Lefosse

ATAQUE CIBERNÉTICO

As primeiras 24 horas

Como agir, preservar evidências e reduzir exposição legal: um roteiro de decisão para a alta direção, do minuto zero ao fim do primeiro dia.

Por que este material existe

Ataques cibernéticos deixaram de ser um problema de tecnologia para se tornar um evento de risco corporativo. A experiência sugere que uma atuação precisa nas primeiras horas após o ataque é essencial para preservar as atividades da empresa e evitar (ou minimizar), entre outras, exposição jurídica e reputacional. Este roteiro foi preparado pelo **Lefosse** e reúne as boas práticas reconhecidas nacional e internacionalmente para as 24 horas seguintes ao conhecimento do incidente, organizadas por janela de tempo.

Como o Lefosse apoia

Resposta integrada

Equipes coesas e com conhecimento multidisciplinar atuando no mesmo ambiente, desde a primeira hora, para apoiar o processo de tomada de decisão.

Prova e responsabilização

Coordenação das atividades de preservação de elementos de prova (forensics digital, cadeia de custódia, etc.) e adoção de medidas de urgência (requerimento cautelares, interlocução com as autoridades criminais, etc.).

Assessoria jurídica integral

Avaliação dos riscos e assessoria jurídica integral perante reguladores (Banco Central, CVM, ANPD, etc.) e gestão do contencioso decorrente em todas as áreas do direito.

Quanto mais cedo a coordenação jurídica é formalizada, maior o conjunto de evidências preservado e menor é o grau de exposição da empresa e de seus administradores.

O roteiro em quatro janelas de tempo

0 - 1h
Ativar e conter

Comitê de crise, isolamento sem desligamento, corte do acesso do atacante e acionamento de advogado.

1 - 6h
Preservar e documentar

Coleta forense, congelamento de logs, ata notarial e cadeia de custódia.

6 - 12h
Dimensionar e decidir

Escopo, exfiltração e credenciais; possíveis gatilhos regulatórios e tomada preliminar de decisão.

12 - 24h
Comunicar e formalizar

Assessment preliminar; notificações às autoridades; medidas jurídicas de urgência.

A gestão de crises decorrentes de ataques cibernéticos exige monitoramento contínuo e adaptação às circunstâncias do caso. As medidas sugeridas nesta cartilha servem como referência e podem demandar ajustes conforme o cenário. Em qualquer hipótese, o suporte de assessoria técnica e jurídica especializada é essencial.

Linha do tempo da resposta

0 - 1h — Ativar e conter

Sem destruir evidência. As decisões da primeira hora definem o que ainda poderá ser provado depois.

FRENTE TÉCNICA | TI E FORENSE DIGITAL

_ **Acione o plano de resposta a incidentes** e o comitê de crise, com um coordenador único e papéis definidos; passe a registrar por escrito todas as ocorrências e decisões.

_ **Isole, não desligue.** Segregue o ativo da rede (cabo/VLAN/EDR). Desligar ou reiniciar apaga memória volátil, processos, conexões e chaves de criptografia que só existem em execução.

_ **Corte o acesso do atacante:** derrube VPN e sessões remotas, suspenda contas privilegiadas e acessos de terceiros e fornecedores, bem como revogue tokens e sessões ativas, incluindo refresh tokens, cookies de SSO e chaves de aplicação. Trocar a senha não encerra a sessão em curso.

_ **Abra canal de comunicação alternativo** (out-of-band). Presuma que o e-mail e a mensageria corporativos estão comprometidos e sendo lidos.

_ **Inicie o registro cronológico do incidente**: data, hora, quem fez, o que fez, em qual ativo.

FRENTE JURÍDICA

_ **Acione o advogado na primeira hora.** Conduzir a apuração sob coordenação jurídica organiza o risco e ampara a confidencialidade do trabalho (sigilo profissional — art. 7º, II e XIX, do Estatuto da OAB).

_ **Contrate a perícia forense com auxílio do advogado**, com escopo, hipóteses e forma de reporte definidos por escrito.

_ Avalie comunicar a seguradora. Apólices exigem comunicação tempestiva e pré-aprovação de fornecedores; o atraso é causa recorrente de negativa de cobertura.

_ **Preserve o contexto contratual:** contratos com fornecedores de TI e nuvem, SLAs, cláusulas de notificação e de responsabilidade — o vetor pode estar na cadeia de terceiros.

_ **Não comunique nada externamente ainda.** Toda declaração precoce vira prova em processo administrativo, cível e penal.

1 - 6h Preservar e documentar

Janela de evidências. Log rotacionado, disco reinstalado e backup restaurado por cima são perdas irreversíveis.

FRENTE TÉCNICA | TI E FORENSE DIGITAL

_ **Colete na ordem de volatilidade** (RFC 3227 e ISO/IEC 27037): memória RAM, conexões e processos ativos, cache e, só então, disco, backups e nuvem.

_ **Imagem forense bit a bit** dos ativos afetados, com hash (SHA-256) do original e da cópia. Trabalhe sempre sobre a cópia, nunca sobre o original.

_ **Congele o expurgo e a rotação de logs** (legal hold técnico): firewall, EDR/antivírus, proxy, VPN, Active Directory, servidores, aplicações, backup e trilhas de auditoria de e-mail em nuvem — que costumam ter retenção curta (7 a 180 dias).

_ **Preserve a trilha financeira:** registros de acesso ao internet banking, ordens de pagamento, alçadas e aprovações, dispositivos, IPs e horários. Comunique os bancos, observe movimentações atípicas e considere reduzir temporariamente o limite de transações.

_ **Guarde os artefatos do ataque:** nota de resgate, e-mails de phishing com cabeçalhos completos, contas e carteiras de criptoativos informadas, domínios, IPs, hashes de arquivos e demais indicadores de comprometimento (IoCs).

_ **Verifique os backups antes de tocar neles:** integridade, isolamento e ausência de comprometimento. Não restaure sobre o ambiente contaminado.

FRENTE JURÍDICA

_ **Ata notarial (art. 384 do CPC)** das telas, da nota de resgate, do site de vazamento e das mensagens do atacante — prova pré-constituída, com fé pública e data certa.

_ **Requeira a guarda de registros a provedores e plataformas** (Marco Civil da Internet — arts. 13, 15, 22 e 23): logs de conexão (1 ano) e de acesso a aplicações (6 meses) podem ser preservados por prazo maior mediante requerimento, e serão fornecidos por ordem judicial.

_ **Mapeie o escopo de dados pessoais:** categorias, volume, titulares, dados sensíveis e dados de clientes sob dever contratual.

_ **Enquadramento preliminar** — invasão de dispositivo (art. 154-A do CP), furto por fraude eletrônica (art. 155, §4º-B), estelionato eletrônico (art. 171, §2º-A), extorsão (art. 158) e organização criminosa. O enquadramento define a autoridade competente e as medidas cabíveis.

_ **Orientação sobre a cadeia de custódia** (arts. 158-A a 158-F do CPP): coleta documentada, lacre lógico e rastreabilidade sustentam a prova em juízo e evitam a nulidade do que foi apurado.

6 - 12h Dimensionar e decidir

O que foi acessado, o que saiu e os deveres legais. O jurídico transforma achado técnico em ponto para decisão.

FRENTE TÉCNICA | TI E FORENSE DIGITAL

_ **Determine vetor inicial, escopo e persistência:** o que foi apenas criptografado e o que foi efetivamente acessado ou exfiltrado; movimentação lateral e contas comprometidas.

_ **Investigue a exfiltração:** volumes anômalos de saída, ferramentas de transferência, áreas de staging e uploads para serviços externos.

_ **Rotacione credenciais e segredos:** senhas, tokens, certificados, chaves de API e contas de serviço. Reforce MFA e revise acessos de terceiros.

_ **Defina o plano de recuperação** por criticidade de negócio, em ambiente limpo e segmentado, com critérios de retorno validados.

FRENTE JURÍDICA

_ **Proteção de dados:** avalie risco relevante a direitos dos titulares. LGPD, art. 48 e Resolução CD/ANPD nº 15/2024 — comunicação à ANPD e aos titulares em até **3 dias úteis** do conhecimento, com conteúdo mínimo obrigatório.

_ **Regulatório bancário:** instituições autorizadas pelo BCB devem observar a Resolução CMN nº 4.893/2021 e a Resolução BCB nº 85/2021 — comunicação de incidentes relevantes, acionamento do plano de continuidade e reporte quanto a fornecedores de nuvem.

_ **Mercado de capitais:** avaliar fato relevante (Resolução CVM nº 44/2021), reporte ao comitê de auditoria e impacto em divulgações periódicas.

_ **Pagamento de resgate:** não há vedação expressa no Brasil, mas há risco de lavagem (Lei nº 9.613/1998), de violação a sanções internacionais e de financiamento a organização criminosa — sem garantia de restituição ou de não publicação. A decisão cabe ao órgão de administração, fundamentada e registrada em ata (arts. 153 e 155 da Lei nº 6.404/1976).

_ **Prepare a comunicação** a clientes, parceiros, colaboradores e imprensa alinhada ao que será dito às autoridades: versões divergentes são exploradas em fiscalização e em juízo.

12 - 24h Comunicar e formalizar

Notificar autoridades, registrar o crime e agir para tentar rastrear ativos e identificar o responsável.

FRENTE TÉCNICA | TI E FORENSE DIGITAL

_ **Relatório técnico preliminar** com linha do tempo, escopo, IoCs, medidas adotadas, anexos e hashes — base das comunicações regulatórias.

_ **Compartilhe indicadores** com o CERT.br e o CSIRT setorial, provedores e parceiros; bloqueie domínios, IPs e contas maliciosas.

_ **Monitore fóruns, mercados ilícitos e sites de vazamento**, além do uso indevido de credenciais, marca e domínios semelhantes.

_ **Rastreie os ativos:** em desvio financeiro, siga a cadeia de contas beneficiárias; em criptoativos, preserve os endereços e acione rastreamento em blockchain e exchanges.

FRENTE JURÍDICA

_ **Registro de ocorrência e notícia-crime** na delegacia especializada em crimes cibernéticos ou na Polícia Federal — e, quando cabível, avaliar oferta de comunicação ao Ministério Público, com requerimento de diligências de preservação e de quebra de sigilo telemático. Em paralelo, considerar o início de investigação interna para apurar as circunstâncias do ataque e eventual envolvimento de terceiros.

_ **Apure a necessidade de comunicar** o incidente, com registro da tempestividade: (i) ANPD e titulares, no prazo regulamentar; Banco Central e demais reguladores setoriais, conforme a atividade (BCB, CVM, SUSEP, ANS); contrapartes com dever contratual de notificação (operadores, controladores e clientes).

_ **Recuperação patrimonial de urgência:** notificação às instituições financeiras, acionamento do MED no Pix, bloqueio cautelar e tutela de urgência (arts. 300 e 301 do CPC), com pedido de quebra de sigilo bancário para identificar os destinatários.

_ **Documente a diligência da empresa:** atas do comitê de crise, decisões e respectivos fundamentos e evidências das medidas técnicas — o principal ativo de defesa perante autoridades.

Recomendações finais

Depois das 24 horas

_ Recuperar em ambiente "limpo", com critérios de retorno validados pelo TI.

_ Acompanhar os procedimentos judiciais: quebras de sigilo, rastreamento de criptoativos, cooperação internacional.

_ Atender titulares e clientes, se o caso, em canal dedicado, com o DPO.

_ Defender a empresa em processos sancionadores, ações individuais e coletivas e no sinistro com a seguradora.

_ Remediar e revisar a governança: o programa de conformidade é relevante para a avaliação das autoridades (ex. ANPD).

O que não fazer nas primeiras horas

Erros que destroem prova e ampliam a responsabilidade.

_ Desligar, formatar ou reinstalar equipamentos afetados antes da coleta forense.

_ Restaurar backup por cima do ambiente ainda comprometido.

_ Tratar o incidente pelo e-mail corporativo possivelmente comprometido.

_ Negociar ou pagar resgate sem análise jurídica, de sanções e de PLD.

_ Notificar reguladores ou o mercado sem validação técnica e jurídica do escopo.

_ Coletar evidência sem registrar quem coletou, quando, como e onde ficou armazenada.

O papel do advogado na sala de crise

Menos um parecer depois; mais uma decisão melhor agora.

_ **Coordena a apuração** e mantém a confidencialidade do que está sendo investigado enquanto o quadro ainda é incerto.

_ **Traduz achado técnico em dever legal:** define o que precisa ser notificado, a quem, em que prazo e com que conteúdo.

_ **Antecipa a consequência** criminal, regulatória, sancionatória e indenizatória de cada decisão tomada sob pressão.

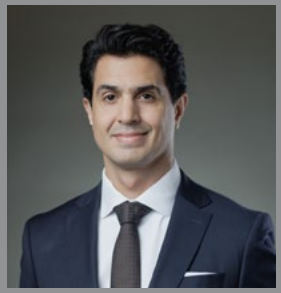
_ **Constrói a prova** que sustenta a persecução penal e a recuperação de ativos — e a defesa da empresa e de seus administradores.

Referências técnicas e normativas

NIST SP 800-61 · ISO/IEC 27035 e 27037 · CIS Controls · ENISA · CERT.br · LGPD e Resolução CD/ANPD nº 15/2024 · Marco Civil da Internet (Lei nº 12.965/2014) · Código de Processo Civil (Lei nº 13.105/2015) · Código Penal (Decreto-lei nº 2.848/1940) · Resolução CMN nº 4.893/2021 · Resolução BCB nº 85/2021 · Resolução CVM nº 44/2021.

Antes de decidir sozinho, entre em contato.

As decisões de maior impacto são tomadas nas primeiras horas, com informação incompleta e sob pressão. O Lefosse reúne especialistas em diferentes áreas do direito que, ao lado da equipe técnica e do time interno da empresa, servirão de ponto de apoio relevante no processo decisório.



Gabriel Queiroz
gabriel.queiroz@lefosse.com
+ 55 11 95387 4505

Renata Cardoso
renata.cardoso@lefosse.com
+ 55 11 99492 1060

Ricardo Nunes
ricardo.nunes@lefosse.com
+ 55 21 96845 8303

Lefosse

lefosse.com