é um problema de TI. É um evento de negócio.

O Board e a Alta Direção que não têm visibilidade sobre a capacidade de resposta a incidentes da organização estão tomando decisões estratégicas com um ponto cego relevante, um que reguladores, investidores e clientes já não toleram.

Impacto Financeiro

Custo médio global de violação de dados: USD 4,88 milhões (IBM Cost of a Data Breach Report 2024). Ransomware em infraestrutura crítica pode superar muito esse valor em perdas operacionais.

Responsabilidade Legal

LGPD, BACEN e regulações setoriais atribuem responsabilidade formal à Alta Direção pela adequação dos controles de segurança e pela resposta a incidentes.

Impacto Reputacional

Incidentes graves ocorridos com empresas listadas em Bolsa resultaram em queda média de 5% a 7% no valor de mercado nos dias subsequentes à divulgação pública.

Risco de Cadeia

Incidentes relevantes podem ter origem em terceiros fornecedores, prestadores de serviço, parceiros de nuvem. A responsabilidade não termina no perímetro da organização.

O Brasil tem obrigações legais de resposta a incidentes.

Não são recomendações.
São exigências com prazo,
responsável designado
e sanção prevista.

LGPD · Art. 48 + Res. ANPD 15/2024 — LGPD / ANPD

Notificação obrigatória à ANPD e aos titulares em até 3 dias úteis após confirmação do incidente com risco ou dano relevante. Criação, manutenção e disponibilidade de registros relacionados aos incidentes

BACEN CMN 4.893/2021 + CMN 5.274/2025 — BACEN

Designação formal de diretor responsável pela política de segurança cibernética. Aprovação, pela alta administração, do PARI. Implementação integrada de monitoramento, resposta a incidentes e gestão de credenciais e acessos. Capacidade operacional efetiva e comprovável.

Decreto 9.637/2018 — PNSI — PNSI

Estabelece a governança da segurança da informação na administração pública federal, com foco em gestão de riscos e tratamento de incidentes, e atribui ao GSI/PR a definição de diretrizes, critérios de monitoramento e requisitos mínimos de segurança a serem observados pelos órgãos públicos.

PL 2.338/2023 — Regulação de IA — PL IA

Aprovado no Senado e em tramitação na Câmara dos Deputados, impõe obrigações de transparência, avaliação de impacto e resposta a incidentes para sistemas de IA de alto risco, com responsabilização de operadores e desenvolvedores.

PL 4.752/2025 — Lei de Cibersegurança — PL Ciber

Em tramitação, institui o Marco Legal da Cibersegurança, cria a Autoridade Nacional de Cibersegurança e estabelece requisitos de prevenção e capacidade de resposta a incidentes para infraestruturas críticas, serviços essenciais e fornecedores do poder público.

Precisão de linguagem cria clareza de ação.

Organizações que confundem eventos com incidentes desperdiçam recursos respondendo ao que não exige resposta formal e frequentemente subnotificam o que exige.

Evento de Segurança

Qualquer ocorrência identificada em um sistema, serviço ou rede que indique uma possível violação da política de segurança ou falha de controle.

ISO/IEC 27035-1:2023

Capacidade de Resposta

Conjunto de pessoas, processos, tecnologias e estruturas organizacionais que permitem à organização detectar, analisar, conter, erradicar e recuperar-se de incidentes de forma estruturada e oportuna.

NIST SP 800-61r3 / CMU CSIRT Guide

Incidente de Segurança

Evento ou série de eventos de segurança indesejados ou inesperados com probabilidade significativa de comprometer operações de negócio e ameaçar a segurança da informação.

ISO/IEC 27035-1:2023

CSIRT / CIRT / IRT

Equipe de Resposta a Incidentes de Segurança: grupo com missão definida, habilidades técnicas e autoridade formal para coordenar a resposta a incidentes.

CMU/CERT Handbook

Três pilares técnicos que fundamentam uma resposta a incidentes madura.

NIST SP 800-61

Rev. 2 (2012) + Rev. 3 (2025)

1. Rev. 2: O ciclo clássico de 4 fases: Preparação, Detecção e Análise, Contenção/Erradicação/Recuperação e Atividade Pós-Incidente
2. Rev. 3 (2025): Integração com NIST CSF 2.0 — as 6 funções Govern, Identify, Protect, Detect, Respond e Recover como espinha dorsal
3. Ciclo de vida contínuo: IR não é evento pontual, é programa permanente de melhoria
4. Métricas: MTTD (Mean Time to Detect) e MTTR (Mean Time to Respond) como KPIs centrais

ISO/IEC 27035

Parts 1 e 2 (2023)

1. 5 fases: Plan & Prepare, Detection & Reporting, Assessment & Decision, Responses, Lessons Learned
2. Requisito de comprometimento da alta administração na política de gestão de incidentes (27035-2)
3. IRT (Incident Response Team): membros de confiança com habilidades técnicas e autoridade formal
4. Integração nativa com ISO 27001:2022, Controle A.5.24: Planejamento e preparação para gestão de incidentes

CMU/CERT Handbook for CSIRTs

Carnegie Mellon University

1. Base dos cursos 'Managing CSIRT' e 'Creating a CSIRT' do CERT.br/CMU
2. O SIM3 é amplamente aceito pela comunidade internacional de CSIRTs e é compatível com as práticas de incident response do CMU/CERT.
3. Taxonomia de serviços do CSIRT: reativos, pró-ativos e de gestão de qualidade da segurança
4. Framework para definição de missão, constituency, autoridade e modelo organizacional do CSIRT

A evolução de um ciclo rígido para uma abordagem integrada ao negócio.

NIST SP 800-61 Rev. 2 — 2012

1 **Preparação**

Políticas, equipes, ferramentas, planos e exercícios. Fundação antes do incidente.

2 **Detecção e Análise**

Identificação, triagem, priorização e documentação do incidente.

3 **Contenção · Erradicação · Recuperação**

Isolamento, eliminação da causa raiz e restauração dos sistemas afetados.

4 **Atividade Pós-Incidente**

Lições aprendidas, relatório final e melhoria dos processos e controles.

NIST SP 800-61 Rev. 3 — Abril 2025

GV **Govern**

Políticas, papéis, responsabilidades e métricas de IR integradas à governança corporativa.

ID **Identify**

Inventário de ativos, avaliação de riscos e inteligência de ameaças como insumos contínuos.

PR **Protect**

Controles preventivos que reduzem probabilidade e impacto — integrados ao plano de IR.

DE **Detect**

Capacidade de detecção e alerta — SIEM, EDR, threat hunting e análise de anomalias.

RS **Respond**

Contenção, erradicação, comunicação e coordenação multi-stakeholder durante o incidente.

RC **Recover + Improve**

Restauração, lições aprendidas e melhoria contínua integrada ao ciclo — não post-facto.

Do planejamento às lições aprendidas — uma abordagem integrada à gestão de riscos.

1 Plan & Prepare

- Política de gestão de incidentes aprovada pela Alta Direção
- Plano de resposta documentado e comunicado
- Equipe de resposta (IRT) estabelecida e treinada
- Relacionamentos com stakeholders internos e externos definidos
- Exercícios e simulações periódicos realizados

2 Detection & Reporting

- Monitoramento contínuo de eventos de segurança
- Mecanismos de reporte acessíveis a toda a organização
- Triagem e classificação inicial de eventos
- Escalada para equipe de resposta conforme criticidade
- Notificação a partes interessadas conforme plano

3 Assessment & Decision

- Avaliação técnica e de impacto ao negócio
- Classificação do incidente por tipo e severidade
- Decisão sobre estratégia de resposta
- Ativação de planos de continuidade quando necessário
- Comunicação estruturada interna e externa

4 Responses

- Contenção para limitar propagação e danos
- Erradicação da causa raiz confirmada
- Recuperação controlada e monitorada
- Preservação de evidências forenses
- Registro detalhado de todas as ações tomadas

5 Lessons Learned

- Análise de causa raiz estruturada (RCA)
- Relatório pós-incidente com cronologia completa
- Identificação de lacunas em controles e processos
- Atualização de políticas, planos e playbooks
- Comunicação de melhorias para a Alta Direção

Missão, modelos e serviços de um CSIRT efetivo.

Modelos organizacionais

Centralizado

Uma equipe serve toda a organização. Eficiente em custo, ideal para organizações de médio porte. Exige visibilidade transversal.

Distribuído

Equipes por divisão ou unidade de negócio com coordenação central. Adequado para grandes grupos com operações diversas.

Coordenado

Equipe central coordena sem responsabilidade operacional direta. Comum em grupos com subsidiárias autônomas.

Virtual / Ad Hoc

Membros convocados conforme a necessidade. Adequado para organizações menores. Exige treinamento e documentação robustos.

Categorias de serviço (CMU/CERT)

Reativos	· Triagem de alertas e eventos · Análise e resposta a incidentes · Suporte à resposta — forense e contenção · Coordenação da resposta entre equipes · Gestão de vulnerabilidades reportadas
Pró-Ativos	· Inteligência de ameaças (CTI) · Monitoramento contínuo e threat hunting · Anúncios de segurança e alertas · Auditoria e avaliação de sistemas · Desenvolvimento de ferramentas de segurança
Gestão de Qualidade	· Análise de riscos e risco residual · Continuidade de negócios e recuperação · Conscientização e treinamento em SI · Consultoria estratégica interna · Avaliação da maturidade do CSIRT (SIM3)

Antes de existir uma equipe, é preciso existir uma estrutura.

Baseado no Handbook for CSIRTs (CMU/CERT) e nos cursos 'Creating a CSIRT' e 'Managing CSIRT' do CERT.br

Missão e Escopo Definidos

Declaração formal do propósito do CSIRT, a constituency que serve, os tipos de incidentes cobertos e os serviços prestados. Sem missão clara, o CSIRT atende tudo — e não atende nada bem.

Autoridade e Mandato

O CSIRT precisa de autoridade formal para agir: isolar sistemas, convocar equipes, comunicar externamente. Sem mandato explícito aprovado pela Alta Direção, a equipe está de mãos atadas no momento crítico.

Políticas e Playbooks

Procedimentos documentados para os incidentes mais prováveis — ransomware, vazamento de dados, comprometimento de credenciais, DDoS. Playbooks eliminam a improvisação sob pressão.

Relacionamentos e Escalada

Mapeamento de quem acionar: jurídico, comunicação, executivos, ANPD, BACEN, polícia especializada, CERT.br, seguradoras, fornecedores críticos. Contatos estabelecidos antes do incidente, não durante.

Ferramentas e Infraestrutura

Canal de comunicação seguro e independente, sistema de rastreamento de incidentes, capacidade forense básica e acesso a inteligência de ameaças (CTI). A infraestrutura do CSIRT não pode depender dos sistemas comprometidos.

Métricas e Melhoria

MTTD, MTTR, taxa de contenção, custo por incidente e aderência ao plano. O que não é medido não melhora — e o que não melhora repete o mesmo incidente com o mesmo impacto.

Governança de incidentes não é delegação. É responsabilidade.

Conselho de Administração

- Aprovar a política de segurança cibernética e o PARI (exigência BACEN CMN 4.893, art. 9º)
- Receber relatório anual de cibersegurança até 31 de março de cada ano (BACEN, art. 8º)
- Garantir que os riscos cibernéticos estejam incorporados ao framework de gestão de riscos corporativos
- Deliberar sobre investimentos materiais em segurança
- Exigir métricas de maturidade da capacidade de resposta em reuniões periódicas

CEO e Alta Direção

- Designar formalmente o Diretor responsável pela cibersegurança (BACEN CMN 4.893, art. 7º)
- Garantir recursos adequados — orçamento, pessoal e autoridade — para o CSIRT
- Aprovar a estratégia de comunicação de crise e os limites de decisão durante incidentes
- Participar de exercícios tabletop de nível executivo pelo menos anualmente
- Assegurar integração entre resposta a incidentes, continuidade de negócios e gestão de crises

CIO / CISO

- Estruturar, capacitar e manter operacional o CSIRT ou a capacidade de resposta equivalente
- Produzir relatórios executivos de incidentes em linguagem de impacto de negócio
- Coordenar, com o jurídico e o DPO, as comunicações com os orgãos reguladores, com o BACEN e a ANPD nos prazos adequados
- Conduzir exercícios de simulação e atualizar playbooks com base em lições aprendidas
- Reportar métricas de maturidade (MTTD, MTTR e custo por incidente) à liderança

Silêncio custa mais caro do que transparência estruturada.

Comunicação Interna

Cadeia de escalada

Definir previamente quem aciona quem e quando. Sem cadeia clara, o incidente escala pelo pânico, não pela lógica.

Canal de comunicação seguro

E-mail e chat corporativos podem estar comprometidos no incidente. O plano precisa de um canal alternativo pré-estabelecido.

Declarações internas padronizadas

Colaboradores recebem informação oficial ou buscam fontes informais. Comunicados internos rápidos e objetivos evitam o segundo problema.

Registro contínuo de ações

Tudo documentado com timestamp para relatório final, para o jurídico, para os orgãos reguladores como a ANPD e para as lições aprendidas.

Comunicação Externa e Regulatória

ANPD — Res. 15/2024

Notificação em até 3 dias úteis após confirmação do incidente com risco ou dano relevante aos titulares. Registro obrigatório por 5 anos.

BACEN — CMN 4.893/5.274

Reporte ao regulador conforme plano de ação e resposta a incidentes aprovado pelo Conselho. Prazo e formato definidos na política interna.

Clientes e parceiros afetados

Comunicação direta, objetiva e com orientações práticas. O silêncio implica ocultação; a comunicação inadequada amplifica o dano reputacional.

Imprensa e público

Declaração preparada antes, não improvisada durante. O time de comunicação corporativa atua com o roteiro aprovado pela liderança.

O que o Board deve perguntar ao CISO nas reuniões de governança.

MTTD

Mean Time to Detect

Tempo médio entre a ocorrência do incidente e sua detecção. Benchmark: < 24h para incidentes críticos. IBM 2024: média global de 194 dias.

MTTR

Mean Time to Respond

Tempo médio entre a detecção e a contenção/resolução. Benchmark: < 4h para contenção inicial. ISO 27035 e NIST SP 800-61.

NR%

Notificação Regulatória

Conformidade com o prazo de notificação à ANPD (3 dias úteis — Res. 15/2024) e ao BACEN conforme PARI aprovado pelo Conselho.

Perguntas que o Conselho deve fazer periodicamente

1. Qual foi o último incidente de segurança relevante? Qual foi o impacto e o que foi feito para evitar recorrência?
2. O plano de resposta a incidentes foi testado nos últimos 12 meses? Com que resultado?
3. Temos capacidade de notificar a ANPD no prazo de 3 dias úteis se houver um vazamento de dados hoje?
4. Qual é o MTTD atual e como ele se compara ao benchmark do setor?
5. Os fornecedores críticos têm capacidade de resposta a incidentes compatível com os nossos requisitos?

IA amplifica ameaças e cria novas obrigações de governança.

IA como vetor de ataque

Deepfakes e clonagem de voz

Usados para manipular processos de autenticação, autorizar transações e impersonar executivos em golpes de engenharia social, cada vez mais comuns e convincentes.

Phishing hiperpersonalizado

Modelos de linguagem (LLMs) geram mensagens de phishing com qualidade e personalização que tornam obsoletas as defesas baseadas em identificação de erros gramaticais.

Automação de ataques em escala

IA reduz o custo e o tempo de ataques de força bruta, enumeração de vulnerabilidades e Account Takeover, ampliando a superfície e a velocidade dos incidentes.

IA como objeto de governança

PL 2.338/2023 — Lei de IA

Em tramitação. Sistemas de IA de alto risco terão obrigações de gestão de incidentes, avaliação de impacto e notificação de falhas, semelhante ao que a LGPD fez com dados pessoais.

ISO/IEC 42001 — SGIA

Sistema de Gestão de IA (framework para governança de sistemas de IA), incluindo gestão de riscos específicos de IA e integração com SGSI (ISO 27001) e gestão de privacidade (ISO 27701).

NIST AI RMF

Framework de gestão de riscos de IA do NIST : mapa, medição, gerenciamento e governança de riscos em sistemas de IA, com seção específica sobre resposta a incidentes envolvendo IA.

Implicações para o CSIRT

Playbooks específicos para IA

Incidentes envolvendo sistemas de IA têm características distintas: alucinações com impacto operacional, viés em decisões automatizadas, vazamento via prompts. Playbooks tradicionais não cobrem esses cenários.

Detecção de deepfakes no processo

O CSIRT precisa de capacidade para identificar e responder a ataques que usam deepfakes como vetor de entrada , especialmente em processos de autenticação e autorização.

Governança integrada SI + IA

Organizações que adotam IA precisam integrar os riscos de IA ao seu framework de gestão de incidentes, o mesmo ativo pode ser vetor de ataque e objeto de incidente simultaneamente.

ROTEIRO DE AÇÃO — POR ONDE COMEÇAR

Da avaliação à capacidade operacional — um caminho estruturado e proporcional.

1 Curto Prazo — 0 a 90 dias

- Diagnosticar a capacidade atual de resposta frente à ISO 27035 e NIST SP 800-61
- Verificar conformidade com BACEN CMN 5.274 e ANPD Res. 15/2024
- Designar formalmente o responsável pela política de cibersegurança
- Inventariar os incidentes dos últimos 24 meses e avaliar a qualidade das respostas
- Garantir que o plano de resposta está documentado — mesmo que básico

2 Médio Prazo — 90 a 180 dias

- Estruturar ou formalizar a equipe de resposta (CSIRT / IRT) com missão e autoridade definidas
- Desenvolver playbooks para os 5 cenários de maior probabilidade/impacto
- Estabelecer o canal de comunicação seguro e independente para uso em incidentes
- Realizar o primeiro exercício tabletop com participação de executivos e jurídico
- Apresentar métricas iniciais de maturidade ao Conselho

3 Longo Prazo — 180 a 365 dias

- Integrar resposta a incidentes ao framework de gestão de riscos corporativos
- Buscar alinhamento com ISO 27001 (controle A.5.24) e iniciar processo de certificação
- Estruturar inteligência de ameaças (CTI) integrada ao CSIRT
- Incluir IA no escopo de governança de incidentes (ISO 42001 / NIST AI RMF)
- Avaliar maturidade do CSIRT com o modelo SIM3 (CMU/CERT / FIRST)

A capacidade de resposta a incidentes que sua organização precisa começa com um diagnóstico honesto.

Como a IT SECURE pode ajudar

- Diagnóstico da capacidade de resposta frente à ISO 27035, NIST SP 800-61 e regulações do BACEN e ANPD
- Estruturação do CSIRT — missão, modelos organizacionais, playbooks e infraestrutura
- Elaboração do Plano de Ação e Resposta a Incidentes (PARI) conforme CMN 4.893/5.274
- Treinamentos in-company para equipes técnicas, jurídico e alta liderança
- Exercícios tabletop de simulação de incidentes para diferentes públicos
- Integração da resposta a incidentes com ISO 27001, ISO 27701 e ISO 42001

Carlos A. I. Bernardo · CISSP · MBA GRC · ISO 22301 LI
Formação: Managing CSIRT · Creating a CSIRT
(CERT.br / Carnegie Mellon University)

Rafael de Queiroz Batista · CDPSE · ISO 27701 LI · MSc

contato@itsecure.com.br

+55 (11) 94794-8808

itsecure.com.br

A conversa inicial é sem custo
e sem compromisso.