RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

As primeiras horas após um ataque cibernético: detecção, contenção, preservação de evidências e recuperação como determinantes da resiliência organizacional

The first hours after a cyberattack: detection, containment, evidence preservation and recovery as determinants of organizational resilience

Las primeras horas tras un ataque cibernético: detección, contención, preservación de evidencias y recuperación como determinantes de la resiliencia organizacional

Cassiano Rodolfo Jung
Mestrando em Cybersecurity pela American Global Tech University (AGTU). Especialista em Inteligência e Investigação em Fontes Abertas (OSINT) pela WB Educação. Especialista em Computação Forense e Segurança da Informação pelo Instituto de Pós-Graduação e Graduação (IPOG). Especialista em Gestão Estratégica da Tecnologia da Informação pela Universidade Estácio de Sá. Tecnólogo em Segurança da Informação pela Universidade do Vale do Rio dos Sinos (UNISINOS).

RESUMO
O intervalo que separa a descoberta de um incidente cibernético das primeiras decisões de resposta concentra escolhas difíceis de reverter, como isolar ou manter sistemas em operação, preservar ou descartar vestígios voláteis e comunicar ou aguardar a confirmação dos fatos. Este artigo analisa como a detecção, a contenção, a preservação de evidências digitais, a comunicação regulatória e a recuperação operacional, quando conduzidas nas primeiras horas, condicionam a capacidade de uma organização de retomar suas atividades após um ataque. Trata-se de pesquisa qualitativa, de natureza exploratória e descritiva, construída por meio de revisão narrativa da literatura científica e de análise documental de normas técnicas, guias governamentais, relatórios setoriais e legislação. Os resultados indicam que o tempo de permanência do invasor no ambiente, a ordem de coleta dos dados voláteis, a disponibilidade de cópias de segurança isoladas e a existência prévia de papéis e canais de decisão definidos explicam boa parte da diferença entre incidentes contidos e crises prolongadas. Conclui-se que a qualidade da resposta inicial depende menos de improviso técnico e mais de preparação organizacional, o que exige tratar a resposta a incidentes como capacidade de gestão de risco, articulada à governança, à perícia digital e à continuidade de negócios.
Palavras-chave: Resposta a incidentes. Computação forense. Ransomware. Continuidade de negócios. Resiliência cibernética.

ABSTRACT
The interval between the discovery of a cyber incident and the first response decisions concentrates choices that are hard to reverse, such as isolating or keeping systems online, preserving or discarding volatile traces, and notifying stakeholders or waiting for facts to be confirmed. This article examines how detection, containment, digital evidence preservation, regulatory communication and operational recovery, when carried out in the first hours, shape an organization's ability to resume operations after an attack. It is a qualitative, exploratory and descriptive study based on a narrative review of the scientific literature and on documentary analysis of technical standards, government guidance, industry reports and legislation. The findings indicate that attacker dwell time, the order in which volatile data are collected, the availability of isolated backups and the prior definition of decision roles and channels account for much of the difference between contained incidents and prolonged crises. The study concludes that the quality of the initial response depends less on technical improvisation than on organizational preparedness, which requires treating incident response as a risk management capability linked to governance, digital forensics and business continuity.
Keywords: Incident response. Digital forensics. Ransomware. Business continuity. Cyber resilience.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

1 INTRODUÇÃO

Incidentes de segurança da informação deixaram de ser eventos raros, tratados de forma isolada pelas equipes de tecnologia, e passaram a integrar a rotina de risco de organizações de todos os portes. O relatório de investigações de violações de dados publicado pela Verizon em 2025 analisou mais de 22 mil incidentes, dos quais 12.195 foram confirmados como violações, e registrou a presença de *ransomware* em 44% desses casos (Verizon, 2025). No mesmo período, o estudo conduzido pelo Ponemon Institute para a IBM estimou o custo médio global de uma violação em US$ 4,44 milhões e o ciclo médio de identificação e contenção em 241 dias (IBM, 2025). Esses números revelam a frequência do problema e também a duração dos seus efeitos, que se estendem muito além do momento em que o ataque é percebido.

Entre a descoberta de um ataque e a estabilização do ambiente existe uma janela curta em que decisões de grande consequência precisam ser tomadas com informação incompleta. Desligar um servidor pode interromper a propagação de um código malicioso e, ao mesmo tempo, apagar da memória volátil os vestígios que permitiriam reconstruir a intrusão. Restaurar rapidamente os sistemas pode reduzir o prejuízo operacional, mas também reintroduzir o invasor se a via de acesso original não tiver sido identificada. Comunicar cedo demais pode gerar informações imprecisas, enquanto comunicar tarde demais pode violar prazos legais e comprometer a confiança de clientes e reguladores. É nesse conjunto de tensões que se concentra o objeto deste trabalho.

O objetivo deste artigo é analisar como a detecção, a contenção, a preservação de evidências digitais, a comunicação regulatória e a recuperação operacional, quando conduzidas nas primeiras horas após a descoberta de um incidente, influenciam a capacidade de uma organização de se recuperar. Parte-se da hipótese de que a qualidade dessa resposta inicial resulta mais da preparação prévia, expressa em papéis definidos, procedimentos testados e infraestrutura de recuperação isolada, do que da habilidade técnica mobilizada no momento da crise. Para sustentar essa discussão, o texto articula normas técnicas internacionais, estudos acadêmicos sobre equipes de resposta, relatórios setoriais com dados empíricos recentes e a legislação brasileira aplicável, além de casos documentados publicamente.

2 METODOLOGIA

A pesquisa adota abordagem qualitativa, de natureza exploratória e descritiva, nos termos propostos por Gil (2008), para quem os estudos exploratórios buscam proporcionar maior familiaridade com um problema e os descritivos procuram caracterizar fenômenos e estabelecer relações entre variáveis.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

A escolha se justifica pelo caráter multidisciplinar do tema, que envolve aspectos técnicos, organizacionais, jurídicos e de gestão, e pela inexistência de uma base de dados única capaz de medir, de forma comparável, o efeito das decisões tomadas nas primeiras horas de um incidente. Por essa razão, o estudo privilegia a integração de fontes de natureza diversa em vez da mensuração estatística de um único conjunto de dados.

Quanto aos procedimentos, foram combinadas a pesquisa bibliográfica e a pesquisa documental. A revisão de literatura seguiu o formato de revisão narrativa, que, segundo Rother (2007), é apropriada para descrever e discutir o estado da arte de um assunto sob o ponto de vista teórico e contextual, sem a pretensão de esgotar as fontes ou de aplicar critérios sistemáticos de busca e seleção. Foram consultados artigos publicados em periódicos revisados por pares, como *Computers & Security*, *Information & Management*, *International Journal of Information Management*, *Human Factors* e *Frontiers in Psychology*, identificados por meio de buscas no Google Acadêmico e nos portais das respectivas editoras, além de obras de referência em perícia digital e em gestão de organizações de alta confiabilidade.

A análise documental contemplou publicações técnicas do National Institute of Standards and Technology (NIST), normas da International Organization for Standardization (ISO) e da International Electrotechnical Commission (IEC), o documento RFC 3227 da Internet Engineering Task Force, o guia conjunto de agências norte-americanas sobre *ransomware*, a Lei Geral de Proteção de Dados Pessoais, o Código de Processo Penal com as alterações introduzidas pela Lei nº 13.964/2019 e a Resolução CD/ANPD nº 15/2024. Também foram examinados relatórios setoriais com dados empíricos amplamente citados pela literatura, publicados por Mandiant, IBM, Verizon e Sophos, e registros públicos de dois incidentes de grande repercussão, o ataque do NotPetya à empresa A. P. Møller-Maersk, em 2017, e o ataque de *ransomware* à Colonial Pipeline, em 2021.

O material foi organizado em seis eixos temáticos, definidos a partir das fases de resposta descritas nas normas de referência, a saber, os modelos de resposta, a detecção, a contenção, a preservação de evidências, a comunicação e a recuperação. Em cada eixo, procurou-se confrontar o que as normas recomendam com o que os estudos empíricos e os casos documentados revelam sobre a prática. Reconhece-se como limitação o fato de os relatórios setoriais serem produzidos por empresas privadas, com amostras e metodologias próprias que não permitem comparação direta entre si. Por isso, seus números são tratados como indicadores de tendência, e não como medidas exatas do fenômeno.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

3 MODELOS DE REFERÊNCIA PARA A RESPOSTA A INCIDENTES E SUA EVOLUÇÃO

Durante mais de uma década, a principal referência internacional para a organização da resposta a incidentes foi a segunda revisão da publicação especial 800-61 do NIST, elaborada por Cichonski *et al.* (2012). O documento descreve um ciclo composto por quatro fases, a preparação, a detecção e análise, a contenção, erradicação e recuperação e as atividades pós-incidente, e enfatiza que a resposta não termina com a restauração dos sistemas, pois o aprendizado obtido deve retornar à fase de preparação. O guia também recomenda que as organizações formalizem políticas, planos e procedimentos de resposta e definam a estrutura e os papéis da equipe responsável, o que permite que o processo seja documentado, comunicado aos gestores e verificado por auditorias internas e externas.
No campo da normalização internacional, a série ISO/IEC 27035 cumpre papel semelhante. A edição de 2023 da primeira parte da norma organiza a gestão de incidentes em cinco fases, o planejamento e preparação, a detecção e notificação, a avaliação e decisão, as respostas e as lições aprendidas (ISO, 2023). A separação entre a detecção e a fase de avaliação e decisão é especialmente relevante para o tema deste artigo, pois reconhece que nem todo evento detectado constitui um incidente e que a classificação correta, feita logo no início, determina a escala dos recursos mobilizados. Cichonski *et al.* (2012) observam, nesse sentido, que para muitas organizações a parte mais difícil do processo é justamente detectar e avaliar com precisão os possíveis incidentes, distinguindo precursores, indicadores e falsos positivos em meio a grande volume de alertas.
Em abril de 2025, o NIST publicou a terceira revisão da SP 800-61, assinada por Nelson *et al.* (2025), que substitui a versão de 2012 e altera de forma significativa a perspectiva adotada. Em vez de um ciclo próprio, a resposta a incidentes passa a ser descrita como um perfil comunitário do Cybersecurity Framework 2.0, distribuída entre as seis funções do modelo, governar, identificar, proteger, detectar, responder e recuperar (NIST, 2024). Segundo os autores, a resposta a incidentes deve ser incorporada às atividades de gestão de riscos de cibersegurança, de modo que a preparação, a redução do número e do impacto dos incidentes e a melhoria da detecção, da resposta e da recuperação sejam tratadas de forma integrada (Nelson *et al.*, 2025). Nessa perspectiva, a resposta deixa de ser uma atividade acionada apenas quando algo dá errado e passa a depender de decisões de governança, de inventário de ativos e de controles preventivos tomados antes do ataque.
A literatura acadêmica confirma que a distância entre o modelo normativo e a prática é real. Tøndel, Line e Jaatun (2014) realizaram revisão sistemática sobre a gestão de incidentes de segurança e organizaram as práticas relatadas segundo as fases da ISO/IEC 27035, concluindo que a prática observada é, em linhas gerais, compatível com a norma, mas identificando quais recomendações se mostram mais difíceis de seguir no cotidiano das organizações. Baskerville, Spagnoletti e Kim

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

(2014), a partir de estudo comparativo de casos em três organizações europeias, mostraram que as estratégias de segurança tendem a privilegiar a prevenção de ameaças previsíveis, embora a capacidade de resposta seja indispensável para lidar com ameaças imprevisíveis, o que exige equilíbrio deliberado entre os dois paradigmas.

Outro ponto recorrente na literatura é a desconexão entre as equipes de resposta e a gestão estratégica da segurança. Em estudo de caso sobre a resposta a incidentes na prática, Ahmad, Hadgkiss e Ruighaver (2012) observaram que a organização analisada seguia de perto as boas práticas do setor, mas concentrava sua atuação nos aspectos técnicos e na continuidade do negócio, deixando de realizar atividades de aprendizagem após os incidentes. Em estudo posterior, realizado em uma organização financeira australiana, Ahmad, Maynard e Shanks (2015) identificaram deficiências sistêmicas nas práticas de resposta e pouca comunicação entre os responsáveis pelos incidentes e a gestão de segurança, o que impede a organização de aprender com seus próprios ataques. O Quadro 1 sintetiza a correspondência entre os três modelos discutidos nesta seção, evidenciando que, apesar das diferenças de nomenclatura, todos reservam etapas específicas para a preparação, a detecção e o aprendizado posterior ao incidente.

Quadro 1 – Correspondência entre modelos de referência para resposta a incidentes

NIST SP 800-61 Rev. 2 (2012)	ISO/IEC 27035-1 (2023)	NIST SP 800-61 Rev. 3 e CSF 2.0 (2025)
Preparação	Planejamento e preparação	Governar, Identificar e Proteger
Detecção e análise	Detecção e notificação, Avaliação e decisão	Detectar
Contenção, erradicação e recuperação	Respostas	Responder e Recuperar
Atividades pós-incidente	Lições aprendidas	Identificar (melhoria contínua)

Fonte: elaborado pelo autor com base em Cichonski et al. (2012), ISO (2023), NIST (2024) e Nelson et al. (2025).

4 DETECÇÃO E TEMPO DE PERMANÊNCIA DO INVASOR

A expressão primeiras horas pressupõe que o incidente foi percebido, mas, na prática, a resposta começa a ser condicionada muito antes, pelo intervalo em que o invasor permanece no ambiente sem ser notado. A Mandiant, divisão de resposta a incidentes do Google Cloud, mede esse intervalo pelo indicador conhecido como "*dwell time*", definido como o número de dias entre o início da intrusão e sua identificação. Segundo o relatório M-Trends 2025, a mediana global desse tempo foi de 11 dias

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

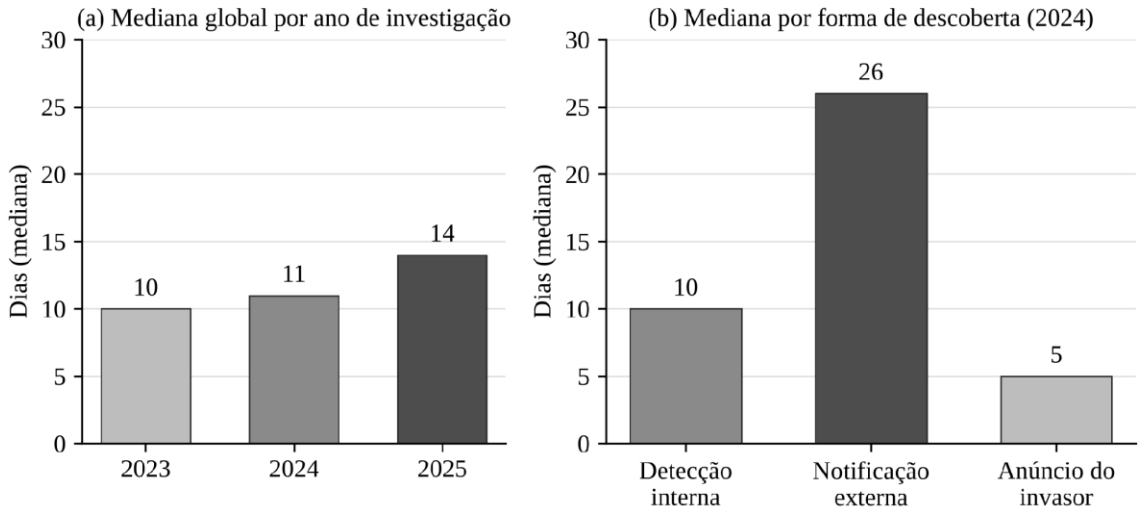
RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

nas investigações conduzidas em 2024, ligeiramente acima dos 10 dias observados em 2023 (Mandiant, 2025). A edição seguinte registrou nova elevação, com mediana de 14 dias nas investigações de 2025 (Mandiant, 2026).

Mais revelador do que a mediana global é o contraste entre as formas de descoberta. Nas investigações de 2024, quando a própria organização identificou a atividade maliciosa, a mediana foi de 10 dias, enquanto nos casos em que a descoberta partiu de uma entidade externa ela chegou a 26 dias. Quando o próprio invasor anunciou sua presença, situação típica dos ataques de *ransomware* em que a nota de resgate é o primeiro sinal percebido, a mediana caiu para 5 dias (Mandiant, 2025). A Figura 1 apresenta esses valores. O valor de 5 dias não deve ser lido como sinal de eficiência defensiva, pois, nesses casos, a descoberta não resulta do monitoramento da vítima, e sim da decisão do atacante de se revelar, o que coloca a organização em posição de responder sob pressão máxima.

Figura 1 – Tempo mediano de permanência do invasor no ambiente, em dias



Fonte: elaborado pelo autor com dados de Mandiant (2025; 2026).

Os números da Mandiant e os da IBM medem fenômenos distintos e não devem ser confundidos. Enquanto a Mandiant calcula a mediana do tempo de permanência nas intrusões que investigou, o estudo da IBM estima a média de dias necessários para identificar e conter uma violação de dados, incluindo a restauração dos serviços, em uma amostra de 600 organizações. Ainda assim, ambos apontam na mesma direção. O ciclo medido pela IBM caiu para 241 dias no estudo de 2025, o menor patamar em nove anos e 17 dias abaixo do resultado do ano anterior, o que sugere ganhos de eficiência que, embora relevantes, ainda deixam as organizações expostas por meses (IBM, 2025).

A capacidade de detectar precocemente depende de visibilidade e de método. O modelo de cadeia de intrusão proposto por Hutchins, Cloppert e Amin (2011) descreve o ataque como uma sequência de

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

etapas, do reconhecimento à execução dos objetivos, e sustenta que o defensor pode frustrar a operação adversária ao interromper qualquer uma delas. A base de conhecimento MITRE ATT&CK, descrita por Strom *et al.* (2018), aprofundou essa lógica ao catalogar táticas e técnicas efetivamente observadas em ataques reais, permitindo que as equipes de monitoramento formulem hipóteses de detecção orientadas por comportamento, e não apenas por assinaturas de códigos já conhecidos. Os dados mais recentes mostram por que isso importa, já que a exploração de vulnerabilidades respondeu por 32% das intrusões investigadas em 2025 e o *phishing* por voz alcançou 11% (Mandiant, 2026).

A detecção não é apenas um problema de ferramentas, mas também de cognição. Endsley (1995) descreveu a consciência situacional em três níveis, a percepção dos elementos do ambiente, a compreensão do seu significado e a projeção de seu estado futuro, e mostrou que falhas em qualquer um deles comprometem a tomada de decisão em sistemas dinâmicos. Por analogia, aplicado a um centro de operações de segurança, o modelo pode ajudar a explicar por que um alerta corretamente gerado pode ser ignorado, quando o analista percebe o evento mas não compreende sua relação com outros sinais, ou porque uma intrusão compreendida tarde demais já não permite contenção eficaz. Van der Kleij, Kleinhuis e Young (2017), ao investigarem equipes de resposta nos Países Baixos, propuseram um modelo de necessidades que distribui os fatores de desempenho entre os níveis organizacional, de equipe, individual e instrumental, indicando que problemas de desempenho podem se originar em qualquer um desses níveis ou na combinação entre eles.

5 CONTENÇÃO E TOMADA DE DECISÃO SOB PRESSÃO

A contenção é a fase em que a resposta a incidentes produz seus efeitos mais imediatos sobre a operação da organização. Cichonski *et al.* (2012) recomendam que a estratégia de contenção seja escolhida com base em critérios definidos previamente, entre os quais o potencial de dano e de subtração de recursos, a necessidade de preservação de evidências, a disponibilidade dos serviços, o tempo e os recursos exigidos, a eficácia esperada da medida e a duração da solução. Os autores recomendam ainda que as organizações elaborem estratégias de contenção distintas para cada tipo principal de incidente, com critérios claramente documentados, justamente para facilitar a tomada de decisão quando o incidente ocorre.

O caso da Colonial Pipeline ilustra a escala que essas decisões podem assumir. Segundo o depoimento do então presidente da empresa ao Comitê de Segurança Interna e Assuntos Governamentais do Senado norte-americano, um funcionário encontrou uma nota de resgate em um sistema da rede de tecnologia da informação pouco antes das 5 horas da manhã de 7 de maio de 2021, e às 6h10 a empresa confirmou que as cerca de 5.500 milhas de dutos, o equivalente a aproximadamente 8.850

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

quilômetros, haviam sido paralisadas (Blount, 2021). A rede transportava quase metade do combustível consumido na costa leste dos Estados Unidos, e a operação só começou a ser retomada na noite de 12 de maio. O mesmo depoimento atribui o acesso inicial a um perfil legado de rede virtual privada (VPN) que não deveria estar em uso.

O episódio mostra que a contenção pode exigir a interrupção deliberada de operações antes que se saiba se foram atingidas. No mesmo depoimento, o executivo afirmou que a paralisação buscou isolar e conter o ataque para evitar que o código malicioso se espalhasse para a rede de tecnologia operacional, que controla os dutos, caso isso ainda não tivesse ocorrido, e reconheceu que a empresa não conhecia, naquele momento, nem o ponto de origem nem o alcance do ataque (Blount, 2021). O intervalo de pouco mais de uma hora entre a descoberta e a paralisação total indica que uma decisão dessa magnitude foi tomada antes de qualquer diagnóstico completo, o que reforça a recomendação de Cichonski *et al.* (2012) de documentar previamente os critérios de contenção.

O guia conjunto sobre *ransomware* publicado pela agência norte-americana de cibersegurança e infraestrutura em parceria com outras agências recomenda determinar quais sistemas foram afetados e isolá-los imediatamente, desconectando a rede no nível dos comutadores quando o comprometimento for amplo (CISA, 2023). O mesmo documento orienta que os equipamentos só sejam desligados quando não for possível desconectá-los da rede, advertindo que o desligamento elimina evidências armazenadas na memória volátil. O guia também recomenda o uso de canais de comunicação alternativos, como chamadas telefônicas, para evitar que o invasor, eventualmente presente nos sistemas de correio e mensagens, acompanhe a coordenação da resposta e antecipe as medidas de contenção.

A literatura sobre organizações de alta confiabilidade oferece uma lente útil para compreender esse comportamento. Weick e Sutcliffe (2015) identificam cinco princípios que distinguem organizações capazes de operar em ambientes de alto risco com baixa incidência de falhas graves, a preocupação com o fracasso, a relutância em simplificar interpretações, a sensibilidade às operações, o compromisso com a resiliência e a deferência à competência técnica. Este último princípio é particularmente pertinente à contenção, pois propõe que, em situações críticas, a autoridade decisória migre para quem detém o conhecimento mais preciso sobre o problema, independentemente da posição hierárquica. Aplicado a um incidente cibernético, o princípio sugere que o analista que compreende a mecânica do ataque tenha acesso direto a quem pode autorizar a interrupção de sistemas.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

6 PRESERVAÇÃO DE EVIDÊNCIAS DIGITAIS NAS PRIMEIRAS HORAS

A pressão pela retomada das operações tende a colocar a preservação de evidências em segundo plano, embora as orientações técnicas sejam claras quanto à prioridade da coleta sobre as intervenções corretivas. O documento RFC 3227, elaborado por Brezinski e Killalea (2002), estabelece que a coleta deve seguir a ordem de volatilidade, começando pelos registradores e pela memória cache, passando pelas tabelas de roteamento, pela tabela de processos e pela memória principal, pelos sistemas de arquivos temporários e pelo disco, até chegar aos registros remotos, à topologia da rede e às mídias de arquivamento. O mesmo documento recomenda não desligar o sistema antes de concluir a coleta e não confiar nos programas instalados na máquina comprometida, que podem ter sido alterados pelo invasor.

Kent *et al.* (2006), no guia do NIST dedicado à integração de técnicas forenses à resposta a incidentes, descrevem o processo forense em quatro etapas, a coleta, o exame, a análise e o relato, e chamam a atenção para o fato de que muitas decisões tomadas durante a resposta, como reiniciar um servidor ou aplicar uma correção, alteram irreversivelmente o estado dos dados. Por essa razão, os autores recomendam que as organizações disponham de capacidade forense, apoiada em políticas e procedimentos que orientem, entre outras atividades, a coleta de dados voláteis antes do desligamento dos sistemas. Orientação semelhante aparece no guia sobre *ransomware*, que recomenda a captura de imagem e de memória de uma amostra dos equipamentos afetados (CISA, 2023).

No plano normativo internacional, a ISO/IEC 27037 estabelece diretrizes para a identificação, a coleta, a aquisição e a preservação de evidências digitais (ISO, 2012). A norma sustenta que o tratamento dessas evidências deve ser auditável, repetível, reprodutível e justificável, de modo que um terceiro possa avaliar as ações realizadas e, quando aplicável, obter os mesmos resultados a partir dos mesmos dados. Casey (2011) acrescenta que a integridade da evidência digital depende de documentação rigorosa de cada ação executada, do uso de funções de *hash* para demonstrar que os dados não foram alterados e da compreensão das limitações das ferramentas empregadas, já que a evidência digital é, por natureza, fácil de modificar sem deixar rastros evidentes.

No Brasil, a preservação de evidências ganhou contornos legais mais precisos com a Lei nº 13.964/2019, que inseriu os artigos 158-A a 158-F no Código de Processo Penal e definiu a cadeia de custódia como o conjunto de procedimentos utilizados para manter e documentar a história cronológica do vestígio, desde seu reconhecimento até o descarte (Brasil, 2019). O artigo 158-B detalha as etapas desse percurso, que incluem o reconhecimento, o isolamento, a fixação, a coleta, o acondicionamento, o transporte, o recebimento, o processamento, o armazenamento e o descarte. O texto legal não distingue a natureza do vestígio, de modo que seus requisitos alcançam também os

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

vestígios digitais, e falhas cometidas nas primeiras horas podem comprometer o aproveitamento da prova em eventual persecução penal decorrente do incidente.

A tensão entre preservar e restaurar, portanto, não se resolve pela escolha de um dos polos. O guia sobre *ransomware* propõe uma solução intermediária ao recomendar a captura de imagem e de memória de uma amostra dos equipamentos afetados, e não de todos, o que permite reunir elementos para a investigação sem paralisar a recuperação (CISA, 2023). A aplicação dessa estratégia, contudo, pressupõe procedimentos de coleta e armazenamento seguro das imagens definidos antes do incidente, como recomendam Kent *et al.* (2006). Sem essa preparação, a restauração imediata tende a apagar os vestígios que permitiriam identificar a via de entrada, o alcance do comprometimento e a eventual subtração de dados, com o consequente risco de reinfecção, para o qual o próprio guia alerta ao tratar da fase de recuperação.

7 COMUNICAÇÃO, GOVERNANÇA E OBRIGAÇÕES REGULATÓRIAS

A comunicação durante um incidente envolve públicos distintos, cada qual com necessidades e prazos próprios, como a alta administração, as equipes internas, os clientes, os fornecedores, as autoridades reguladoras e, em alguns casos, as forças de segurança e a imprensa. A introdução da função governar no Cybersecurity Framework 2.0 reconhece que a definição de papéis, responsabilidades e autoridades em cibersegurança é atribuição da direção da organização, e não apenas da área técnica (NIST, 2024). Na resposta a incidentes, essa definição se traduz em saber, antes da crise, quem decide sobre a comunicação externa, quem fala em nome da empresa e quais informações podem ser divulgadas sem prejudicar a investigação ou a contenção.

No ordenamento brasileiro, o artigo 48 da Lei Geral de Proteção de Dados Pessoais determina que o controlador comunique à Autoridade Nacional de Proteção de Dados e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (Brasil, 2018). O prazo foi fixado pela Resolução CD/ANPD nº 15, de 24 de abril de 2024, que estabelece três dias úteis, contados do conhecimento de que o incidente afetou dados pessoais, tanto para a comunicação à autoridade quanto para a comunicação aos titulares, admitindo complementação fundamentada em até vinte dias úteis e prazo em dobro para agentes de tratamento de pequeno porte (ANPD, 2024). A mesma norma exige que o registro do incidente seja mantido por, no mínimo, cinco anos, inclusive quando não houver comunicação.

A resolução também define critérios objetivos para caracterizar o risco ou dano relevante, exigindo que o incidente possa afetar significativamente interesses e direitos fundamentais dos titulares e que envolva ao menos um tipo específico de dado, como dados sensíveis, dados de crianças, adolescentes

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

RCMOS – Revista Científica Multidisciplinar O Saber.
ISSN: 2675-9128. São Paulo-SP.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

ou idosos, dados financeiros, dados de autenticação, dados protegidos por sigilo ou dados em larga escala (ANPD, 2024). Como o prazo de comunicação é contado em dias úteis a partir do conhecimento do incidente, essa classificação precisa começar nas primeiras horas, quando a extensão do comprometimento ainda é incerta. A integração entre a equipe técnica, responsável por determinar quais dados foram acessados, e o encarregado pelo tratamento de dados pessoais, a quem a lei atribui a interlocução com a autoridade e com os titulares, torna-se assim um requisito operacional, e não apenas uma recomendação de boa governança.

Outras jurisdições adotam prazos igualmente curtos, o que afeta diretamente organizações com operações internacionais. O Regulamento Geral sobre a Proteção de Dados da União Europeia, em seu artigo 33, determina que a violação de dados pessoais seja notificada à autoridade de controle sem demora injustificada e, sempre que possível, no prazo de 72 horas após o responsável ter tido conhecimento do fato (União Europeia, 2016). Nos Estados Unidos, a regra aprovada pela Securities and Exchange Commission em 2023 exige que companhias de capital aberto divulguem incidentes de cibersegurança considerados materiais no prazo de quatro dias úteis após a determinação da materialidade (United States, 2023). A sobreposição desses prazos obriga as organizações a manter modelos de comunicação e fluxos de aprovação prontos antes de qualquer incidente.

A comunicação com fornecedores e parceiros ganhou importância à medida que os ataques passaram a explorar relações de confiança entre empresas. O relatório da Verizon de 2025 indica que a participação de terceiros nas violações dobrou, alcançando 30% dos casos analisados (Verizon, 2025). Isso significa que, em parcela considerável dos incidentes, a resposta exige coordenação com organizações externas, cujos processos, prazos e prioridades podem divergir dos da vítima. A experiência relatada por Ahmad, Maynard e Shanks (2015) mostra ainda que a falta de comunicação interna entre a resposta e a gestão de segurança impede o aprendizado organizacional, o que sugere que a comunicação deve ser tratada como parte do próprio processo de resposta, com registros que alimentem a revisão posterior do incidente.

8 RECUPERAÇÃO, CONTINUIDADE DE NEGÓCIOS E PAPEL DAS CÓPIAS DE SEGURANÇA

A recuperação é frequentemente tratada como a última fase da resposta, mas suas condições de sucesso são definidas muito antes do incidente. O guia do NIST para planejamento de contingência, elaborado por Swanson *et al.* (2010), recomenda que a organização realize uma análise de impacto nos negócios para estabelecer, para cada sistema, o tempo máximo tolerável de indisponibilidade, o objetivo de tempo de recuperação e o objetivo de ponto de recuperação, que expressa a quantidade

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

máxima de dados que se admite perder. A ISO 22301 insere essas definições em um sistema de gestão da continuidade de negócios, com requisitos de planejamento, operação, avaliação de desempenho e melhoria contínua (ISO, 2019). Sem esses parâmetros, falta à equipe um critério objetivo para definir a ordem de restauração, que o próprio guia associa aos resultados da análise de impacto.

O papel das cópias de segurança mudou de forma significativa com a profissionalização dos ataques de *ransomware*. Na pesquisa da Sophos com 5.000 líderes de tecnologia e segurança em 14 países, 94% das organizações atingidas por *ransomware* relataram que os invasores tentaram comprometer suas cópias de segurança durante o ataque, e 57% dessas tentativas tiveram êxito (Sophos, 2024a). O mesmo estudo estimou o custo médio de recuperação, excluídos eventuais pagamentos de resgate, em US$2,73 milhões. Os dados mais recentes da Mandiant (2026) confirmam a tendência, ao registrar grupos de *ransomware* direcionando seus esforços para a infraestrutura de cópias de segurança, para os serviços de identidade e para as plataformas de gerenciamento de virtualização.

O caso da A. P. Møller-Maersk, atingida pelo NotPetya em 27 de junho de 2017, tornou-se referência sobre a fragilidade das estratégias de recuperação. Segundo reportagem de Greenberg (2018), o código malicioso destruiu os controladores de domínio da empresa em todo o mundo, e a reconstrução da infraestrutura só foi possível porque um único controlador, instalado em um escritório em Gana, estava desconectado da rede por causa de uma queda de energia no momento do ataque. A empresa reconstruiu cerca de 4 mil servidores e 45 mil computadores, a rede foi restabelecida em dez dias e o prejuízo foi estimado pelo presidente do conselho entre US$250 milhões e US$300 milhões. O episódio mostra que a recuperação dependeu de um acaso, e não de uma cópia isolada mantida de forma planejada.

A lição técnica desses casos foi incorporada às recomendações oficiais. O guia conjunto sobre *ransomware* orienta que os dados sejam restaurados a partir de cópias de segurança desconectadas e criptografadas, seguindo uma ordem de prioridade baseada nos serviços críticos, e alerta para o risco de reinfectar sistemas já limpos durante a restauração (CISA, 2023). Ross *et al.* (2021), no guia do NIST sobre engenharia de sistemas resilientes, propõem que a resiliência cibernética seja estruturada em torno de quatro objetivos, antecipar, resistir, recuperar e adaptar, abordagem que parte do pressuposto de que a proteção pode falhar e busca assegurar a continuidade das funções essenciais mesmo em condições adversas.

A decisão sobre o pagamento de resgate também se associa à disponibilidade de meios próprios de recuperação. Em levantamento com 2.974 profissionais de organizações atingidas por *ransomware*, a Sophos verificou que as vítimas cujas cópias de segurança foram comprometidas pagaram o resgate em 67% dos casos, contra 36% entre as que mantiveram suas cópias intactas, e que apenas 26% das primeiras se recuperaram totalmente em até uma semana, ante 46% das demais (Sophos, 2024b). O

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

estudo da IBM registrou que a proporção de vítimas que se recusaram a pagar subiu de 59% para 63% em 2025 (IBM, 2025). A capacidade de recuperação, contudo, depende de planos testados. Grance *et al.* (2006) defendem que os planos de tecnologia da informação sejam submetidos a programas regulares de testes, treinamentos e exercícios, incluindo simulações de mesa e exercícios funcionais, justamente para revelar falhas que só apareceriam durante uma crise real.

9 CONCLUSÃO

Este artigo partiu da premissa de que as primeiras horas após a descoberta de um ataque cibernético concentram decisões cujos efeitos se estendem por semanas ou meses. A análise da literatura, das normas técnicas, dos relatórios setoriais e dos casos documentados confirma essa premissa e permite qualificá-la. As decisões iniciais são de fato determinantes, mas sua qualidade raramente é produzida no momento da crise, pois resulta de condições criadas antes do incidente, como a definição de papéis, a existência de procedimentos testados e a disponibilidade de infraestrutura de recuperação isolada do ambiente de produção.

A evolução dos modelos de referência expressa esse entendimento. A substituição do ciclo próprio da segunda revisão da SP 800-61 por um perfil integrado ao Cybersecurity Framework 2.0 indica que a resposta a incidentes deixou de ser concebida como atividade técnica acionada apenas em situações excepcionais e passou a ser compreendida como capacidade de gestão de risco, vinculada à governança. A literatura acadêmica reforça essa leitura ao demonstrar a persistente desconexão entre equipes de resposta e gestão estratégica da segurança, o que limita a capacidade das organizações de aprender com os próprios incidentes.

No eixo da detecção, os dados mostram que o tempo de permanência do invasor continua medido em dias e que a mediana global subiu de 10 para 14 dias entre as investigações de 2023 e de 2025. O contraste entre a descoberta interna, a notificação externa e o anúncio feito pelo próprio atacante evidencia que a forma como o incidente é percebido condiciona o espaço de manobra disponível. Quando o primeiro sinal é a nota de resgate, a resposta começa em desvantagem, pois o adversário já cumpriu seus objetivos. Investir em visibilidade, em detecção orientada por comportamento e em consciência situacional das equipes é, portanto, investir na qualidade das primeiras horas.

No eixo da contenção, as fontes analisadas convergem para a importância de critérios de decisão definidos antecipadamente, de autoridade clara para interromper operações e de canais de comunicação alternativos, que permitem agir com rapidez sem agir às cegas. O caso da Colonial Pipeline mostra que a interrupção preventiva de operações pode ser necessária antes mesmo de se conhecer a origem e o alcance do ataque, o que só é viável quando a organização sabe quem tem

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

legitimidade para tomar essa decisão e quais critérios a sustentam. Os princípios das organizações de alta confiabilidade oferecem fundamentação teórica consistente para essa prática.

A preservação de evidências digitais mostrou-se um ponto crítico, exposto ao risco de ser sacrificado em nome da rapidez. A ordem de volatilidade, os princípios de auditabilidade e reprodutibilidade e as exigências da cadeia de custódia previstas no Código de Processo Penal brasileiro convergem para a mesma conclusão de que a coleta precisa ocorrer antes das intervenções corretivas. A perda dessas evidências compromete a investigação, a responsabilização dos autores e a própria segurança da recuperação, pois impede saber se o acesso do invasor foi efetivamente eliminado. A preparação forense deve ser tratada como parte integrante da resposta, e não como atividade acessória.

As obrigações regulatórias acrescentam uma dimensão temporal que não pode ser ignorada. O prazo de três dias úteis fixado pela Autoridade Nacional de Proteção de Dados, somado aos prazos de outras jurisdições, exige que a avaliação do risco aos titulares seja iniciada nas primeiras horas, com integração efetiva entre a equipe técnica e o encarregado pelo tratamento de dados pessoais. A crescente participação de terceiros nas violações amplia essa exigência, pois a comunicação passa a envolver cadeias de fornecedores cujos processos nem sempre estão alinhados aos da organização afetada.

No eixo da recuperação, os dados sobre ataques direcionados às cópias de segurança e o caso da Maersk mostram que a existência de uma cópia não basta, sendo necessário que ela esteja isolada, íntegra e restaurável dentro dos objetivos de tempo definidos pela análise de impacto nos negócios. Os dados que associam o comprometimento das cópias de segurança a maior propensão ao pagamento de resgate e a recuperação mais lenta indicam que a capacidade própria de recuperação amplia a margem de decisão da organização diante da extorsão. Essa margem, contudo, só existe quando os planos de continuidade são exercitados periodicamente e ajustados a partir das falhas identificadas.

Como limitação, registra-se que parte relevante dos dados empíricos utilizados provém de relatórios setoriais elaborados por empresas privadas, com amostras e metodologias distintas, o que impede comparações diretas e recomenda cautela na generalização dos resultados. Sugere-se, para pesquisas futuras, a realização de estudos empíricos com organizações brasileiras que avaliem a relação entre maturidade em resposta a incidentes, tempo de recuperação e cumprimento dos prazos regulatórios, bem como investigações sobre a aplicação da cadeia de custódia a vestígios digitais em incidentes corporativos. Tais estudos permitiriam verificar, em contexto nacional, a hipótese central sustentada neste trabalho.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

REFERÊNCIAS

AHMAD, Atif; HADGKISS, Justin; RUIGHAVER, A. B. Incident response teams: challenges in supporting the organisational security function. **Computers & Security**, [Amsterdam], v. 31, n. 5, p. 643-652, 2012.

AHMAD, Atif; MAYNARD, Sean B.; SHANKS, Graeme. A case analysis of information systems and security incident responses. **International Journal of Information Management**, [Amsterdam], v. 35, n. 6, p. 717-723, 2015. DOI: 10.1016/j.ijinfomgt.2015.08.001.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Resolução CD/ANPD nº 15, de 24 de abril de 2024**. Aprova o Regulamento de Comunicação de Incidente de Segurança. Brasília, DF: ANPD, 2024.

BASKERVILLE, Richard; SPAGNOLETTI, Paolo; KIM, Jongwoo. Incident-centered information security: managing a strategic balance between prevention and response. **Information & Management**, [Amsterdam], v. 51, n. 1, p. 138-151, 2014. DOI: 10.1016/j.im.2013.11.004.

BLOUNT, Joseph A. **Testimony of Joseph A. Blount, Jr., President and Chief Executive Officer, Colonial Pipeline Company, before the United States Senate Committee on Homeland Security and Governmental Affairs**. Washington, DC: U.S. Senate, 8 jun. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018.

BRASIL. **Lei nº 13.964, de 24 de dezembro de 2019**. Aperfeiçoa a legislação penal e processual penal. Brasília, DF: Presidência da República, 2019.

BREZINSKI, Dominique; KILLALEA, Tom. **Guidelines for evidence collection and archiving**. RFC 3227. [S. l.]: Internet Engineering Task Force, 2002.

CASEY, Eoghan. **Digital evidence and computer crime**: forensic science, computers and the internet. 3. ed. Waltham: Academic Press, 2011.

CICHONSKI, Paul; MILLAR, Tom; GRANCE, Tim; SCARFONE, Karen. **Computer security incident handling guide**. Gaithersburg: National Institute of Standards and Technology, 2012. (NIST Special Publication 800-61, rev. 2). DOI: 10.6028/NIST.SP.800-61r2.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) *et al.* **#StopRansomware guide**. Washington, DC: CISA, 2023.

ENDSLEY, Mica R. Toward a theory of situation awareness in dynamic systems. **Human Factors**, [Thousand Oaks], v. 37, n. 1, p. 32-64, 1995. DOI: 10.1518/001872095779049543.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2008.

GRANCE, Tim; NOLAN, Tamara; BURKE, Kristin; DUDLEY, Rich; WHITE, Gregory; GOOD, Travis. **Guide to test, training, and exercise programs for IT plans and capabilities**. Gaithersburg: National Institute of Standards and Technology, 2006. (NIST Special Publication 800-84).

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

GREENBERG, Andy. The untold story of NotPetya, the most devastating cyberattack in history. **Wired**, San Francisco, 22 ago. 2018.

HUTCHINS, Eric M.; CLOPPERT, Michael J.; AMIN, Rohan M. **Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains**. Bethesda: Lockheed Martin Corporation, 2011.

IBM. **Cost of a data breach report 2025**. Armonk: IBM Corporation, 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27037**: information technology, security techniques, guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO, 2012.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO 22301**: security and resilience, business continuity management systems, requirements. Geneva: ISO, 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO). **ISO/IEC 27035-1**: information technology, information security incident management, part 1, principles and process. Geneva: ISO, 2023.

KENT, Karen; CHEVALIER, Suzanne; GRANCE, Tim; DANG, Hung. **Guide to integrating forensic techniques into incident response**. Gaithersburg: National Institute of Standards and Technology, 2006. (NIST Special Publication 800-86).

MANDIANT. **M-Trends 2025**. Mountain View: Google Cloud, 2025.

MANDIANT. **M-Trends 2026**. Mountain View: Google Cloud, 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **The NIST Cybersecurity Framework (CSF) 2.0**. Gaithersburg: NIST, 2024. (NIST Cybersecurity White Paper 29). DOI: 10.6028/NIST.CSWP.29.

NELSON, Alexander; REKHI, Sanjay; SOUPPAYA, Murugiah; SCARFONE, Karen. **Incident response recommendations and considerations for cybersecurity risk management**: a CSF 2.0 community profile. Gaithersburg: National Institute of Standards and Technology, 2025. (NIST Special Publication 800-61, rev. 3). DOI: 10.6028/NIST.SP.800-61r3.

ROSS, Ron; PILLITTERI, Victoria; GRAUBART, Richard; BODEAU, Deborah; MCQUAID, Rosalie. **Developing cyber-resilient systems**: a systems security engineering approach. Gaithersburg: National Institute of Standards and Technology, 2021. (NIST Special Publication 800-160, v. 2, rev. 1). DOI: 10.6028/NIST.SP.800-160v2r1.

ROTHER, Edna Terezinha. Revisão sistemática X revisão narrativa. **Acta Paulista de Enfermagem**, São Paulo, v. 20, n. 2, p. v-vi, 2007.

SOPHOS. **The state of ransomware 2024**. Abingdon: Sophos, 2024a.

SOPHOS. **The impact of compromised backups on ransomware outcomes**. Abingdon: Sophos, 2024b.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.

Ano VII, v.2 2026 | submissão: 06/05/2026 | aceito: 09/06/2026 | publicação: 11/07/2026

STROM, Blake E.; APPLEBAUM, Andy; MILLER, Doug P.; NICKELS, Kathryn C.; PENNINGTON, Adam G.; THOMAS, Cody B. **MITRE ATT&CK**: design and philosophy. McLean: The MITRE Corporation, 2018.

SWANSON, Marianne; BOWEN, Pauline; PHILLIPS, Amy Wohl; GALLUP, Dean; LYNES, David. **Contingency planning guide for federal information systems**. Gaithersburg: National Institute of Standards and Technology, 2010. (NIST Special Publication 800-34, rev. 1). DOI: 10.6028/NIST.SP.800-34r1.

TØNDEL, Inger Anne; LINE, Maria B.; JAATUN, Martin Gilje. Information security incident management: current practice as reported in the literature. **Computers & Security**, [Amsterdam], v. 45, p. 42-57, 2014.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial da União Europeia**, Luxemburgo, L 119, p. 1-88, 4 maio 2016.

UNITED STATES. Securities and Exchange Commission. **Cybersecurity risk management, strategy, governance, and incident disclosure**. Release n. 33-11216. Washington, DC: SEC, 2023.

VAN DER KLEIJ, Rick; KLEINHUIS, Geert; YOUNG, Heather. Computer security incident response team effectiveness: a needs assessment. **Frontiers in Psychology**, Lausanne, v. 8, art. 2179, 2017. DOI: 10.3389/fpsyg.2017.02179.

VERIZON. **2025 data breach investigations report**. Basking Ridge: Verizon Business, 2025.

Este é um artigo publicado em acesso aberto (Open Access) sob a licença CreativeCommons Attribution, que permite uso, distribuição e reprodução em qualquer meio, sem restrições desde que o trabalho original seja corretamente citado.