

Resposta a incidentes em ambiente regulado

Contenção coordenada, cadeia de custódia e comunicação dentro do prazo regulatório

Matriz de contenção por classe de ativo, protocolo de coleta e custódia de evidência, mapa de prazos de notificação por jurisdição e modelo de comunicação executiva.

Documento técnico xFabric · revisão 2026.2 · uso corporativo

Contexto e fundamentação

Em ambiente regulado, a qualidade da resposta é medida pela evidência preservada e pela comunicação no prazo, não apenas pelo tempo de contenção.

Contenção sem destruição de evidência

A primeira decisão de um incidente é o conflito entre contenção imediata e preservação de estado. Desligar uma instância elimina memória volátil; isolá-la em rede preserva a evidência e interrompe a movimentação lateral.

O playbook precisa declarar previamente, por classe de ativo, qual ação de contenção é autorizada, quem pode executá-la e qual evidência deve ser coletada antes da execução.

- Captura de memória e de disco antes de qualquer alteração de estado
- Isolamento em rede preferido a desligamento em ativo com dado regulado
- Revogação de sessão e rotação de credencial registradas com carimbo confiável
- Snapshot de configuração de nuvem no momento da detecção

Cadeia de custódia operacional

Toda evidência coletada recebe identificador, hash, responsável pela coleta e registro de cada transferência. O armazenamento é imutável e segregado do ambiente comprometido.

Sem cadeia de custódia, a investigação continua tecnicamente válida, mas perde valor jurídico e regulatório exatamente no momento em que ele é exigido.

Prazos de notificação e responsabilidade nomeada

Ambientes regulados operam com relógios simultâneos: autoridade de proteção de dados, regulador setorial, seguradora, cliente contratual e, quando aplicável, mercado. Cada relógio começa em um evento distinto, quase sempre antes da conclusão da análise.

O playbook define, por jurisdição, quem redige, quem aprova e qual conteúdo mínimo é enviado em cada janela, com versão preliminar preparada antes do incidente.

Encerramento e lição estrutural

O encerramento exige três artefatos: causa raiz com evidência, controle corretivo com dono e prazo, e detecção nova ou ajustada que reduza o tempo de identificação de uma recorrência.

Um incidente encerrado sem alteração no backlog de engenharia de detecção não produziu aprendizado verificável.

Matriz de contenção por classe de ativo

Classe de ativo	Ação autorizada	Coleta prévia obrigatória
Endpoint corporativo	Isolamento em rede	Memória volátil e artefatos de processo

Servidor com dado regulado	Isolamento, sem desligamento	Memória, disco e snapshot de configuração
Workload em nuvem	Revogação de credencial e isolamento de sub-rede	Snapshot de volume e trilha de API
Identidade	Revogação de sessão e rotação de segredo	Registro de autenticação e de consentimento
Fronteira de rede	Bloqueio de rota ou destino	Captura de tráfego e registro de fluxo

Protocolo de custódia da evidência

- Identificador único, hash e responsável pela coleta registrados no ato
- Armazenamento imutável, segregado do ambiente comprometido
- Cada transferência registrada com origem, destino, hora e autorizador
- Cópia de trabalho utilizada na análise; original preservado intacto
- Retenção conforme jurisdição e requisito contratual, com expurgo documentado

Mapa de prazos e responsabilidades

Os relógios regulatórios correm em paralelo e começam em eventos distintos. O playbook fixa previamente redator, aprovador e conteúdo mínimo de cada comunicação, com minuta preparada fora do incidente.

Destinatário	Gatilho	Responsável pela emissão
Autoridade de proteção de dados	Indício de acesso a dado pessoal	Encarregado, com aprovação jurídica
Regulador setorial	Impacto em serviço regulado	Compliance, com aprovação executiva
Cliente contratual	Cláusula de notificação acionada	Gerente de contrato, com validação técnica
Seguradora	Abertura de sinistro	Financeiro, com dossiê técnico anexo
Público interno	Necessidade de ação do usuário	Comunicação, com texto aprovado pelo IR

Critérios de encerramento

- Causa raiz documentada com evidência referenciada por identificador
- Controle corretivo implantado, com dono nomeado e prazo cumprido

- Detecção nova ou ajustada em produção, com teste registrado
- Comunicação final emitida a cada destinatário aplicável
- Revisão pós-incidente concluída com itens de backlog priorizados

Pontos de decisão

- Coleta antes de contenção, exceto quando o risco de propagação for maior que o valor da evidência.
- Cadeia de custódia é requisito de engenharia, não formalidade jurídica.
- Encerramento sem detecção nova ou ajustada indica ciclo incompleto.