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

Ano VII, v.2 2026 | submissão: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

Governança da segurança cibernética como responsabilidade da alta administração em pequenas e médias empresas

Cybersecurity governance as a responsibility of top management in small and medium-sized enterprises

Gobernanza de la ciberseguridad como responsabilidad de la alta dirección en pequeñas y medianas empresas

Eduardo Henrique Bergel Cosenza Junior
Bacharel em Direito. MBA em Direito da Saúde e Compliance Hospitalar. Formação técnica em transações imobiliárias. Advogado inscrito na Ordem dos Advogados do Brasil (OAB).

RESUMO

O presente artigo examina os fundamentos teóricos e normativos que sustentam a atribuição da segurança cibernética à alta administração, com ênfase nas pequenas e médias empresas. Parte-se da constatação de que a dependência crescente de dados, sistemas e fornecedores de tecnologia transformou o risco cibernético em risco de negócio, com efeitos sobre a continuidade operacional, a reputação e o resultado financeiro. A pesquisa adota abordagem qualitativa, de natureza exploratória e descritiva, conduzida por meio de revisão narrativa de literatura com elementos de revisão integrativa e de análise documental de normas técnicas, marcos de referência e legislação. O referencial articula a literatura sobre governança da segurança da informação, a teoria da agência, a teoria dos escalões superiores, a economia da segurança da informação, os estudos sobre comportamento de conformidade, a teoria dos acidentes organizacionais e a teoria das organizações de alta confiabilidade, em diálogo com a família ISO/IEC 27000, o NIST Cybersecurity Framework 2.0, a Lei Geral de Proteção de Dados Pessoais e a regulamentação da Autoridade Nacional de Proteção de Dados. Os resultados indicam que a segurança cibernética integra o dever de diligência dos administradores e que sua efetividade depende de decisões de governança sobre investimento, cultura, gestão de terceiros e preparação para incidentes. Conclui-se que pequenas e médias empresas podem exercer essa responsabilidade por meio de medidas proporcionais ao seu porte, desde que o tema seja assumido diretamente por seus dirigentes.

Palavras-chave: segurança cibernética; governança corporativa; alta administração; gestão de riscos; proteção de dados.

ABSTRACT

This article examines the theoretical and regulatory foundations for assigning cybersecurity to top management, with emphasis on small and medium-sized enterprises. It starts from the observation that growing dependence on data, systems and technology suppliers has turned cyber risk into business risk, with effects on operational continuity, reputation and financial performance. The research adopts a qualitative, exploratory and descriptive approach, carried out through a narrative literature review with elements of integrative review and through documentary analysis of technical standards, reference frameworks and legislation. The theoretical framework combines the literature on information security governance, agency theory, upper echelons theory, the economics of information security, studies on compliance behavior, the theory of organizational accidents and the theory of high reliability organizations, in dialogue with the ISO/IEC 27000 family, the NIST Cybersecurity Framework 2.0, the Brazilian General Data Protection Law and the regulations of the Brazilian National Data Protection Authority. The results indicate that cybersecurity is part of the directors' duty of care and that its effectiveness depends on governance decisions regarding investment, culture, third-party management and incident preparedness. The study concludes that small and medium-sized enterprises can fulfill this responsibility through measures proportionate to their size, provided that their leaders take direct ownership of the issue.

Keywords: cybersecurity; corporate governance; top management; risk management; data

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

protection.

1 INTRODUÇÃO

Durante boa parte das últimas décadas, a segurança da informação foi tratada nas organizações como atribuição do setor de tecnologia, delegada a técnicos e medida pela aquisição de equipamentos e programas de proteção. Essa compreensão tornou-se insuficiente à medida que dados, sistemas e serviços digitais passaram a sustentar praticamente todas as atividades empresariais, do faturamento à relação com clientes. Von Solms e Van Niekerk (2013) observaram que a segurança cibernética ultrapassa a proteção da informação em sentido estrito, pois envolve a proteção de pessoas, ativos e interesses que podem ser atingidos por meio do ciberespaço. Quando um ataque interrompe a operação, expõe dados de clientes ou compromete a reputação de uma empresa, o problema deixa de ser técnico e passa a ser estratégico, alcançando diretamente a esfera de decisão de quem dirige o negócio.

O movimento é visível nos referenciais normativos mais recentes. A versão 2.0 do Cybersecurity Framework, publicada pelo National Institute of Standards and Technology em 2024, acrescentou às funções tradicionais de identificar, proteger, detectar, responder e recuperar uma nova função denominada governar, voltada ao estabelecimento da estratégia, das responsabilidades e da supervisão do risco cibernético pela liderança (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2024). Na União Europeia, a Diretiva (UE) 2022/2555 passou a exigir que os órgãos de administração de entidades essenciais e importantes aprovem as medidas de gestão de riscos de cibersegurança, supervisionem sua implementação e frequentem formação específica (UNIÃO EUROPEIA, 2022). No Brasil, a Lei Geral de Proteção de Dados Pessoais impôs aos agentes de tratamento deveres de segurança, de comunicação de incidentes e de governança, com sanções que podem alcançar parcela relevante do faturamento (BRASIL, 2018).

Pequenas e médias empresas ocupam posição particular nesse cenário. Dispõem de menos recursos e de estruturas técnicas mais enxutas, mas tratam dados pessoais, dependem de fornecedores de tecnologia e estão sujeitas às mesmas ameaças que atingem grandes organizações. O objetivo deste artigo é examinar, à luz da literatura de administração, de governança e de compliance, os fundamentos teóricos que sustentam a atribuição da segurança cibernética à alta administração, com atenção especial às empresas de menor porte. Busca-se compreender por que o risco cibernético deve ser tratado como risco de negócio e quais mecanismos de governança, de due diligence de terceiros e de resposta a incidentes permitem ao dirigente exercer essa responsabilidade. Após a metodologia, seis seções desenvolvem o tema, seguidas das considerações finais.

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

2 METODOLOGIA

A pesquisa possui abordagem qualitativa e caráter teórico-conceitual, com objetivos exploratórios e descritivos. Conforme Gil (2017), a pesquisa exploratória permite ampliar a familiaridade com um problema e formular proposições a seu respeito, ao passo que a pesquisa descritiva se ocupa da caracterização de fenômenos e das relações entre eles. O fenômeno aqui examinado é o deslocamento da segurança cibernética do campo técnico para o campo da governança corporativa, e as relações analisadas envolvem esse deslocamento, as teorias organizacionais que o explicam e os instrumentos normativos que o materializam.

O procedimento central foi a revisão narrativa de literatura, com elementos de revisão integrativa. Snyder (2019) indica que essas modalidades são apropriadas quando se pretende acompanhar o desenvolvimento de um campo de pesquisa, articular contribuições de diferentes disciplinas e propor sínteses conceituais, sem a pretensão de agregar estatisticamente resultados empíricos. Torraco (2005) acrescenta que a revisão integrativa permite reunir e criticar a literatura representativa de um tema de modo a gerar novas perspectivas, característica pertinente a um objeto situado na interseção entre sistemas de informação, administração, economia e direito.

A seleção do corpus partiu de trabalhos amplamente reconhecidos sobre governança da segurança da informação, como os de Von Solms e Von Solms (2004) e Posthumus e Von Solms (2004), sobre economia da segurança, como os de Anderson (2001) e Gordon e Loeb (2002), e sobre comportamento de conformidade, como os de Bulgurcu, Cavusoglu e Benbasat (2010) e Siponen e Vance (2010). A partir dessas obras, procedeu-se ao rastreamento de estudos relacionados publicados em periódicos revisados por pares, como MIS Quarterly, Information Systems Research, Computers & Security e Journal of Information Systems. Os critérios de inclusão foram a pertinência direta ao tema, a relevância reconhecida na literatura e a possibilidade de verificação integral da fonte.

Em caráter complementar, realizou-se análise documental de normas técnicas, marcos de referência e legislação. Foram examinados a ABNT NBR ISO/IEC 27001:2022, a ABNT NBR ISO/IEC 27002:2022, a ISO/IEC 27014:2020, a ABNT NBR ISO 31000:2018, o NIST Cybersecurity Framework 2.0 e as publicações NIST SP 800-161 Rev. 1 e NIST SP 800-61 Rev. 3, além da Lei nº 13.709/2018, das resoluções da Autoridade Nacional de Proteção de Dados sobre agentes de pequeno porte e sobre comunicação de incidentes, da Lei nº 6.404/1976, do Código Civil, do Decreto nº 11.856/2023 e da Diretiva (UE) 2022/2555. Para a ilustração da dimensão econômica do problema, utilizaram-se dados publicados nos relatórios anuais Cost of a Data Breach, da IBM, e no Data Breach Investigations Report, da Verizon.

O material foi organizado por categorização temática em seis eixos, correspondentes às seções 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.

Ano VII, v.2 2026 | submissão: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

desenvolvimento do artigo. Reconhece-se como limitação a natureza exclusivamente teórica e documental da investigação, bem como o fato de que os relatórios setoriais utilizados se baseiam em amostras próprias, não necessariamente representativas das empresas brasileiras de pequeno porte. Por essa razão, os dados quantitativos são empregados apenas como ilustração da magnitude do fenômeno, e as proposições formuladas devem ser verificadas em pesquisas empíricas futuras.

3 DA SEGURANÇA DA INFORMAÇÃO À GOVERNANÇA CIBERNÉTICA

A literatura sobre segurança da informação percorreu um caminho que vai da preocupação técnica à preocupação organizacional. Dhillon e Backhouse (2001), ao revisarem as correntes de pesquisa então existentes, sustentaram que a abordagem predominante, centrada em controles técnicos e em modelos formais de acesso, era insuficiente para lidar com problemas que tinham origem nas estruturas sociais, nas normas e nas responsabilidades dentro das organizações. Os autores defendem uma perspectiva socioorganizacional, na qual a segurança é compreendida como resultado da interação entre pessoas, processos e tecnologia, e não apenas como propriedade de sistemas computacionais. Essa mudança de enfoque abriu espaço para que a gestão e, posteriormente, a governança passassem a ocupar o centro do debate.

Von Solms e Von Solms (2004) contribuíram para essa transição ao identificar dez erros recorrentes na gestão da segurança da informação, entre os quais a percepção de que a segurança é um problema exclusivamente técnico, a ausência de envolvimento da alta administração, a falta de políticas formais e a inexistência de mecanismos de acompanhamento e de conformidade. Os autores propuseram que esses elementos fossem utilizados pela gestão como lista de verificação para avaliar a completude de um plano de governança da segurança. Posthumus e Von Solms (2004), no mesmo ano, apresentaram um modelo de governança da segurança da informação que situa o tema no âmbito da governança corporativa, sob responsabilidade do conselho e da alta administração, e que integra às considerações técnicas as exigências de natureza empresarial, legal e regulatória.

Schneier (2000) sintetizou o espírito dessa evolução ao afirmar que a segurança é um processo, e não um produto. A aquisição de ferramentas tecnológicas, por mais sofisticadas que sejam, não substitui a definição de objetivos, a atribuição de responsabilidades, o monitoramento contínuo e a revisão periódica dos controles. Soomro, Shah e Ahmed (2016), em revisão de literatura sobre o papel da gestão na segurança da informação, concluíram que a literatura convergia para a necessidade de uma abordagem holística, na qual as atividades gerenciais, como desenvolvimento de políticas, alocação de recursos, conscientização e alinhamento com a estratégia, recebem a mesma atenção que os aspectos técnicos e passam a ser tratadas como parte da responsabilidade dos gestores.

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

Os referenciais normativos acompanharam esse movimento. A ISO/IEC 27014:2020 trata especificamente da governança da segurança da informação e estrutura a atuação do órgão de governança em processos de avaliação, direção, monitoramento e comunicação, distinguindo-os das atividades de gestão (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION, 2020). A ABNT NBR ISO/IEC 27001:2022, que estabelece os requisitos de um sistema de gestão da segurança da informação, exige que a alta direção demonstre liderança e comprometimento, assegurando que a política e os objetivos de segurança sejam compatíveis com a direção estratégica da organização e que os recursos necessários estejam disponíveis (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2022a). A inclusão da função governar no NIST Cybersecurity Framework 2.0 representa o ponto mais recente dessa trajetória. A função abrange o contexto organizacional, a estratégia de gestão de riscos, os papéis, responsabilidades e autoridades, a política, a supervisão e a gestão de riscos da cadeia de suprimentos cibernética, e é apresentada como elemento que informa a forma como a organização executa as demais funções (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2024). No Brasil, o Decreto nº 11.856/2023 instituiu a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança, sinalizando a incorporação do tema à agenda pública (BRASIL, 2023). O conjunto dessas referências indica que a segurança cibernética passou a ser compreendida como dimensão da governança corporativa, cuja direção cabe a quem responde pelo destino da organização.

4 A RESPONSABILIDADE DOS ADMINISTRADORES SOB AS TEORIAS DA AGÊNCIA E DOS ESCALÕES SUPERIORES

A teoria da agência oferece um primeiro fundamento para compreender por que a segurança cibernética não pode ser integralmente delegada. Jensen e Meckling (1976) definiram a relação de agência como aquela em que o principal delega ao agente a realização de atividades em seu nome, e demonstraram que a divergência de interesses e a assimetria de informações entre ambos geram custos de monitoramento, de garantia e de perda residual. Quando o proprietário ou o dirigente delega a segurança a uma equipe interna ou a um prestador externo, instaura-se exatamente esse tipo de relação. O agente detém informações técnicas que o principal não domina, e seus incentivos nem sempre coincidem com os da organização, pois o custo de uma falha recai sobretudo sobre a empresa e seus titulares de dados.

Eisenhardt (1989) argumentou que a eficiência dos contratos de agência depende, entre outros fatores, da existência de sistemas de informação capazes de tornar observável o comportamento do agente.

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

No campo da segurança cibernética, esses sistemas correspondem a indicadores de maturidade, relatórios periódicos, auditorias e testes de resposta a incidentes. Sem eles, o dirigente não tem como avaliar se a segurança delegada está sendo efetivamente exercida, e a ausência de incidentes aparentes pode ser confundida com proteção adequada. A literatura de agência sugere, portanto, que o envolvimento da alta administração não substitui a competência técnica, mas é condição para que a delegação seja controlada e para que os custos de agência permaneçam em nível aceitável.

A teoria dos escalões superiores, formulada por Hambrick e Mason (1984), acrescenta uma segunda perspectiva ao sustentar que os resultados organizacionais refletem, em parte, as características, as experiências e os valores dos membros da alta administração. Estudos empíricos aplicaram essa teoria à segurança cibernética. Kwon et al. (2013) examinaram a associação entre o envolvimento de executivos de tecnologia na alta gestão, a estrutura de sua remuneração e a ocorrência de violações de segurança da informação. Haislip, Lim e Pinsker (2021), com base em violações reportadas entre 2005 e 2017, verificaram que diretores-presidentes com conhecimento em tecnologia da informação e a presença do principal executivo de tecnologia na equipe de alta gestão estavam associados a menor ocorrência de violações, concluindo que o risco é responsabilidade compartilhada da cúpula.

O ordenamento jurídico brasileiro oferece um terceiro fundamento, de natureza normativa. A Lei nº 6.404/1976, em seu art. 153, determina que o administrador da companhia empregue, no exercício de suas funções, o cuidado e a diligência que todo homem ativo e probo costuma empregar na administração de seus próprios negócios, e o art. 158 trata de sua responsabilidade pelos prejuízos causados quando proceder com culpa ou dolo ou com violação da lei ou do estatuto (BRASIL, 1976). O art. 1.011 do Código Civil reproduz o dever de cuidado e diligência para os administradores das sociedades em geral (BRASIL, 2002). Em um ambiente em que a dependência de sistemas e dados é intensa e as ameaças são amplamente conhecidas, a omissão diante do risco cibernético dificilmente se compatibiliza com esse padrão de conduta.

A LGPD reforça essa leitura ao exigir que os agentes de tratamento adotem medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas, nos termos do art. 46, e ao prever, no art. 50, a possibilidade de formulação de regras de boas práticas e de governança (BRASIL, 2018). Entre as sanções administrativas previstas no art. 52, figura a multa simples de até dois por cento do faturamento da pessoa jurídica no Brasil no último exercício, limitada a cinquenta milhões de reais por infração, cuja aplicação foi disciplinada pelo regulamento de dosimetria da Autoridade Nacional de Proteção de Dados (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2023). A combinação entre dever de diligência, exigências regulatórias e evidências empíricas sustenta a conclusão de que a segurança cibernética integra o núcleo das responsabilidades do dirigente.

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

5 A ECONOMIA DA SEGURANÇA E A MENSURAÇÃO DO RISCO CIBERNÉTICO

A economia da segurança da informação consolidou-se como campo de pesquisa a partir da constatação de que muitas falhas de segurança decorrem de incentivos mal alinhados, e não de deficiências tecnológicas. Anderson (2001) argumentou que sistemas frequentemente falham porque as pessoas que poderiam protegê-los não são as que arcam com as consequências de sua falha, fenômeno que aproxima a segurança dos problemas clássicos de externalidades e de risco moral. Anderson e Moore (2006), em artigo publicado na revista Science, ampliaram essa análise e mostraram que conceitos como externalidades de rede, assimetria de informação e seleção adversa explicam parte relevante das dificuldades enfrentadas por organizações e mercados na proteção de seus sistemas.

Gordon e Loeb (2002) propuseram um modelo econômico para a definição do nível ótimo de investimento em segurança da informação. Partindo da relação entre a vulnerabilidade da informação, a probabilidade de ocorrência de violações e a perda potencial, os autores demonstraram que, para determinadas classes de funções de probabilidade, o investimento ótimo não ultrapassa cerca de 37 por cento, ou um sobre o número de Euler, da perda esperada. Mais do que o valor numérico, cuja generalidade foi discutida por estudos posteriores, a contribuição do modelo está em demonstrar que o investimento em segurança deve ser decidido com base no valor da informação protegida e na redução de risco obtida, o que é, por definição, uma decisão de gestão.

A mensuração do risco cibernético em termos financeiros é condição para que essa decisão seja tomada com fundamento. Freund e Jones (2015) apresentaram o modelo Factor Analysis of Information Risk, que decompõe o risco em frequência de eventos de perda e magnitude das perdas, permitindo expressá-lo em valores monetários comparáveis aos demais riscos da organização. Hubbard e Seiersen (2016) criticaram o uso disseminado de matrizes qualitativas, que classificam riscos como baixos, médios ou altos, e defenderam métodos quantitativos que permitam comparar alternativas de investimento. Essas propostas dialogam com a ABNT NBR ISO 31000:2018, que recomenda que a análise de riscos considere a probabilidade dos eventos e a magnitude de suas consequências (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018).

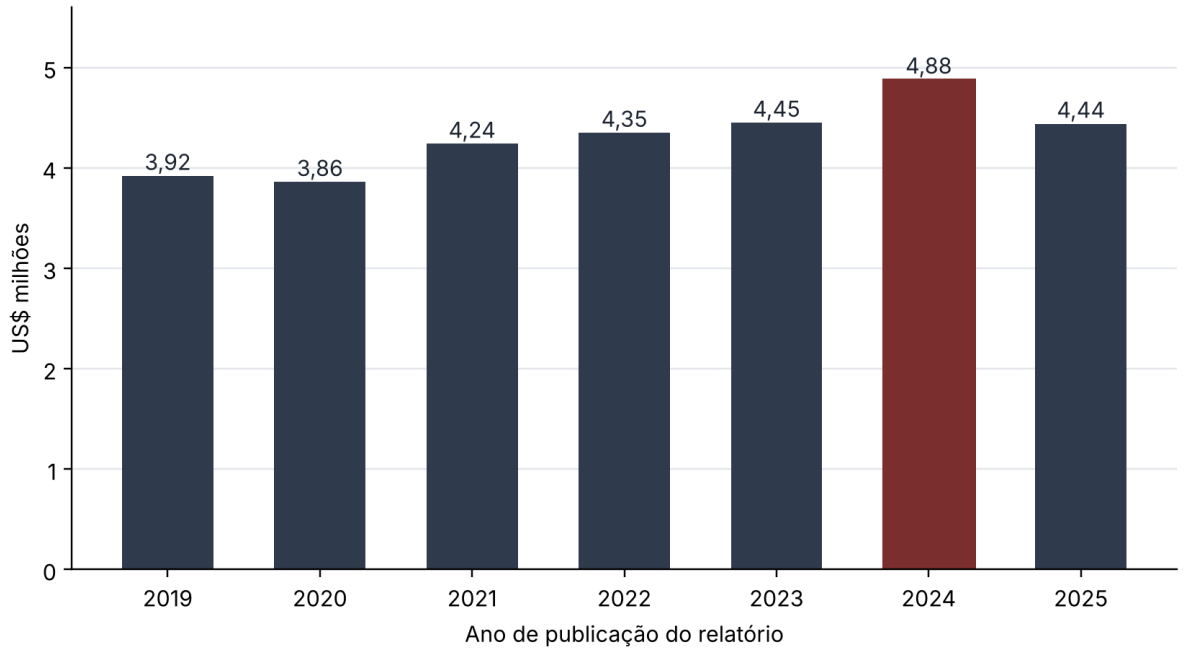
Os efeitos econômicos das violações foram documentados por estudos de eventos e por levantamentos setoriais. Cavusoglu, Mishra e Raghunathan (2004) verificaram que as empresas que anunciaram violações de segurança perderam, em média, 2,1 por cento de seu valor de mercado nos dois dias seguintes ao anúncio. Os relatórios anuais da IBM, conduzidos com o Ponemon Institute, estimam o custo médio global de uma violação de dados e permitem acompanhar sua evolução, conforme

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

apresenta a Figura 1. O valor médio passou de 3,92 milhões de dólares no relatório de 2019 para 4,88 milhões no relatório de 2024, o maior da série, e recuou para 4,44 milhões no relatório de 2025, redução atribuída à maior rapidez na identificação e na contenção dos incidentes (IBM, 2019; 2024; 2025).

Figura 1 – Custo médio global de uma violação de dados por ano de publicação do relatório (US$ milhões)



Fonte: elaborada pelo autor com dados de IBM (2019; 2020; 2021; 2022; 2023; 2024; 2025).

Para o contexto brasileiro, o relatório de 2025 estimou o custo médio de uma violação em 7,19 milhões de reais, ante 6,75 milhões no ano anterior (IBM, 2025). Esses valores derivam de amostras próprias da pesquisa, compostas por organizações de diferentes portes e setores, e não devem ser transpostos diretamente para pequenas empresas, mas indicam a ordem de grandeza das perdas envolvidas, que abrangem detecção, contenção, notificação, perda de negócios e resposta pós-incidente. A redução observada em 2025, associada pela própria pesquisa à melhoria da capacidade de detecção e contenção, sugere que decisões de gestão sobre preparação e resposta afetam diretamente o custo final dos incidentes, o que reforça o argumento de que o tema deve ser tratado como questão econômica e estratégica, e não apenas operacional.

6 O FATOR HUMANO E A CULTURA DE CONFORMIDADE

A dimensão humana ocupa posição central na segurança cibernética. O Data Breach Investigations

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

Report de 2024, elaborado pela Verizon a partir da análise de milhares de incidentes e violações confirmadas, indicou que 68 por cento das violações envolveram um elemento humano não malicioso, como erros ou a manipulação por engenharia social, e que 32 por cento envolveram alguma técnica de extorsão, incluindo ransomware (VERIZON, 2024). Esses dados reforçam a percepção de que controles tecnológicos, embora indispensáveis, são insuficientes quando as pessoas que operam os sistemas desconhecem os riscos ou não se sentem responsáveis por evitá-los. Para o dirigente, o dado indica que o investimento em pessoas e em processos é tão relevante quanto o investimento em tecnologia, e que a exposição da empresa depende diretamente das condições de trabalho e de informação oferecidas aos seus colaboradores.

A pesquisa em sistemas de informação dedicou atenção extensa aos fatores que explicam o cumprimento das políticas de segurança pelos empregados. Bulgurcu, Cavusoglu e Benbasat (2010) demonstraram que a intenção de cumprir essas políticas é influenciada pela atitude do empregado, pelas crenças normativas e pela autoeficácia, e que a atitude, por sua vez, é moldada por crenças sobre os benefícios e os custos do cumprimento e do descumprimento, sobre as quais a conscientização em segurança da informação exerce influência relevante. Herath e Rao (2009) verificaram que pressões sociais, a certeza de detecção e a percepção de que o próprio comportamento contribui para a segurança estão associadas a intenções mais favoráveis ao cumprimento das políticas, enquanto a severidade das punições apresentou, de forma contrária ao esperado pelas abordagens puramente dissuasórias, efeito negativo sobre essas intenções.

A abordagem baseada em dissuasão recebeu atenção específica. D'Arcy, Hovav e Galletta (2009) constataram que o conhecimento, pelos usuários, da existência de políticas de segurança, de programas de conscientização e de monitoramento de computadores está associado à percepção de severidade das sanções e, por meio dela, à redução da intenção de uso indevido dos sistemas. Siponen e Vance (2010), por sua vez, mostraram que empregados recorrem a técnicas de neutralização, como a negação de dano ou a invocação de lealdades superiores, para justificar violações das políticas, e que essas racionalizações podem reduzir o efeito das sanções. A combinação desses resultados indica que normas e punições produzem efeito limitado se não forem acompanhadas de explicação clara sobre os motivos dos controles.

A teoria dos acidentes organizacionais de Reason (1997) oferece uma moldura útil para interpretar esses achados. O autor distinguiu as falhas ativas, cometidas por quem está na linha de frente, das condições latentes, criadas por decisões de projeto, de gestão e de alocação de recursos, que permanecem adormecidas no sistema até que se combinem com falhas ativas para produzir um acidente. Aplicada à segurança cibernética, essa distinção sugere que o clique de um empregado em uma mensagem fraudulenta é, com frequência, apenas a falha ativa que revela condições latentes

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

anteriores, como ausência de treinamento, permissões excessivas, falta de autenticação multifator ou inexistência de procedimentos para verificar solicitações incomuns de pagamento.

Para a alta administração, a principal implicação é que a cultura de segurança é produto de escolhas gerenciais. A ABNT NBR ISO/IEC 27002:2022 inclui, entre os controles relativos a pessoas, a conscientização, a educação e o treinamento em segurança da informação, os termos e condições de contratação e o processo disciplinar (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2022b). A Diretiva (UE) 2022/2555 vai além e exige que os próprios membros dos órgãos de administração recebam formação, além de incentivar que treinamento semelhante seja oferecido regularmente aos empregados (UNIÃO EUROPEIA, 2022). O exemplo da liderança, a coerência entre discurso e alocação de recursos e a disposição de ouvir e corrigir falhas sem buscar culpados individuais são elementos que a literatura associa à formação de uma cultura de conformidade efetiva.

7 TERCEIROS, CADEIA DE SUPRIMENTOS E DUE DILIGENCE CIBERNÉTICA

A dependência de fornecedores de tecnologia tornou-se característica estrutural das empresas contemporâneas, sobretudo das de menor porte, que recorrem a serviços em nuvem, sistemas de gestão contratados como serviço, provedores de pagamento e prestadores de suporte técnico. Cada uma dessas relações amplia a superfície de ataque da organização. O Data Breach Investigations Report de 2024 registrou que 15 por cento das violações analisadas envolveram um terceiro, como custodiantes de dados ou fornecedores de software, o que representou aumento de 68 por cento em relação ao período anterior (VERIZON, 2024). A segurança da empresa passa a depender, em medida considerável, das práticas de quem ela contrata, o que transforma a escolha e o acompanhamento de fornecedores em decisão de gestão de riscos.

A economia dos custos de transação ajuda a compreender por que essa dependência exige governança específica. Williamson (1985) demonstrou que transações caracterizadas por ativos específicos, incerteza e racionalidade limitada das partes demandam estruturas de governança mais elaboradas do que a simples troca de mercado. Contratos de tecnologia apresentam essas características com intensidade, pois envolvem dados da empresa armazenados em sistemas de terceiros, integrações difíceis de substituir e informações técnicas que o contratante raramente consegue avaliar. A assimetria informacional, nesse contexto, favorece a seleção de fornecedores com práticas deficientes, pois a qualidade da segurança oferecida não é diretamente observável no momento da contratação.

A due diligence cibernética de fornecedores é a resposta organizacional a esse problema. A ABNT NBR ISO/IEC 27002:2022 dedica um conjunto de controles às relações com fornecedores, que

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

abrange a segurança da informação nessas relações, o tratamento da segurança nos acordos com fornecedores, a gestão da segurança na cadeia de suprimentos de tecnologia da informação e comunicação, o monitoramento e a gestão de mudanças nos serviços prestados e a segurança no uso de serviços em nuvem (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2022b). A publicação NIST SP 800-161 Rev. 1 detalha práticas de gestão de riscos da cadeia de suprimentos cibernética e recomenda que a profundidade das avaliações seja proporcional à criticidade do fornecedor e do serviço prestado (BOYENS et al., 2022).

A LGPD confere a essa diligência uma dimensão jurídica direta. O art. 39 determina que o operador realize o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria, e o art. 42 estabelece hipóteses de responsabilidade solidária entre controladores e operadores pelos danos causados em razão do tratamento de dados pessoais (BRASIL, 2018). Na prática, a empresa que contrata um sistema de gestão, um serviço de armazenamento ou um prestador de atendimento continua a responder pelos dados de seus clientes, o que torna indispensável conhecer as práticas do fornecedor e estabelecer, em contrato, obrigações claras de segurança, confidencialidade, comunicação de incidentes, auditoria e devolução ou eliminação de dados ao término da relação.

Para pequenas e médias empresas, a aplicação desses referenciais requer proporcionalidade. Não é viável submeter todos os fornecedores a avaliações exaustivas, mas é possível classificá-los segundo o acesso que têm a dados pessoais e a sistemas críticos e concentrar a diligência nos casos de maior risco. Questionários padronizados, verificação de certificações reconhecidas, cláusulas contratuais de segurança, previsão de prazos para comunicação de incidentes e reavaliações periódicas compõem um conjunto acessível de medidas. O NIST Cybersecurity Framework 2.0, ao inserir a gestão de riscos da cadeia de suprimentos na função governar, sinaliza que a escolha e a supervisão de parceiros tecnológicos são decisões que pertencem à liderança, e não apenas à área de compras ou de tecnologia (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 2024).

8 RESPOSTA A INCIDENTES, RESILIÊNCIA ORGANIZACIONAL E DEVERES REGULATÓRIOS

A literatura e os referenciais técnicos partem da premissa de que nenhuma organização está imune a incidentes, o que desloca parte da atenção da prevenção para a capacidade de resposta. A publicação NIST SP 800-61 Rev. 3, de 2025, reorganizou as recomendações sobre resposta a incidentes à luz do Cybersecurity Framework 2.0 e passou a tratá-la como parte integrante da gestão de riscos cibernéticos, associando as atividades de preparação, detecção, resposta e recuperação às funções

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

desse referencial, inclusive à função governar, e não como atividade isolada da área técnica (NELSON et al., 2025). Essa integração implica que decisões sobre papéis, comunicação, recursos e prioridades de recuperação sejam tomadas antes do incidente e com participação da liderança, que responderá pelas consequências operacionais, financeiras e reputacionais do evento.

A teoria das organizações de alta confiabilidade oferece fundamentos para essa preparação. Weick e Sutcliffe (2007) identificaram cinco princípios presentes em organizações que operam em ambientes de alto risco com baixa incidência de falhas graves, a preocupação com falhas, a relutância em simplificar interpretações, a sensibilidade às operações, o compromisso com a resiliência e a deferência à competência técnica. Os autores sustentaram que essas organizações tratam pequenos desvios como sinais de problemas maiores, evitam explicações simplistas e preparam-se para conter e recuperar-se de eventos inesperados. Transpostos para a segurança cibernética, esses princípios sugerem o registro e a análise de quase incidentes, a realização de exercícios simulados e a definição prévia de quem tem autoridade para decidir em situação de crise.

Os deveres regulatórios conferem urgência a essa preparação. O art. 48 da LGPD 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 (BRASIL, 2018). A Resolução CD/ANPD nº 15/2024 regulamentou esse dever e estabeleceu que a comunicação seja realizada em até três dias úteis, contados do conhecimento, pelo controlador, de que o incidente afetou dados pessoais, além de definir critérios para caracterizar o risco ou dano relevante, como o envolvimento de dados sensíveis, de dados de crianças, adolescentes ou idosos, de dados financeiros, de dados de autenticação ou de dados em larga escala (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2024). O cumprimento desse prazo é dificilmente alcançável sem procedimentos previamente definidos.

A regulação brasileira reconhece, contudo, as particularidades das empresas de menor porte. A Resolução CD/ANPD nº 2/2022 estabeleceu tratamento diferenciado e simplificado para agentes de tratamento de pequeno porte, com flexibilização de algumas obrigações e de prazos (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2022), e a Resolução CD/ANPD nº 15/2024 determinou que os prazos de comunicação de incidentes sejam contados em dobro para esses agentes (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2024). A própria autoridade publicou guia orientativo de segurança da informação dirigido a esses agentes, com recomendações de medidas administrativas e técnicas, como a adoção de política de segurança da informação, a conscientização e o treinamento dos funcionários, a gestão de contratos, o controle de acesso, a proteção dos dados armazenados e o gerenciamento de vulnerabilidades (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2021). A flexibilização, porém, não elimina o dever de segurança, apenas adequa sua

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

forma de cumprimento ao porte da organização.

A resiliência, nesse quadro, é tanto uma capacidade técnica quanto um atributo de governança. A ABNT NBR ISO 31000:2018 estabelece que a gestão de riscos deve ser integrada a todas as atividades organizacionais e que a alta direção é responsável por assegurar essa integração (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2018). A recuperação após um incidente depende de decisões anteriores sobre cópias de segurança, contratos com fornecedores, comunicação com clientes e alocação de recursos, todas situadas no campo da direção da empresa. Os dados da IBM (2025) associaram a redução do custo médio das violações à identificação e à contenção mais rápidas, o que confirma que a preparação para responder constitui investimento com retorno mensurável e reforça a responsabilidade da liderança por sua existência.

CONSIDERAÇÕES FINAIS

Este artigo examinou os fundamentos teóricos e normativos que sustentam a atribuição da segurança cibernética à alta administração, com atenção às pequenas e médias empresas. A revisão demonstrou que o tema percorreu, na literatura e nos referenciais técnicos, um caminho que parte do controle técnico, passa pela gestão e chega à governança, refletindo a crescente dependência das organizações em relação a dados e sistemas digitais e a consequente elevação do risco cibernético à condição de risco estratégico, com efeitos sobre a continuidade, a reputação e o resultado financeiro das empresas.

A evolução do campo mostrou que a segurança da informação deixou de ser compreendida como propriedade de sistemas e passou a ser vista como resultado da interação entre pessoas, processos e tecnologia. A inclusão da função governar no NIST Cybersecurity Framework 2.0 e as exigências de liderança da ISO/IEC 27001 consolidam a compreensão de que a direção estratégica da segurança cabe aos dirigentes, cabendo às equipes técnicas a execução dos controles definidos a partir dessa direção.

A teoria da agência explicou por que a delegação da segurança, sem mecanismos de informação e de controle, gera custos e expõe a organização a riscos que o dirigente não consegue observar. A teoria dos escalões superiores e os estudos empíricos que a aplicaram indicaram que a composição e o conhecimento da alta administração estão associados à ocorrência de violações, o que reforça a responsabilidade compartilhada da cúpula e afasta a ideia de que o tema possa ser confiado a um único profissional ou a um fornecedor externo sem supervisão.

No plano jurídico, o dever de diligência previsto na Lei das Sociedades por Ações e no Código Civil, somado às obrigações de segurança e de governança da LGPD, oferece base normativa para afirmar que a omissão diante do risco cibernético é incompatível com o padrão de conduta exigido dos

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

administradores. As sanções previstas na legislação e a regulamentação da autoridade nacional conferem concretude a esse dever, aproximando a segurança cibernética das demais obrigações de conformidade que já integram a rotina de qualquer administrador.

A economia da segurança demonstrou que o investimento em proteção deve ser decidido com base no valor da informação e na redução de risco obtida, decisão de natureza gerencial. Os dados sobre o custo das violações, ainda que derivados de amostras que não representam especificamente as pequenas empresas brasileiras, evidenciam a magnitude das perdas e mostram que a capacidade de detecção e contenção influencia diretamente o resultado financeiro, de modo que a preparação para responder a incidentes deve ser compreendida como investimento, e não como despesa acessória.

A análise do fator humano revelou que a maior parte das violações envolve erros, manipulação ou condições organizacionais que os favorecem. A conscientização, a coerência entre discurso e prática e a correção das condições latentes criadas por decisões de gestão aparecem como elementos centrais de uma cultura de conformidade capaz de reduzir a exposição da organização. Essa cultura não surge de forma espontânea, pois depende de decisões gerenciais sobre treinamento, comunicação interna e alocação de recursos.

A dependência de fornecedores de tecnologia ampliou o perímetro de risco das empresas e tornou a due diligence cibernética parte indispensável da governança. A responsabilidade do controlador pelos dados tratados por terceiros, prevista na LGPD, exige seleção criteriosa, cláusulas contratuais adequadas e supervisão proporcional à criticidade de cada relação. Em empresas de menor porte, nas quais os serviços tecnológicos são majoritariamente contratados, essa diligência representa parcela expressiva da própria gestão da segurança.

Como contribuição, o estudo propõe que pequenas e médias empresas tratem a segurança cibernética como risco de negócio, sob responsabilidade direta de seus dirigentes, apoiada em medidas proporcionais ao porte, como definição de responsáveis, classificação de fornecedores, treinamento, cópias de segurança e plano de resposta a incidentes. Recomenda-se que pesquisas futuras investiguem empiricamente o nível de envolvimento dos dirigentes de empresas brasileiras de menor porte com o tema e seus efeitos sobre a ocorrência e o custo de incidentes.

REFERÊNCIAS

ANDERSON, R. Why information security is hard: an economic perspective. In: ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, 17., 2001, New Orleans. **Proceedings** [...]. Los Alamitos: IEEE Computer Society, 2001. p. 358-365.

ANDERSON, R.; MOORE, T. The economics of information security. **Science**, v. 314, n. 5799, p. 610-613, 2006.

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO 31000**: gestão de riscos: diretrizes. Rio de Janeiro: ABNT, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001**: segurança da informação, segurança cibernética e proteção à privacidade: sistemas de gestão da segurança da informação: requisitos. Rio de Janeiro: ABNT, 2022a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002**: segurança da informação, segurança cibernética e proteção à privacidade: controles de segurança da informação. Rio de Janeiro: ABNT, 2022b.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia orientativo**: segurança da informação para agentes de tratamento de pequeno porte. Brasília, DF: ANPD, 2021.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. **Diário Oficial da União**, Brasília, DF, 28 jan. 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. **Diário Oficial da União**, Brasília, DF, 27 fev. 2023.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Resolução CD/ANPD nº 15, de 24 de abril de 2024. Aprova o Regulamento de Comunicação de Incidente de Segurança. **Diário Oficial da União**, Brasília, DF, 26 abr. 2024.

BOYENS, J. et al. **Cybersecurity supply chain risk management practices for systems and organizations**. Gaithersburg: National Institute of Standards and Technology, 2022. (NIST Special Publication 800-161 Rev. 1).

BRASIL. Lei nº 6.404, de 15 de dezembro de 1976. Dispõe sobre as Sociedades por Ações. **Diário Oficial da União**, Brasília, DF, 17 dez. 1976.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**, Brasília, DF, 11 jan. 2002.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União**, Brasília, DF, 15 ago. 2018.

BRASIL. Decreto nº 11.856, de 26 de dezembro de 2023. Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. **Diário Oficial da União**, Brasília, DF, 27 dez. 2023.

BULGURCU, B.; CAVUSOGLU, H.; BENBASAT, I. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. **MIS Quarterly**, v. 34, n. 3, p. 523-548, 2010.

CAVUSOGLU, H.; MISHRA, B.; RAGHUNATHAN, S. The effect of internet security breach

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

announcements on market value: capital market reactions for breached firms and internet security developers. **International Journal of Electronic Commerce**, v. 9, n. 1, p. 69-104, 2004.

D'ARCY, J.; HOVAV, A.; GALLETTA, D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. **Information Systems Research**, v. 20, n. 1, p. 79-98, 2009.

DHILLON, G.; BACKHOUSE, J. Current directions in IS security research: towards socio-organizational perspectives. **Information Systems Journal**, v. 11, n. 2, p. 127-153, 2001.

EISENHARDT, K. M. Agency theory: an assessment and review. **Academy of Management Review**, v. 14, n. 1, p. 57-74, 1989.

FREUND, J.; JONES, J. **Measuring and managing information risk**: a FAIR approach. Oxford: Butterworth-Heinemann, 2015.

GIL, A. C. **Como elaborar projetos de pesquisa**. 6. ed. São Paulo: Atlas, 2017.

GORDON, L. A.; LOEB, M. P. The economics of information security investment. **ACM Transactions on Information and System Security**, v. 5, n. 4, p. 438-457, 2002.

HAISLIP, J.; LIM, J.-H.; PINSKER, R. The impact of executives' IT expertise on reported data security breaches. **Information Systems Research**, v. 32, n. 2, p. 318-334, 2021.

HAMBRICK, D. C.; MASON, P. A. Upper echelons: the organization as a reflection of its top managers. **Academy of Management Review**, v. 9, n. 2, p. 193-206, 1984.

HERATH, T.; RAO, H. R. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. **Decision Support Systems**, v. 47, n. 2, p. 154-165, 2009.

HUBBARD, D. W.; SEIERSEN, R. **How to measure anything in cybersecurity risk**. Hoboken: Wiley, 2016.

IBM. **Cost of a data breach report 2019**. Armonk: IBM Security, 2019.

IBM. **Cost of a data breach report 2020**. Armonk: IBM Security, 2020.

IBM. **Cost of a data breach report 2021**. Armonk: IBM Security, 2021.

IBM. **Cost of a data breach report 2022**. Armonk: IBM Security, 2022.

IBM. **Cost of a data breach report 2023**. Armonk: IBM Security, 2023.

IBM. **Cost of a data breach report 2024**. Armonk: IBM Security, 2024.

IBM. **Cost of a data breach report 2025**: the AI oversight gap. Armonk: IBM Security, 2025.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION; INTERNATIONAL ELECTROTECHNICAL COMMISSION. **ISO/IEC 27014**: information security, cybersecurity and

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

privacy protection: governance of information security. Geneva: ISO, 2020.

JENSEN, M. C.; MECKLING, W. H. Theory of the firm: managerial behavior, agency costs and ownership structure. **Journal of Financial Economics**, v. 3, n. 4, p. 305-360, 1976.

KWON, J. et al. The association between top management involvement and compensation and information security breaches. **Journal of Information Systems**, v. 27, n. 1, p. 219-236, 2013.

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

NELSON, A. et al. **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).

POSTHUMUS, S.; VON SOLMS, R. A framework for the governance of information security. **Computers & Security**, v. 23, n. 8, p. 638-646, 2004.

REASON, J. **Managing the risks of organizational accidents**. Aldershot: Ashgate, 1997.

SCHNEIER, B. **Secrets and lies**: digital security in a networked world. New York: John Wiley & Sons, 2000.

SIPONEN, M.; VANCE, A. Neutralization: new insights into the problem of employee information systems security policy violations. **MIS Quarterly**, v. 34, n. 3, p. 487-502, 2010.

SNYDER, H. Literature review as a research methodology: an overview and guidelines. **Journal of Business Research**, v. 104, p. 333-339, 2019.

SOOMRO, Z. A.; SHAH, M. H.; AHMED, J. Information security management needs more holistic approach: a literature review. **International Journal of Information Management**, v. 36, n. 2, p. 215-225, 2016.

TORRACO, R. J. Writing integrative literature reviews: guidelines and examples. **Human Resource Development Review**, v. 4, n. 3, p. 356-367, 2005.

UNIÃO EUROPEIA. Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União (Diretiva SRI 2). **Jornal Oficial da União Europeia**, Luxemburgo, L 333, p. 80-152, 27 dez. 2022.

VERIZON. **2024 data breach investigations report**. Basking Ridge: Verizon Business, 2024.

VON SOLMS, B.; VON SOLMS, R. The 10 deadly sins of information security management. **Computers & Security**, v. 23, n. 5, p. 371-376, 2004.

VON SOLMS, R.; VAN NIEKERK, J. From information security to cyber security. **Computers & Security**, v. 38, p. 97-102, 2013.

WEICK, K. E.; SUTCLIFFE, K. M. **Managing the unexpected**: resilient performance in an age of

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: 14/08/2026 | aceito: 10/09/2026 | publicação: 24/10/2026

uncertainty. 2. ed. San Francisco: Jossey-Bass, 2007.

WILLIAMSON, O. E. **The economic institutions of capitalism**: firms, markets, relational contracting. New York: Free Press, 1985.

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.