1ª Edição

QUANDO A SEGURANÇA VIRA ESTRATÉGIA

Responsabilidade, Governança e Assunção de risco nas Organizações Modernas

LUIZ PAIVA
Executivo Sênior • Cibersegurança & Estratégia Corporativa

QUANDO A SEGURANÇA VIRA ESTRATÉGIA

Responsabilidade, governança e assunção de risco nas organizações modernas

1ª Edição

Autor

Luiz Paiva

DOI: 10.47538/AC-2026.35

ISBN: 978-6-55321-115-5

9 786553 211155

Ano 2026

QUANDO A SEGURANÇA VIRA ESTRATÉGIA

Responsabilidade, governança e assunção de risco nas organizações modernas

1ª Edição

CIP-BRASIL. CATALOGAÇÃO NA PUBLICAÇÃO
SINDICATO NACIONAL DOS EDITORES DE LIVROS, RJ

P169q

Paiva, Luiz Henrique de Paula
Quando a segurança vira estratégia [recurso eletrônico] : Responsabilidade, governança e assunção de risco nas organizações modernas / Luiz Henrique de Paula Paiva. - 1. ed. - Natal [RN] : Amplamente, 2026.
recurso digital

Formato: ebook
Modo de acesso: world wide web
Inclui bibliografia
ISBN 978-65-5321-115-5 (recuso eletrônico)
DOI 10.47538/AC-2026.35

1. Administração de empresas. 2. Comportamento organizacional. 3. Sistemas de segurança. 3. Livros eletrônicos.

26-104516.0

CDD: 658.4
CDU: 005.4

Carla Rosa Martins Gonçalves - Bibliotecária - CRB-7/4782

Editora Amplamente
Empresarial Amplamente Ltda.
CNPJ: 35.719.570/0001-10
publicacoes@editoraamplamente.com.br
www.editoraamplamente.com
Telefone: (84) 999707-2900
Caixa Postal: 3402
CEP: 59082-971
Natal - Rio Grande do Norte – Brasil

Editora-Chefe: Dayana Lúcia R. de Freitas
Assistentes Editoriais: Caroline Rodrigues de F. Fernandes; Margarete Freitas Baptista
Bibliotecária: Carla Rosa Martins Gonçalves CRB-7/4782
Projeto Gráfico, Edição de Arte e Diagramação: Luciano Luan Gomes Paiva; Caroline Rodrigues de F. Fernandes
Capa: Canva®/Freepik®
Parecer e Revisão por pares: Revisores CONSULTORIA TÉCNICA E REVISÃO CRÍTICA: Rita de Cássia Soares Duque

Ano 2026

SUMÁRIO

SOBRE O AUTOR

Luiz Henrique de Paula Paiva é um executivo sênior com mais de duas décadas de experiência liderando iniciativas estratégicas diretas em tecnologia, cibersegurança e infraestrutura em ambientes corporativos de alta complexidade.

Ao longo de sua trajetória, construiu uma carreira marcada pela interseção entre visão estratégica e excelência técnica, atuando diretamente na proteção de ativos críticos, na mitigação de riscos corporativos e no desenvolvimento de operações resilientes em grandes organizações. Sua experiência abrange desde a arquitetura de soluções executivas até a liderança de áreas comerciais e de pré-vendas, consolidando uma visão integrada entre tecnologia, negócios e geração de valor.

Com atuação relevante no desenvolvimento de negócios de alto impacto, estabeleceu e fortaleceu parcerias com alguns dos principais fabricantes globais de tecnologia, especialmente nos Estados Unidos e em Israel, mercados reconhecidos por sua liderança em inovação e segurança digital.

Reconhecido por sua alta capacidade de liderar equipes de alta performance, Luiz Paiva combina disciplina operacional, pensamento estratégico e foco em resultados para conduzir projetos complexos em escala nacional. Sua experiência também se estende à formação e capacitação de profissionais, contribuindo ativamente para o desenvolvimento de competências técnicas e estratégicas no setor.

Sua atuação é pautada por rigor, consistência e visão de longo prazo, atributos essenciais para organizações que compreendem a segurança não apenas como proteção, mas como um pilar estratégico para crescimento, reputação e sustentabilidade dos negócios. Possui cases de sucesso compartilhados em artigos,

publicações, palestras e treinamentos e atua de forma direta com gestão e resultados consolidados a longo prazo.

AGRADECIMENTOS

Este livro é resultado de uma trajetória construída ao longo de muitos anos, marcada por desafios, aprendizados e conquistas que jamais seriam possíveis de forma isolada.

Em primeiro lugar, meu mais profundo agradecimento à minha família, base de tudo. Pelo apoio incondicional, pela compreensão e total suporte nos momentos de ausência e, principalmente, por serem meu maior alicerce em todas as fases dessa jornada. São vocês que dão sentido a cada conquista.

Estendo também meu reconhecimento a todos os profissionais com quem tive a oportunidade de trabalhar ao longo da minha carreira. Equipes técnicas, comerciais e estratégicas incluindo grandes executivos, conselhos, que, com competência e comprometimento, contribuíram diretamente para a construção de resultados relevantes e para a evolução contínua dos projetos que lideramos juntos.

Aos grandes executivos com quem compartilhei experiências, decisões e aprendizados, deixo minha admiração e respeito. As trocas em ambientes de alta exigência foram fundamentais para o amadurecimento da minha visão sobre negócios, liderança, risco e estratégia.

Registro ainda meu agradecimento às grandes empresas onde atuei e às organizações parceiras que confiaram e confiam no meu trabalho. Cada projeto, cada desafio e cada entrega foram determinantes para a consolidação da minha trajetória profissional e para a construção do conhecimento que sustenta este livro.

Por fim, agradeço a todos que, direta ou indiretamente, fizeram parte dessa caminhada. Este conteúdo é, acima de tudo, um reflexo das conexões, das experiências e das relações construídas ao longo do tempo.

APRESENTAÇÃO

Nas últimas décadas, as organizações atravessaram uma transformação estrutural profunda. A digitalização dos negócios, a ampliação da conectividade e a crescente dependência de sistemas complexos reposicionaram o risco como elemento central das decisões corporativas. Nesse contexto, a segurança deixa de ser um tema técnico e passa a ocupar um espaço inevitavelmente estratégico.

Ainda assim, em muitas organizações, persiste uma abordagem fragmentada. A segurança é frequentemente tratada como um conjunto de controles, ferramentas ou responsabilidades isoladas, dissociada da governança, da tomada de decisão e da própria estrutura de poder corporativo. O resultado é um desalinhamento crítico: reconhecem-se vulnerabilidades, mas não se constrói, de forma consistente, a capacidade institucional de interpretá-las, priorizá-las e responder a elas com coerência estratégica.

É nesse ponto essencial que esta obra se posiciona.

Mais do que discutir práticas ou tecnologias, este livro propõe uma mudança de perspectiva. A segurança é apresentada como um elemento estruturante da organização diretamente vinculada à forma como responsabilidades são distribuídas, como decisões são tomadas e como o risco é compreendido e assumido em ambientes de incerteza.

A partir dessa premissa, o autor introduz o Método RGA, uma estrutura analítica que integra responsabilidade, governança e assunção de risco em uma lógica única e aplicável. Ao fazer isso, oferece ao leitor uma forma mais clara e consistente de transformar exposições difusas em direcionamento estratégico, fortalecendo a capacidade organizacional de resposta em cenários complexos.

Esta não é uma obra destinada exclusivamente a especialistas técnicos. É um livro voltado a executivos, líderes e tomadores de decisão que compreendem que o risco já não pode ser tratado de forma periférica. Ao contrário, ele deve ser incorporado ao centro da estratégia, influenciando decisões que impactam a continuidade operacional, reputação e valor de mercado.

Ao longo das próximas páginas, o leitor encontrará não apenas conceitos, mas uma estrutura concreta de revisão, argumentações e olhar crítico. Um convite para revisar pressupostos, reorganizar a leitura dos problemas e reposicionar a segurança como um ativo estratégico, e não apenas como um mecanismo de proteção. Porque, no ambiente corporativo atual, não se trata mais de proteger sistemas. Trata-se de sustentar decisões.

PREFÁCIO

Ao longo da minha experiência, aprendi que os maiores desafios das organizações não estão na ausência de tecnologia, mas na forma como decisões são estruturadas em cenários de grande risco.

São poucos os profissionais que conseguem transitar com consistência entre complexidade técnica e clareza de decisões estratégicas, e o Luiz Paiva é um deles. Este livro reflete essa capacidade, a esse modelo complexo de visão e gestão, no qual a clareza da singularidade dos efeitos da segurança se faz necessária e decisória no ambiente corporativo.

Uma leitura recomendada para líderes, executivos e conselhos que compreendem que, no ambiente atual, decidir certo é inseparável de entender e assumir o risco.

Guillermo Gurvich
Vice President at Vicarius and Board Member

INTRODUÇÃO

Nas organizações modernas, a segurança já não pode ser tratada como questão lateral nem como responsabilidade absorvível por arranjos técnicos isolados. Sua presença atravessa decisões, estruturas, prioridades e respostas institucionais, exigindo leitura mais ampla do que aquela tradicionalmente reservada aos controles operacionais.

O problema que motiva esta obra nasce justamente da permanência de uma compreensão fragmentada. Em muitos contextos, a segurança continua dissociada da responsabilidade decisória, da governança e da assunção qualificada do risco. Quando isso ocorre, a organização até reconhece vulnerabilidades, mas não necessariamente as converte em direção, critério e resposta institucional coerente.

É nessa fratura que o livro se insere. Seu argumento central sustenta que a segurança precisa ser compreendida como matéria estratégica, vinculada à forma pela qual a organização distribui responsabilidades, coordena estruturas, interpreta exposições e decide sob condições de incerteza. O que está em questão, portanto, não é o aperfeiçoamento isolado de práticas técnicas, mas a reorganização do lugar da segurança no interior da decisão organizacional.

Foi diante desse cenário que o autor concebeu o ***Método RGA,*** como estrutura analítica voltada a reconectar dimensões que, nas práticas organizacionais, frequentemente aparecem dissociadas. Ao articular responsabilidade, governança e assunção de risco em uma mesma lógica de leitura, o método oferece um modo mais preciso de transformar vulnerabilidade difusa em inteligibilidade institucional, orientação estratégica e capacidade de resposta.

Por essa razão, o livro não se apresenta como manual de tecnologia, nem como exposição genérica sobre governança corporativa. Sua proposta consiste em oferecer uma estrutura analítica e aplicável para compreender como a segurança pode migrar do campo operacional para o núcleo da direção organizacional.

Nesse movimento, a obra busca fornecer ao leitor não apenas interpretação prática, mas um modo mais organizado, preventivo e replicável de examinar problemas, causas, decisões e riscos nas organizações contemporâneas.

CAPÍTULO I

QUANDO A SEGURANÇA VIRA ESTRATÉGIA

Introdução

Durante muito tempo, a segurança foi compreendida nas organizações como função técnica de suporte, associada à proteção de sistemas, à contenção de falhas operacionais e à preservação de ativos informacionais. Esse enquadramento correspondia a um cenário em que tecnologia, gestão e criação de valor ainda apareciam como esferas relativamente separadas, o que permitia tratar a segurança como matéria circunscrita ao plano operacional (NIST, 2024).

No ambiente contemporâneo, essa separação perdeu consistência. Processos, dados, operações e relações institucionais passaram a depender de infraestruturas digitais interconectadas, de modo que eventos de segurança deixaram de produzir efeitos restritos à área técnica e passaram a repercutir sobre continuidade, estabilidade organizacional e confiança institucional (World Economic Forum, 2021).

Esse deslocamento não decorre de simples atualização terminológica. Ele resulta da transformação do ambiente de risco, hoje marcado por interdependência ampliada, maior sensibilidade reputacional e crescente pressão regulatória. Nessas condições, a segurança passa a ser observada como tema vinculado à coordenação estratégica da organização, e não como atividade periférica de suporte (OECD, 2015; NIST, 2024).

O objetivo deste capítulo consiste em demonstrar que a segurança se tornou eixo estratégico porque o risco por ela

administrado extrapola o plano técnico e alcança desempenho, conformidade, reputação e continuidade operacional. A partir desse reposicionamento, forma-se a base conceitual necessária para o aprofundamento posterior da discussão sobre governança, supervisão e responsabilidade institucional (OECD, 2015; NIST, 2024).

Desenvolvimento

A leitura tradicional da segurança se revela insuficiente quando o risco administrado deixa de afetar somente sistemas e passa a alcançar investidores, mercado, regulação e estabilidade institucional. O problema central já não reside apenas na existência de vulnerabilidades técnicas, mas na capacidade dessas vulnerabilidades de comprometer processos essenciais, decisões estratégicas e a confiabilidade da organização perante seus públicos relevantes (OECD, 2015).

É nesse ponto que a contribuição da OECD assume relevo teórico. Ao sustentar que o risco de segurança digital deve ser tratado em perspectiva econômica e social mais ampla e integrado aos processos decisórios dos stakeholders, o documento desloca a segurança do campo do controle isolado para o campo das escolhas institucionais, onde prioridades, impactos e responsabilidades passam a ser articulados no interior da própria condução organizacional (OECD, 2015).

Em convergência com essa inflexão, o NIST reformulou o Cybersecurity Framework na versão 2.0 e introduziu a função *Govern*, conferindo centralidade à governança, à coordenação e ao alinhamento da segurança com os objetivos organizacionais. Ao apresentar o framework como aplicável a organizações de diferentes portes, setores e níveis de maturidade, o modelo reforça que o risco cibernético deve ser compreendido em chave institucional ampla, e

não como matéria restrita ao plano técnico-operacional (NIST, 2024).

Esse reposicionamento altera a lógica de enquadramento da segurança. A técnica continua indispensável, mas deixa de ser suficiente como linguagem exclusiva para compreender um risco que atravessa a estrutura organizacional. Quando a segurança passa a ser pensada sob a ótica da governança, ela passa também a integrar os modos pelos quais a organização distribui responsabilidades, prioriza recursos e responde à incerteza (NIST, 2024).

A passagem para o campo da estratégia corporativa se consolida quando o risco cibernético passa a ser reconhecido como risco de negócio. Nessa formulação, a relevância da segurança não decorre unicamente da possibilidade de ocorrência de incidentes, mas do fato de que tais eventos podem comprometer operações, perturbar fluxos de receita, afetar relações estratégicas e fragilizar a credibilidade da organização perante diferentes públicos (OECD, 2015; World Economic Forum, 2021).

O enquadramento regulatório recente reforça essa mudança conceitual. Em 2023, a Securities and Exchange Commission adotou regras para padronizar divulgações sobre gestão do risco cibernético, estratégia, governança e incidentes materiais em companhias abertas. Ao exigir informações sobre processos de avaliação de riscos, papel da administração e supervisão do board, a norma insere formalmente a segurança no plano da materialidade informacional e da accountability corporativa (SEC, 2023).

A declaração de Gary Gensler torna esse deslocamento particularmente claro ao afirmar que, para investidores, a perda de uma fábrica em um incêndio ou de milhões de arquivos em um incidente cibernético pode ser igualmente material. A comparação mostra que a segurança passou a integrar o universo dos riscos capazes de alterar a leitura do mercado sobre a organização, sua maturidade de gestão e sua capacidade de sustentar operações em contexto adverso (SEC, 2023).

Em organizações intensivas em dados e dependentes de operações digitais, a indisponibilidade de sistemas deixa de representar simples inconveniente operacional. Ela pode ameaçar entregas, compromissos contratuais e fluxos de receita. De forma semelhante, incidentes de segurança deixam de comunicar somente falha técnica e passam a projetar sinais sobre fragilidade de controles, insuficiência de preparo e baixa maturidade na supervisão de riscos, afetando a confiança de investidores, clientes e parceiros (OECD, 2015; SEC, 2023).

Esse alargamento dos efeitos do risco explica por que a segurança não pode mais ser integralmente delegada à área técnica. O World Economic Forum assinala que o risco cibernético está entre os principais riscos enfrentados pelas empresas e que os conselhos precisam de fundamentos mais sólidos para governá-lo de forma efetiva. A questão, portanto, não está em substituir especialistas, mas em reconhecer que a materialidade do problema exige supervisão compatível com sua relevância institucional (World Economic Forum, 2021).

Sempre que os efeitos do risco alcançam valor, continuidade, conformidade e reputação, a estrutura decisória é convocada a compreender exposições relevantes, estabelecer prioridades e acompanhar a coerência entre risco assumido e capacidade de resposta. Com isso, a segurança deixa de pertencer exclusivamente ao terreno da operação e passa a ocupar a fronteira entre gestão e governança, preparando o deslocamento analítico que será aprofundado nos capítulos seguintes (NIST, 2024; World Economic Forum, 2021).

Considerações finais

O percurso desenvolvido neste capítulo permite sustentar que a segurança se tornou estratégica porque a natureza do risco que ela administra se transformou. Interdependência digital, exigências

regulatórias, sensibilidade reputacional e dependência operacional de sistemas deslocaram o tema para o centro das decisões organizacionais, tornando insuficiente descrevê-lo como função de suporte ou especialidade técnica isolada da arquitetura institucional (NIST, 2024; OECD, 2015).

A visão técnico-operacional não desaparece, mas se revela limitada como chave explicativa. A segurança continua envolvendo controles, processos e especialização, porém seus efeitos extrapolam esse horizonte e alcançam continuidade, conformidade, valor e legitimidade institucional. É esse alargamento que justifica sua incorporação à linguagem da estratégia e do risco corporativo (SEC, 2023; World Economic Forum, 2021).

Uma vez reconhecida essa inflexão, torna-se possível avançar para a discussão sobre quem responde por essa supervisão, como a governança a internaliza e de que modo a liderança organizacional passa a assumir papel mais direto na formulação, no acompanhamento e na responsabilização sobre o risco cibernético como risco de negócio (NIST, 2024; SEC, 2023).

CAPÍTULO II

RESPONSABILIDADE DECISÓRIA, ACCOUNTABILITY E ESTRUTURAS FORMAIS DE RESPONSABILIZAÇÃO

Introdução

Nas organizações contemporâneas, a discussão sobre risco, governança e supervisão institucional tem avançado, muitas vezes, com velocidade superior à reflexão sobre quem, efetivamente, responde pelas decisões que moldam esses processos. Essa assimetria produz um problema recorrente: multiplicam-se estruturas, funções e fluxos de reporte, mas nem sempre permanece visível o centro da responsabilidade decisória (Bovens, 2007; OECD, 2023).

Em contextos organizacionais complexos, esse problema se intensifica porque a decisão raramente aparece concentrada em um único sujeito ou órgão. Há delegação, especialização técnica, circulação desigual de informação e distribuição funcional de tarefas. Nessa configuração, execução, supervisão e deliberação tendem a se separar, nem sempre de modo transparente (Aghion; Tirole, 1997).

Essa configuração não elimina a responsabilidade. Em sentido inverso, torna mais necessária sua reconstrução analítica. Quando a organização não distingue com nitidez quem executa, quem supervisiona, quem detém autoridade formal e quem conserva o dever institucional de responder, instala-se um terreno propício à diluição da accountability e à opacidade do risco (Bovens, 2007; NIST (2024).

É nesse ponto que a responsabilidade decisória adquire relevância teórica e prática. Ela não se confunde com a atividade

técnica, nem se reduz à presença de cargos hierarquicamente elevados. Seu núcleo está na relação entre poder de decidir, capacidade de orientar condutas organizacionais e dever de responder pelas consequências derivadas dessa orientação (Keay; Loughrey, 2015; Aghion; Tirole, 1997).

Este capítulo parte dessa premissa para sustentar que a maturidade institucional depende de arranjos que tornem a responsabilidade identificável, atribuível e exigível. Por essa razão, a análise será organizada em torno da definição de responsabilidade nas organizações complexas, da articulação entre accountability e autoridade, da dissociação entre decisão e consequência, do ownership do risco, da permanência da responsabilidade da alta gestão e, por fim, das estruturas formais de responsabilização.

2.1 Conceito de responsabilidade no contexto das organizações complexas

A responsabilidade, no plano organizacional, não pode ser tratada como mera qualidade moral nem como atributo genérico associado ao desempenho diligente de uma função. Para que tenha densidade analítica, precisa ser compreendida como relação institucionalmente situada, vinculada a deveres, papéis, fóruns de avaliação e consequências possíveis. É nesse enquadramento que a literatura sobre accountability oferece uma formulação conceitual mais precisa (Bovens, 2007).

Bovens (2007) propõe uma definição particularmente útil ao entender accountability, em sentido estrito, como uma relação entre um ator e um fórum, na qual o primeiro tem a obrigação de explicar e justificar sua conduta, enquanto o segundo pode formular questionamentos, emitir juízo e produzir consequências. Essa formulação desloca o debate de uma moralidade abstrata para um arranjo institucional verificável.

Essa precisão conceitual é relevante porque, em organizações complexas, a linguagem da responsabilidade costuma ser empregada de forma ampla e, por vezes, imprecisa. Ora ela designa competência funcional, ora compromisso ético, ora capacidade gerencial, ora dever jurídico. Sem um critério analítico mais rigoroso, essas dimensões tendem a se sobrepor, dificultando a identificação de quem efetivamente responde por decisões que condicionam a ação organizacional (Bovens, 2007).

Bovens (2010) aprofunda esse problema ao distinguir accountability como virtude e accountability como mecanismo. No primeiro caso, o termo remete a uma qualidade normativa desejável, associada à conduta responsável de agentes e organizações. No segundo, refere-se a um dispositivo institucional por meio do qual um ator pode ser chamado a prestar contas perante um fórum. Essa distinção evita que a análise confunda avaliação moral com estrutura de responsabilização.

Com base nesse referencial, este capítulo adota, para fins analíticos, uma diferenciação entre quatro planos de responsabilidade: funcional, institucional, executiva e decisória. Essa distinção não é apresentada como tipologia literal de um único autor, mas como síntese analítica construída a partir da literatura sobre accountability, autoridade organizacional e supervisão institucional (Bovens, 2007; Bovens, 2010; Keay; Loughrey, 2015).

A Figura 1 sintetiza os quatro planos de responsabilidade mobilizados nesta seção e evidencia que a responsabilidade decisória não se confunde com a execução funcional, pois decorre da posição ocupada no circuito de autoridade, orientação e resposta institucional.

Figura 1 – Planos analíticos da responsabilidade nas organizações complexas

Fonte: elaboração própria, com base em Bovens (2007; 2010), Keay e Loughrey (2015) e Aghion e Tirole (1997).

A responsabilidade funcional diz respeito ao cumprimento das atribuições associadas a uma atividade, cargo ou processo específico. Seu foco recai sobre a execução adequada de tarefas e sobre a aderência a rotinas, procedimentos e competências previamente delimitadas. Trata-se, portanto, do nível mais próximo da operação.

A responsabilidade institucional, por sua vez, refere-se ao dever de responder pela integridade e pela orientação do arranjo organizacional como um todo, ou de parte relevante dele. Nesse plano, a responsabilidade não decorre da execução direta de cada ato, mas da posição ocupada na arquitetura de supervisão, direção e controle. É a dimensão que melhor evidência que delegar funções não equivale a extinguir deveres de resposta (Bovens, 2007; Keay; Loughrey, 2015).

A responsabilidade executiva situa-se no espaço intermediário entre formulação e operação. Ela envolve a tradução de diretrizes em coordenação, alocação de recursos, definição de prioridades e monitoramento de cumprimento. Seu traço distintivo não está no simples comando hierárquico, mas na mediação concreta entre objetivos organizacionais e capacidade de implementação.

Já a responsabilidade decisória constitui o núcleo deste capítulo. Ela se configura quando determinado agente ou instância possui autoridade suficiente para definir cursos de ação, validar escolhas estratégicas, aprovar diretrizes ou manter, mesmo após a delegação, o poder formal de orientação e revisão. Nesse caso, a responsabilidade não nasce da execução imediata, mas da posição ocupada no circuito que conforma a decisão organizacional (Aghion; Tirole, 1997; Keay; Loughrey, 2015).

Essa diferenciação se torna necessária porque organizações complexas frequentemente distribuem tarefas sem distribuir, com a mesma clareza, os deveres correspondentes de resposta. O resultado é a formação de zonas cinzentas em que muitos participam do processo, mas poucos permanecem claramente vinculados às consequências da decisão. É justamente dessa fratura que emerge a necessidade de examinar, com maior precisão, a relação entre accountability, autoridade e poder decisório (Bovens, 2007; Aghion; Tirole, 1997).

Perfeito. Segue a seção 2.2, já no mesmo padrão: parágrafos curtos, progressão argumentativa contínua, citações no corpo do texto e o ponto exato em que a próxima figura deve entrar.

2.2 Accountability, autoridade e poder decisório

A discussão sobre accountability exige um passo adicional quando transposta para o ambiente organizacional. Não basta afirmar que um agente deve responder por seus atos. É necessário examinar de que modo essa exigência se articula com a autoridade

que sustenta a decisão e com a posição ocupada pelo agente no circuito institucional de comando, supervisão e resposta. Bovens (2007) permite essa passagem ao definir accountability como relação entre ator e fórum, mas a complexidade organizacional impõe o exame mais preciso da autoridade que antecede a própria prestação de contas.

Nessa direção, accountability não pode ser confundida com mera visibilidade administrativa nem com simples reporte posterior. Seu sentido institucional depende da existência de um vínculo entre poder de orientação, capacidade de influir sobre cursos de ação e dever de responder perante instâncias aptas a avaliar, questionar e produzir consequências. Sem essa ligação, a organização preserva rotinas de informação, mas não necessariamente uma estrutura efetiva de responsabilização (Bovens, 2007).

É nesse ponto que a distinção proposta por Aghion e Tirole (1997) se torna decisiva. Para os autores, a autoridade formal corresponde ao direito de decidir, enquanto a autoridade real se relaciona ao controle efetivo da decisão, condicionado pela distribuição de informação e pela capacidade concreta de influenciar o desfecho organizacional. Essa diferença permite compreender por que o titular jurídico ou hierárquico da decisão nem sempre coincide com o agente que, na prática, conforma a escolha realizada.

Em organizações complexas, essa dissociação é recorrente. A especialização técnica, a descentralização operacional e a circulação desigual de conhecimento produzem situações em que a autoridade formal permanece localizada em determinado nível, ao passo que a autoridade real se desloca para agentes que detêm informação crítica e influência efetiva sobre a decisão. Nesses casos, a responsabilização institucional não pode ser deduzida automaticamente nem da execução material, nem da simples posição no organograma.

Keay e Loughrey (2015) reforçam esse problema ao tratar da accountability do board como estrutura própria da governança

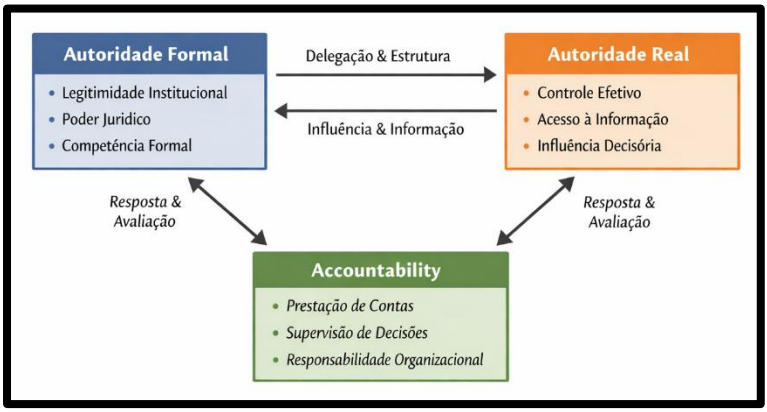
corporativa. A contribuição central dessa leitura está em demonstrar que a delegação de funções não suprime, por si, a responsabilidade do nível que conserva competência formal de supervisão, validação ou revisão. A delegação redistribui tarefas e pode deslocar parcelas de autoridade real, mas não extingue o dever institucional de responder pelas escolhas que continuam inscritas no âmbito da direção e do controle.

Essa formulação exige cautela contra um equívoco recorrente: identificar o responsável apenas pelo lugar ocupado na hierarquia formal. Embora a posição institucional seja indispensável para a imputação, ela não esgota a análise da responsabilidade decisória. Em estruturas complexas, o organograma informa competências e subordinações, mas pode não revelar, com precisão suficiente, onde se concentram a informação relevante, a iniciativa operacional e a capacidade efetiva de conformar a decisão.

Por isso, accountability deve ser compreendida também como critério de inteligibilidade institucional. Ela não opera exclusivamente após a decisão, quando se pergunta quem deve prestar contas. Atua, igualmente, no momento anterior, ao exigir que a organização torne identificáveis os nexos entre decisão, orientação, execução e dever de resposta. Nesse sentido, a accountability não é mero instrumento retrospectivo de cobrança, mas mecanismo de clarificação da própria arquitetura decisória.

A Figura 2 sintetiza a articulação entre autoridade formal, autoridade real e accountability, demonstrando que a responsabilidade decisória emerge da combinação entre legitimidade institucional, controle efetivo da decisão e dever de resposta perante fóruns organizacionais de supervisão.

Figura 2 – Relação entre autoridade formal, autoridade real e accountability nas organizações complexas



Fonte: elaboração própria, com base em Bovens (2007), Aghion e Tirole (1997) e Keay e Loughrey (2015).

No plano da governança, essa exigência se torna ainda mais relevante porque a distância entre decisão estratégica e execução operacional tende a crescer com a especialização organizacional. Quanto maior essa distância, maior o risco de produção de zonas cinzentas em que muitos participam do processo, mas poucos permanecem claramente vinculados às suas consequências. É justamente essa fratura que prepara o problema seguinte: a dissociação entre quem decide e quem suporta, direta ou indiretamente, os efeitos da decisão.

2.3 Dissociação entre decisão e consequência

Uma vez reconhecido que a responsabilidade decisória não se confunde com a execução, torna-se necessário examinar outro problema: a distância entre quem participa da decisão e quem suporta, direta ou indiretamente, seus efeitos. Em organizações

complexas, essa distância não constitui exceção. Ela tende a emergir quando o processo decisório é distribuído, tecnicamente fragmentado e institucionalmente escalonado.

Nessas condições, a consequência da decisão raramente retorna de modo linear ao ponto em que a deliberação foi formada. Seus efeitos podem recair sobre unidades operacionais, áreas de suporte, terceiros, usuários, mercados ou sobre a própria reputação institucional. Quanto mais longa e fragmentada a cadeia entre decisão e efeito, maior a dificuldade de preservar a visibilidade da responsabilidade correspondente.

El Zein, Bahrami e Hertwig (2019) oferecem uma chave analítica útil para compreender esse fenômeno ao sustentar que decisões coletivas não são buscadas somente por seu potencial de aumentar a acurácia, mas também por reduzirem a carga material e psicológica da responsabilidade individual. Segundo os autores, decidir com outros pode proteger o indivíduo das consequências negativas ao reduzir arrependimento, punição e estresse. Ainda que o estudo não trate diretamente de governança corporativa, sua contribuição é valiosa para explicar por que a partilha decisória pode vir acompanhada de dispersão subjetiva da responsabilidade.

Transposta para o plano organizacional, essa percepção permite compreender que a decisão compartilhada nem sempre produz corresponsabilização efetiva. Em certos arranjos, ela produz o oposto: uma zona difusa em que muitos influenciam, poucos assumem e quase ninguém permanece claramente vinculado ao conjunto das consequências. O problema, portanto, não está na cooperação decisória em si, mas na ausência de mecanismos capazes de impedir que a pluralidade de intervenções se converta em anonimato institucional.

É justamente nesse ponto que a literatura sobre ownership do risco se torna decisiva. Årstad e Engen (2018) afirmam que o conceito de risk ownership permite enfrentar a questão da agência em sistemas sociotécnicos complexos e argumentam que grandes

acidentes podem ser vistos como falhas de ownership do risco. A relevância dessa formulação está em mostrar que o risco não se torna governável apenas porque foi identificado, mensurado ou distribuído em relatórios; ele exige também a identificação de quem deve mantê-lo sob vigilância, resposta e coordenação.

Essa exigência altera o modo de compreender a dissociação entre decisão e consequência. O problema não decorre apenas do fato de que diferentes agentes participam de momentos distintos do processo. Ele surge, sobretudo, quando a organização permite que a consequência se espalhe sem que o vínculo de resposta permaneça claramente ancorado. Em outras palavras, a complexidade não elimina a necessidade de imputação; ao contrário, torna essa necessidade mais rigorosa.

Nesse contexto, a dissociação entre decisão e consequência pode assumir ao menos três formas organizacionalmente relevantes. A primeira ocorre quando a decisão é aprovada em determinado nível, mas seus efeitos adversos recaem sobre instâncias que não participaram de sua formulação. A segunda aparece quando a influência sobre a decisão é distribuída entre múltiplos agentes, tornando difícil identificar quem, de fato, deveria responder por sua direção final. A terceira se manifesta quando o risco é reconhecido como relevante, mas permanece sem owner funcionalmente visível e institucionalmente legitimado.

Essas três formas não devem ser tratadas como desvios ocasionais. Elas constituem possibilidades recorrentes em arranjos marcados por especialização, delegação, multiplicidade de fóruns e circulação assimétrica de informação. Por isso, a maturidade institucional não pode ser medida apenas pela existência de processos decisórios ou estruturas de reporte. Ela depende, de modo mais exigente, da capacidade de impedir que a consequência se desprenda da responsabilidade correspondente.

Nesse ponto, o debate deixa de ser apenas descritivo. A dissociação entre decisão e consequência não é um dado neutro da

complexidade organizacional. Ela representa uma fragilidade de governança, porque compromete a rastreabilidade da decisão, obscurece a alocação do risco e dificulta a ativação de mecanismos corretivos. Quando não se sabe com nitidez quem deve responder, a organização preserva circulação de tarefas, mas enfraquece a capacidade de correção institucional.

Por essa razão, o problema da consequência não pode ser tratado como etapa posterior e acidental da decisão. Ele já está contido no próprio desenho do processo decisório. Toda arquitetura organizacional que distribui influência, escalona validações e segmenta execução precisa, simultaneamente, preservar a inteligibilidade da resposta. Sem isso, a organização corre o risco de transformar coordenação em difusão, participação em anonimato e complexidade em opacidade.

A seção seguinte avança justamente nesse ponto ao examinar o ownership do risco não como categoria acessória, mas como mecanismo necessário para reconectar decisão, vigilância, resposta e consequência no interior da governança organizacional.

Figura 3 – Dissociação entre decisão, consequência e ownership do risco nas organizações complexas

Fonte: elaboração própria, com base em El Zein, Bahrami e Hertwig (2019).

A Figura 3 sintetiza a fratura entre decisão e consequência em estruturas organizacionais complexas, evidenciando que a dispersão da influência decisória e a ausência de owner claramente identificado fragilizam a rastreabilidade institucional da responsabilidade.

2.4 Ownership do risco e atribuição formal de papéis

Se a seção anterior demonstrou que a complexidade organizacional pode dissociar decisão e consequência, esta seção parte de uma pergunta mais exigente: como reconectar institucionalmente aquilo que a fragmentação tende a dispersar. A resposta passa pelo ownership do risco, entendido não como rótulo administrativo, mas como mecanismo de atribuição visível de vigilância, coordenação e dever de resposta.

Nesse contexto, a governança do risco não pode ser reduzida à existência de controles, relatórios ou mapas de exposição. Tais instrumentos são relevantes, mas não resolvem, por si, o problema da imputação. Um risco pode estar identificado, classificado e monitorado sem que exista, de modo inequívoco, um responsável institucionalmente reconhecido por acompanhar sua evolução, articular respostas e manter sua inteligibilidade diante das instâncias de supervisão.

Lundqvist (2015) oferece uma formulação particularmente importante para este ponto ao sustentar que o ERM deve ser compreendido como composição entre *traditional risk management* e *risk governance*, sendo esta última a etapa ativa que leva além do gerenciamento tradicional. A contribuição do argumento está em mostrar que a maturidade do risco não depende apenas de técnicas de identificação e tratamento, mas da existência de uma arquitetura de governança capaz de situar o risco no interior das responsabilidades organizacionais.

É justamente nessa passagem que o ownership do risco adquire centralidade. Seu sentido não está em personalizar

artificialmente problemas complexos, mas em impedir que riscos relevantes permaneçam institucionalmente órfãos. Em estruturas organizacionais densas, nas quais múltiplas áreas influenciam uma mesma exposição, a ausência de *owner* tende a produzir um efeito recorrente: muitos acompanham parcialmente, poucos coordenam e quase ninguém responde pela preservação da coerência entre risco, decisão e consequência.

Essa lógica fica ainda mais clara quando se observa a orientação normativa recente do NIST. No CSF 2.0, a função *Govern* inclui a categoria GV.RR, Roles, Responsibilities, and Authorities, que exige o estabelecimento, a comunicação e a aplicação de papéis, responsabilidades e autoridades relacionados ao gerenciamento do risco cibernético. O ponto relevante aqui não é apenas a formalização documental, mas a compreensão de que a governança do risco depende de clareza institucional sobre quem responde por quê, em que nível e perante quais fóruns.

Nessa mesma direção, o NIST IR 8286 Rev. 1 afirma ser vital que diretores e líderes seniores tenham compreensão clara da postura de risco cibernético e que os responsáveis pela identificação, avaliação e tratamento do risco compreendam os objetivos estratégicos da organização ao tomar decisões. A implicação disso é direta: o ownership do risco não pode ser pensado como tarefa isolada de áreas técnicas, porque ele precisa permanecer articulado à governança, à estratégia e às responsabilidades fiduciárias da organização.

Com isso, o ownership do risco deve ser compreendido em pelo menos três dimensões complementares. A primeira é a dimensão de vigilância, pela qual determinado risco precisa permanecer sob acompanhamento contínuo e inteligível. A segunda é a dimensão de coordenação, que exige articulação entre áreas, funções e níveis decisórios afetados pela mesma exposição. A terceira é a dimensão de resposta, que preserva o vínculo entre risco

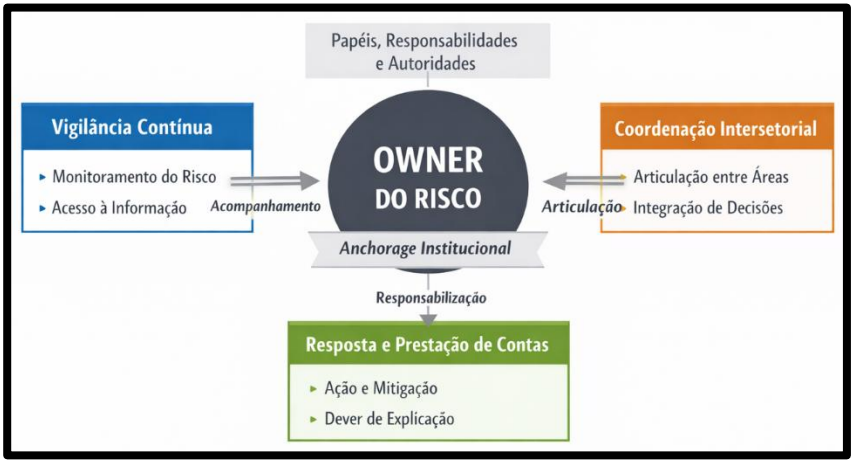
identificado, ação esperada e dever de explicação perante instâncias de supervisão.

Sem essas três dimensões, a atribuição de *owner* tende a se degradar em formalidade burocrática. O nome do responsável pode até constar em políticas, matrizes ou registros, mas sem autoridade suficiente, acesso à informação e capacidade de coordenação, o ownership deixa de operar como elo de governança e passa a funcionar como mera anotação procedimental. Em outras palavras, não basta nomear; é necessário tornar a atribuição operável e institucionalmente reconhecível.

Essa observação também impede que o debate seja reduzido à ideia de culpabilização individual. O ownership do risco não serve para deslocar toda a carga da governança para um único agente. Sua função é outra: preservar um centro visível de ancoragem institucional que impeça a dissolução da responsabilidade em estruturas excessivamente segmentadas. O *owner* não substitui a supervisão superior nem elimina o papel de outras áreas; ele viabiliza a rastreabilidade da resposta no interior de uma arquitetura organizacional distribuída.

Por isso, a atribuição formal de papéis precisa ser lida como condição de maturidade institucional. Quando a organização sabe quem acompanha, quem coordena, quem valida e quem responde, o risco deixa de circular como abstração gerencial e passa a integrar, com maior nitidez, os circuitos de decisão e supervisão. É essa reconexão que prepara a próxima etapa do capítulo: a permanência da responsabilidade da alta gestão e do conselho, mesmo quando a operação cotidiana do risco se encontra distribuída por diferentes funções e níveis.

Figura 4 – Ownership do risco e atribuição formal de papéis na governança organizacional



Fonte: elaboração própria, com base em Lundqvist (2015), NIST CSF 2.0 e NIST IR 8286 Rev. 1.

A Figura 4 sintetiza o ownership do risco como mecanismo de ancoragem institucional, evidenciando que vigilância, coordenação e resposta dependem da atribuição formal de papéis, responsabilidades e autoridades articuladas à governança e aos objetivos estratégicos.

2.5 Permanência da responsabilidade da alta gestão e do conselho

O reconhecimento de owners, papéis formais e estruturas de coordenação não encerra o problema da responsabilidade organizacional. Ao contrário, ele recoloca em outro nível a questão central do capítulo: quem permanece institucionalmente vinculado à supervisão do risco quando sua gestão cotidiana se encontra distribuída por diferentes áreas, funções e especialistas. É nesse

ponto que a responsabilidade da alta gestão e do conselho se impõe como dimensão irrenunciável da governança.

Essa permanência não decorre da execução direta de cada ação de controle, nem da participação contínua em todas as decisões operacionais. Ela decorre da posição ocupada por essas instâncias na arquitetura de direção, supervisão, validação e resposta institucional. Em outras palavras, quanto mais a organização distribui a execução, mais relevante se torna a preservação de níveis superiores capazes de orientar prioridades, acompanhar exposições relevantes e exigir inteligibilidade sobre os riscos assumidos.

Os *G20/OECD Principles of Corporate Governance 2023* reforçam essa compreensão ao situar o *board* no centro da supervisão da estratégia, da gestão de riscos e dos sistemas de governança corporativa. O ponto mais importante, para esta seção, é que a supervisão do risco não aparece como atribuição periférica ou eventual, mas como dimensão constitutiva das responsabilidades do conselho. Isso significa que a delegação gerencial e a especialização funcional não desfazem o vínculo entre o nível superior da organização e o dever de zelar pela coerência do sistema de controle e resposta.

Essa formulação exige afastar um equívoco recorrente: o de imaginar que a maturidade da governança se prova pela simples existência de funções especializadas abaixo do nível superior. A presença de gestores de risco, comitês, estruturas de conformidade, auditoria interna ou owners formais é necessária, mas não suficiente. Tais mecanismos fortalecem a governança precisamente porque permitem que a alta gestão e o conselho exerçam melhor sua função de supervisão, e não porque os substituam.

O NIST IR 8286 Rev. 1 (2025) é particularmente útil para aprofundar essa passagem. O documento afirma ser vital que diretores e líderes seniores compreendam a postura de risco cibernético da organização e que aqueles que identificam, avaliam e tratam riscos compreendam, ao decidir, os objetivos estratégicos da

organização. Essa dupla exigência mostra que a governança do risco depende de integração vertical: o nível estratégico precisa compreender o risco, e o nível técnico-operacional precisa agir em coerência com as diretrizes estratégicas.

A consequência analítica disso é clara. A alta gestão e o conselho não são chamados a absorver toda a operacionalização do risco, mas a manter a responsabilidade por sua orientação institucional. Essa responsabilidade se manifesta, entre outros aspectos, na definição de prioridades, na aprovação de diretrizes, na avaliação da suficiência dos arranjos de controle, na análise de exposições materiais e na exigência de reporte inteligível. Onde esse vínculo se enfraquece, a governança tende a perder densidade, mesmo que as estruturas técnicas sejam sofisticadas.

Keay e Loughrey (2015) reforçam esse argumento ao tratar da accountability do *board* como moldura própria da governança corporativa. A importância dessa contribuição, no contexto do capítulo, está em deixar claro que o conselho não responde porque executa, mas porque ocupa a posição institucional a partir da qual a organização valida, supervisiona e sustenta seus compromissos decisórios. A responsabilidade superior, portanto, não deriva da proximidade com cada ato operacional, mas da permanência da competência de direção e supervisão.

Essa compreensão também impede que a distribuição de papéis seja confundida com transferência integral de responsabilidade. A lógica da boa governança não consiste em empurrar o risco para baixo na hierarquia, mas em construir uma arquitetura em que diferentes níveis assumam funções distintas sem romper a continuidade da resposta institucional. O owner acompanha e coordena. As funções especializadas apoiam, monitoram e estruturam. A alta gestão e o conselho permanecem responsáveis pela orientação, pela suficiência do sistema e pela inteligibilidade das exposições mais relevantes.

Sob esse prisma, a permanência da responsabilidade da alta gestão e do conselho não representa concentração indevida, mas condição de coerência organizacional. Sem esse nível superior de ancoragem, a governança corre o risco de se tornar uma justaposição de controles parciais, relatórios fragmentados e respostas sem unidade estratégica. A consequência não é apenas falha formal de supervisão, mas perda de capacidade institucional de reconhecer, priorizar e tratar riscos de modo compatível com os objetivos da organização.

Por isso, a maturidade institucional não se mede apenas pela quantidade de estruturas de apoio ao risco, mas pela capacidade de manter, no topo da organização, uma responsabilidade que não desaparece com a delegação. Quanto mais sofisticado o arranjo organizacional, mais indispensável se torna a clareza sobre esse ponto. A governança não substitui a responsabilidade superior; ela a torna mais exigente, mais informada e mais rastreável.

A permanência da responsabilidade da alta gestão e do conselho não se expressa pela execução direta das rotinas de controle, mas pela posição que essas instâncias ocupam na estrutura de supervisão, orientação institucional e dever de resposta. Para tornar essa arquitetura mais inteligível, a figura a seguir sintetiza o modo pelo qual a governança superior se desdobra em funções estruturantes e se conecta à gestão operacional de riscos, sem romper a continuidade da responsabilização institucional.

A Figura 5 demonstra que a responsabilidade da alta gestão e do conselho permanece no topo da governança do risco, desdobrando-se em três eixos centrais: supervisão estratégica, orientação institucional e dever de resposta. Esses eixos se materializam em diretrizes e prioridades, integridade do sistema e análise e validação, alcançando a gestão operacional de riscos e suas funções especializadas. Desse modo, a imagem evidencia que a distribuição operacional de papéis não elimina a responsabilidade

superior, mas a torna dependente de uma estrutura capaz de conectar decisão, acompanhamento e resposta institucional.

Figura 5 – Permanência da responsabilidade da alta gestão e do conselho na governança do risco

Fonte: elaboração própria, com base em OECD (2023), NIST IR 8286 Rev. 1 (2025) e Keay e Loughrey (2015).

Dessa forma, a permanência da responsabilidade da alta gestão e do conselho não constitui resíduo simbólico da hierarquia, mas condição de coerência da governança do risco. É essa permanência que impede que a distribuição de funções se converta em dispersão de deveres e que a sofisticação operacional produza, paradoxalmente, opacidade institucional. Por isso, a etapa seguinte da análise não consiste mais em identificar quem permanece responsável, mas em examinar quais estruturas formais tornam essa responsabilidade visível, rastreável e exigível no interior da organização.

2.6 Estruturas formais de responsabilização

A responsabilidade organizacional atinge seu ponto mais sensível quando deixa o plano das formulações abstratas e precisa ser convertida em arranjos institucionais concretos. Até aqui, o capítulo demonstrou que a decisão não pode permanecer dissociada da resposta, que o risco exige *owner* identificável e que a alta gestão e o conselho conservam deveres superiores de supervisão. Resta, então, examinar de que modo essa responsabilidade se materializa em estruturas capazes de torná-la visível, rastreável e exigível.

Esse deslocamento é decisivo porque, em organizações complexas, a simples consciência de que alguém deve responder não basta para sustentar a governança. Sem linhas formais de reporte, critérios de escalonamento, funções claramente diferenciadas e mecanismos de *assurance*, a responsabilidade tende a permanecer dependente de interpretações circunstanciais. O problema, nesse caso, não é ausência completa de funções, mas insuficiência de articulação entre elas.

É por isso que a responsabilização institucional não pode ser tratada como efeito espontâneo da hierarquia. Ela depende de desenho organizacional. A organização precisa tornar inteligível quem acompanha, quem executa, quem monitora, quem supervisiona e por quais vias a informação circula até alcançar os níveis aptos a avaliar, corrigir e responder. Quando esses nexos permanecem opacos, a governança se fragiliza mesmo diante de estruturas aparentemente sofisticadas.

Nesse ponto, o problema deixa de ser identificar, em tese, quem deveria responder e passa a ser demonstrar como essa resposta se sustenta institucionalmente. A maturidade organizacional revela-se, portanto, menos na quantidade de áreas envolvidas e mais na capacidade de conectar papéis, autoridade, reporte e supervisão em uma arquitetura coerente de responsabilização.

A partir dessa premissa, esta seção examina as estruturas formais que permitem estabilizar a responsabilidade no interior da governança. O foco recai sobre linhas de reporte, segregação funcional, fóruns de supervisão, funções de monitoramento e mecanismos de *assurance*, compreendidos não como acessórios administrativos, mas como condições para que a responsabilidade não se perca na complexidade do sistema.

Nesse sentido, estruturas formais de responsabilização não servem para burocratizar a governança, mas para impedir que a distribuição funcional se converta em dispersão de deveres. Quando os papéis são visíveis, as competências são diferenciadas e os fluxos de informação são previsíveis, a organização amplia sua capacidade de rastrear decisões, reconhecer fragilidades e ativar correções com maior coerência institucional.

Esse desenho exige, ao menos, quatro componentes articulados. O primeiro corresponde às linhas de reporte, que asseguram o encaminhamento da informação até os níveis aptos a avaliar e decidir. O segundo refere-se à segregação funcional, que diferencia execução, monitoramento, supervisão e avaliação independente. O terceiro envolve os critérios de escalonamento, indispensáveis para que situações relevantes não permaneçam retidas em níveis inadequados de tratamento. O quarto diz respeito aos mecanismos de assurance, que fortalecem a verificação, a consistência e a confiabilidade da resposta organizacional.

A relevância desses componentes está em tornar a responsabilidade menos dependente de interpretações casuísticas. Em vez de reagir ao evento apenas depois que a falha se materializa, a organização passa a operar com uma arquitetura em que a informação circula, a supervisão é acionável e a resposta pode ser cobrada com maior nitidez. Onde essa estrutura não existe, a tendência é que o sistema funcione por aproximações, sobreposição de papéis e correções tardias.

Para tornar essa arquitetura mais inteligível, a figura a seguir sintetiza as estruturas formais de responsabilização que conectam governança superior, linhas de reporte, segregação funcional, escalonamento decisório e mecanismos de monitoramento no interior da organização.

Figura 6 – Estruturas formais de responsabilização na governança organizacional

Fonte: elaboração própria, com base em The IIA (2020), NIST CSF 2.0 e Slapničar et al. (2023).

A Figura 6 demonstra que a responsabilização institucional depende de uma arquitetura formal composta por supervisão superior, linhas de reporte, segregação funcional, escalonamento decisório e mecanismos de assurance e monitoramento. Desse modo, a imagem evidencia que a responsabilidade não se sustenta apenas na existência de cargos ou funções isoladas, mas na articulação entre papéis, fluxos de informação e instâncias capazes de supervisionar, corrigir e exigir resposta.

Considerações Finais

A análise desenvolvida neste capítulo permitiu demonstrar que a responsabilidade, nas organizações complexas, não pode ser reduzida à execução nem tratada como efeito automático da hierarquia. Sua compreensão exige observar a relação entre decisão, autoridade, risco e resposta institucional, pois é nesse entrelaçamento que se define quem permanece vinculado, de modo efetivo, às consequências do agir organizacional.

Nesse sentido, o capítulo sustentou que a responsabilidade decisória constitui elemento central de inteligibilidade da governança. Em estruturas marcadas por especialização, delegação e circulação desigual de informação, a decisão tende a se distribuir sem que, no mesmo movimento, permaneçam igualmente claros os deveres correspondentes de resposta. É justamente essa fratura que torna insuficiente uma leitura puramente funcional da responsabilidade e exige mecanismos capazes de preservar sua ancoragem institucional.

A análise também evidenciou que a coerência da governança depende da capacidade de impedir que risco, decisão e consequência circulem de forma dissociada. Quando não há clareza sobre quem acompanha, coordena, valida e responde, a organização enfraquece sua própria capacidade de supervisão, correção e aprendizado. Por essa razão, o ownership do risco, a permanência da responsabilidade da alta gestão e do conselho e a formalização de linhas de reporte, monitoramento e assurance não aparecem como camadas isoladas, mas como partes complementares de uma mesma arquitetura de responsabilização.

Desse modo, a principal conclusão do capítulo reside na afirmação de que a maturidade institucional depende menos da multiplicação de funções e mais da capacidade de manter, ao longo de toda a estrutura organizacional, nexos claros entre autoridade, supervisão e dever de resposta. É essa exigência de coerência institucional que encerra o percurso analítico aqui desenvolvido e

prepara, em bases mais consistentes, o avanço da discussão no capítulo seguinte.

CAPÍTULO III

GOVERNANÇA INTEGRADA: ARTICULAÇÃO ENTRE SEGURANÇA, ESTRATÉGIA E ÁREAS ORGANIZACIONAIS

Introdução

Ao final do capítulo anterior, evidenciou-se que a segurança estratégica requer definição de responsabilidades, clareza quanto aos polos decisórios e reconhecimento institucional de que o risco não pode ser tratado como matéria periférica. Esse avanço, contudo, não resolve integralmente o problema. A existência de responsáveis, por si só, não assegura que a segurança opere de modo coordenado no interior da organização. Quando faltam estruturas capazes de ordenar atribuições, conectar áreas e sustentar decisões, a responsabilidade formal tende a se dispersar entre instâncias, níveis hierárquicos e funções distintas.

É nesse contexto que se insere o problema central deste capítulo. Em numerosas organizações, segurança, risco, compliance, liderança e negócio ainda funcionam de modo pouco articulado, com fraca integração entre fluxos de informação, critérios de priorização e circuitos decisórios. Nessa configuração, a segurança não deixa de existir, mas perde consistência institucional. Em lugar de compor um campo coordenado de direção estratégica, passa a depender de respostas setoriais, iniciativas fragmentadas e arranjos instáveis.

A tese desenvolvida neste capítulo parte dessa constatação. Sem governança integrada, a segurança tende à reatividade, à dispersão e à baixa maturidade organizacional, porque lhe faltam mecanismos institucionais capazes de articular estruturas, competências, informação e decisão em torno de uma orientação

comum. Nessa perspectiva, governança não se reduz a um repertório genérico de controle nem a um conjunto abstrato de boas práticas. Trata-se do arranjo institucional que converte responsabilidade formal em coordenação efetiva, vinculando supervisão, gestão, circulação informacional e direção estratégica.

Com base nesse eixo analítico, o capítulo examina a governança integrada como condição organizacional para que a segurança deixe de operar como prática isolada e passe a constituir dimensão efetiva da estratégia institucional.

3.1 Falta de governança integrada como causa organizacional

A fragilidade da segurança estratégica, em organizações complexas, não decorre necessariamente de insuficiência técnica isolada. Com frequência, ela se forma quando áreas, funções e instâncias decisórias existem formalmente, mas operam com baixa articulação entre si. Nessa configuração, a informação circula de modo fragmentado e perde capacidade de orientar decisões de forma coerente no plano institucional.

Por essa razão, o diagnóstico precisa ser deslocado do plano funcional para o plano organizacional. O ponto central deixa de ser a mera existência de especialistas, controles ou procedimentos e passa a ser a capacidade institucional de coordená-los. Sem esse arranjo, a organização reúne partes, mas não produz integração efetiva.

É nesse sentido que a ausência de governança integrada deve ser compreendida como causa organizacional da fragilidade da segurança estratégica. Em seu sentido institucional, a governança diz respeito à estrutura e aos sistemas pelos quais objetivos são definidos, meios são estabelecidos e o desempenho é monitorado, isto é, 'the structure and systems' (OECD, 2023). Quando essa arquitetura não articula funções, fluxos e instâncias de decisão, a segurança tende a permanecer dispersa

A literatura especializada sustenta esse entendimento ao mostrar que a segurança já não pode ser tratada como domínio estritamente técnico. Soomro, Shah e Ahmed (2016) indicam que sua efetividade depende de alinhamento transversal com a governança, a gestão e os objetivos organizacionais. Nessa mesma linha, a governança da segurança da informação passa a ser compreendida como campo voltado à integração entre segurança, negócio e alta decisão. O ponto comum entre essas leituras está em reconhecer que a vulnerabilidade persiste mesmo quando há recursos e funções estabelecidos, desde que falte o arranjo institucional capaz de lhes conferir coerência.

No plano normativo, o NIST reforça essa perspectiva ao vincular a cibersegurança a uma 'broader enterprise risk management (ERM) strategy' (NIST (2024). O modelo das Três Linhas, do The IIA, aprofunda essa compreensão ao mostrar que governança, gestão e auditoria interna possuem funções distintas, porém interdependentes. A maturidade, portanto, não decorre da fusão de papéis, mas da coordenação entre instâncias complementares. Quando essa coordenação falha, a organização responde de maneira parcial, e não como sistema integrado

Os efeitos dessa fragmentação ultrapassam a esfera administrativa. Ela dificulta a priorização, dispersa responsabilidades, enfraquece a passagem da informação para a decisão e reduz a capacidade de a segurança alcançar o topo organizacional com densidade suficiente. Papazafeiropoulou e Spanaki (2016), ao tratarem governança, risco e compliance 'as an integrated concept', oferecem formulação particularmente pertinente: quando esses campos operam de forma paralela, sem articulação estável, a segurança perde consistência estratégica e passa a depender de acoplamentos frágeis entre áreas com racionalidades distintas.

Essa falha pode ser observada, de modo ilustrativo, em contextos nos quais estruturas formais coexistem com baixa

coerência entre política, supervisão e execução. Nos casos Equifax e SolarWinds, mais do que o incidente em si, sobressai a insuficiência de coordenação institucional entre risco conhecido, controles, acompanhamento interno e comunicação organizacional. O aspecto analiticamente relevante, portanto, não é o evento isolado, mas a desconexão entre elementos que deveriam operar de modo articulado

Sem governança integrada, a segurança não alcança o nível de coordenação necessário para informar prioridades, ordenar respostas e sustentar leitura institucional coerente do risco. A organização pode conservar estruturas, relatórios e competências, mas continua com baixa capacidade de articulação. Nessa medida, a falta de governança integrada não representa deficiência periférica. Ela constitui causa antecedente da dispersão institucional que enfraquece a segurança e reduz sua maturidade. É justamente dessa fragmentação que decorre o próximo problema analítico: a separação entre estratégia e risco no interior do processo decisório.

3.2 A separação entre estratégia e risco

A separação entre estratégia e risco constitui falha de governança porque rompe a conexão entre direção organizacional e leitura das exposições capazes de comprometer objetivos, continuidade e desempenho. Quando esses domínios operam em circuitos distintos, a decisão perde coerência institucional, e a segurança tende a ser deslocada para um plano paralelo, dissociado do centro da orientação organizacional.

Os Princípios G20/OECD oferecem base clara para essa compreensão ao definirem a governança como 'the structure and systems' pelos quais os objetivos são estabelecidos, os meios são definidos e o desempenho é monitorado (OECD, 2023, p. 7). Nessa formulação, estratégia e risco integram o mesmo campo de direção e supervisão. A própria atribuição ao board da 'the strategic

guidance of the company' (OECD, 2023, p. 35) reforça que o risco não pode permanecer relegado a margens técnicas ou administrativas sem comprometer a consistência da orientação institucional.

Por isso, essa dissociação não deve ser interpretada como detalhe operacional. Trata-se de falha institucional que impede a articulação entre prioridades, exposição e resposta em uma mesma arquitetura decisória. O efeito direto é a produção de decisões parciais, formuladas com base em objetivos que não incorporam, de modo suficiente, a leitura das vulnerabilidades que podem restringir sua execução.

O COSO (2017) sustenta essa perspectiva ao integrar enterprise risk management, estratégia e desempenho. Seu ponto decisivo está em rejeitar a ideia de que o risco possa ser administrado em trilha paralela, como se a formulação estratégica pudesse ocorrer primeiro e a análise das exposições relevantes fosse feita posteriormente, em outro espaço decisório. Quando essa lógica prevalece, a organização enfraquece sua capacidade de priorização: a estratégia avança sem leitura articulada das condições de risco, enquanto o risco passa a ser monitorado como inventário técnico, sem influência efetiva sobre escolhas, recursos e escalonamento.

No campo da cibersegurança, o NIST CSF 2.0 explicita essa exigência ao vincular o tema a uma 'broader enterprise risk management (ERM) strategy' (NIST (2024). O NIST IR 8286 Rev. 1 aprofunda essa diretriz ao afirmar que o risco cibernético deve ser lido em conexão com os 'broader mission and business objectives' da organização (QUINN et al., 2025, p. i). A implicação é direta: quando o risco não se articula com missão, objetivos e estratégia, a segurança deixa de informar o centro decisório e passa a atuar de forma tardia, já sob a forma de correção, contenção ou remediação.

Essa separação produz, ainda, um efeito institucional relevante: a desconexão entre segurança e valor organizacional. Quando risco e estratégia seguem por trilhas apartadas, a segurança

perde capacidade de demonstrar sua relação com continuidade, desempenho, reputação e viabilidade institucional. Nessa condição, tende a ser percebida como custo funcional ou exigência técnica, e não como dimensão estratégica da organização.

A ISO 31000 reforça essa leitura ao estabelecer que a gestão de riscos deve ser integrada à governança, à estratégia, ao planejamento, à gestão e à cultura organizacional (ISO, 2018). No mesmo sentido, Hiebl (2024) mostra que o risco não se consolida como componente organizacional relevante quando permanece fora dos sistemas de controle e decisão. Em ambos os casos, a integração aparece como requisito de coerência institucional, e não como complemento acessório.

Nesses termos, a segurança não se estabiliza como dimensão estratégica enquanto estratégia e risco permanecerem dissociados. Sem essa convergência, o risco não alcança o nível superior com inteligibilidade suficiente, e a estratégia não incorpora, de modo maduro, as condições que podem limitar sua execução. Superar essa cisão requer articulação concreta entre segurança, compliance, negócio e liderança. É essa exigência de coordenação entre campos organizacionais que conduz à seção seguinte.

3.3 Segurança, compliance, negócio e liderança

A governança integrada da segurança exige superar leituras setoriais que isolam funções cuja efetividade depende de articulação recíproca. Quando segurança, compliance, negócio e liderança operam em circuitos paralelos, com prioridades pouco conectadas e fluxos informacionais incompletos, a organização perde capacidade de coordenação, e a resposta ao risco tende a assumir forma fragmentada.

Nessas condições, a segurança permanece confinada ao plano técnico, o compliance se restringe ao controle normativo, o negócio persegue metas dissociadas das exposições relevantes, e a liderança

passa a deliberar com informação tardia ou insuficientemente traduzida para a direção estratégica. O problema, portanto, não está na especialização dessas funções, mas na ausência de arranjos institucionais que conectem seus papéis em uma mesma lógica de orientação organizacional.

Essa desarticulação compromete a própria possibilidade de a segurança operar como dimensão estratégica. Quando proteção, conformidade, supervisão e objetivos organizacionais não são aproximados por estruturas de governança, a segurança perde densidade institucional e passa a depender de respostas parciais, setoriais e instáveis.

O NIST CSF 2.0 reforça esse deslocamento ao introduzir a função Govern como espaço em que estratégia, expectativas e política orientam a gestão do risco cibernético. Com isso, a segurança deixa de ocupar posição periférica e passa a integrar o centro da direção organizacional. Na mesma linha, os documentos de integração com enterprise risk management indicam que a liderança precisa receber informação suficiente para sustentar decisões de negócio informadas. Sem essa mediação, o conhecimento técnico produzido pela segurança não se converte em critério efetivo de decisão.

Nesse arranjo, a segurança cumpre funções de identificação, proteção, monitoramento e interpretação das vulnerabilidades que atravessam a organização. Sua atuação, contudo, perde alcance quando permanece dissociada do negócio e dos mecanismos formais de supervisão. O ponto decisivo não é negar sua especificidade técnica, mas impedir que essa especificidade justifique seu confinamento operacional. Quando isolada, a área técnica identifica o risco, mas a organização não o absorve como elemento estruturante da decisão.

O compliance também não deve ser tratado como instância concorrente da segurança. Sua função é complementar, pois atua na consolidação de padrões, na coerência dos processos e na redução

de assimetrias entre dever formal e prática organizacional. Quando segurança e compliance não dialogam, a organização dissocia proteção e conformidade, produzindo controles sem coordenação suficiente ou tratando exigências regulatórias como obrigação externa, e não como parte da integridade do sistema decisório.

Os princípios da OECD reforçam esse entendimento ao vincularem boa governança, direção estratégica, monitoramento da gestão e accountability do board. Nessa formulação, conformidade, supervisão e condução institucional não aparecem como esferas autônomas, mas como partes de um mesmo arranjo de coordenação.

A dimensão do negócio é igualmente constitutiva dessa integração. Tratar a segurança como tema externo ao negócio significa manter uma compreensão estreita da criação de valor, como se desempenho, continuidade, reputação e exposição institucional pudessem ser administrados separadamente. Essa dissociação empobrece a formulação estratégica e reduz a capacidade de avaliar objetivos organizacionais à luz das vulnerabilidades que podem comprometer sua realização. Nessa condição, a segurança tende a ser percebida como custo ou barreira, e não como condição de continuidade e confiança.

A liderança, por sua vez, ocupa posição de síntese institucional. Não lhe cabe substituir as funções técnicas, mas assegurar que segurança, compliance e negócio sejam traduzidos em orientação organizacional coerente. A literatura normativa recente desloca a liderança para esse ponto de convergência. Os princípios da OECD atribuem ao framework de governança a responsabilidade de assegurar direção estratégica, monitoramento da gestão e accountability do board. De modo convergente, a ISO/IEC 27014:2020 estabelece que a governança da segurança da informação envolve avaliar, dirigir, monitorar e comunicar os processos de segurança no âmbito do governing body e da alta administração.

Desse modo, a liderança não ocupa posição exterior ao problema. Ela integra o mecanismo pelo qual a segurança se converte em matéria de direção institucional. Quando essas quatro dimensões permanecem desarticuladas, a organização acumula respostas fragmentadas: a segurança identifica o risco sem tradução estratégica suficiente; o compliance controla sem integrar; o negócio decide sem incorporar adequadamente as exposições que condicionam sua sustentabilidade; e a liderança supervisiona sem fluxo coordenado entre informação, prioridade e resposta.

A governança integrada emerge, assim, como condição de superação dessa fragmentação. Isso não significa dissolver funções distintas, mas articular seus papéis, suas linguagens e seus critérios de atuação em uma mesma arquitetura decisória. É dessa exigência que decorre o próximo passo analítico: examinar os mecanismos concretos pelos quais essa coordenação se torna institucionalmente operável, isto é, os fluxos, as políticas e as estruturas de decisão que sustentam a integração entre áreas.

3.4 Fluxos, políticas e estruturas de decisão

A articulação entre segurança, compliance, negócio e liderança não produz efeitos institucionais consistentes quando permanece no plano declaratório. Em organizações complexas, a integração só se estabiliza quando se traduz em mecanismos capazes de ordenar a circulação de informações, definir critérios de encaminhamento e sustentar instâncias de deliberação. Sem esse suporte, a coordenação tende a depender de improvisações e arranjos descontínuos.

Por isso, a governança integrada não se reduz à presença formal de áreas ou funções especializadas. Seu conteúdo institucional reside na capacidade de transformar informação dispersa em orientação coordenada. É nesse plano que a integração

deixa de ser formulação genérica e passa a compor a estrutura efetiva de condução organizacional.

O NIST Cybersecurity Framework 2.0 reforça essa compreensão ao situar a função Govern como espaço de definição de estratégia, expectativas e políticas para orientar a gestão do risco cibernético. A governança, nesse sentido, não aparece como complemento da segurança, mas como dimensão diretiva que organiza prioridades, papéis e critérios institucionais de atuação. De modo convergente, os materiais de apoio do NIST insistem na clareza de papéis e responsabilidades e na necessidade de políticas organizacionais recorrentes e repetíveis. O ponto central é que a estabilidade da coordenação não pode depender da atuação isolada de agentes específicos.

Os fluxos ocupam posição decisiva nessa arquitetura. Sua função não é promover circulação burocrática de informação, mas assegurar que dados relevantes sobre vulnerabilidades, incidentes, exposição e prioridade cheguem aos níveis adequados da organização em tempo útil e com inteligibilidade suficiente para orientar resposta. Quando isso não ocorre, a informação pode até existir, mas deixa de produzir coordenação. A organização passa, então, a operar com conhecimento fragmentado, o que compromete priorização, supervisão e capacidade de resposta.

O NIST SP 1303 reforça esse ponto ao vincular a integração entre cyber risk e enterprise risk management à necessidade de fornecer à liderança informações adequadas para decisões organizacionais informadas. O fluxo, portanto, não constitui detalhe administrativo. Ele é a via pela qual o risco deixa de permanecer confinado à área técnica e passa a integrar o campo mais amplo da decisão institucional.

As políticas exercem função correlata. Seu papel não se limita a registrar exigências ou consolidar conformidade documental. Elas estabilizam diretrizes, prioridades, responsabilidades e critérios de atuação, reduzindo ambiguidades e diminuindo a dependência de

interpretações contingentes. Quando essa base comum inexiste, ou permanece apenas no plano formal, a coordenação oscila entre iniciativas desconectadas, e a coerência entre proteção, supervisão e resposta se enfraquece.

A ISO 31000 sustenta essa leitura ao afirmar que a gestão de riscos deve estar integrada à governança, à estratégia, ao planejamento, aos processos de reporte e às políticas da organização. A implicação é direta: o tratamento do risco não pode ser separado do desenho institucional que orienta a ação organizacional. Nessa perspectiva, a política funciona como mecanismo de alinhamento organizacional.

As estruturas de decisão conferem materialidade a esse arranjo. São elas que definem onde se delibera, quem prioriza, como temas críticos são escalonados e por quais instâncias a organização produz convergência entre análise, direção e execução. O ponto decisivo não está na existência nominal de comitês, fóruns ou linhas de reporte, mas na capacidade de essas estruturas permitirem que o risco seja absorvido de modo inteligível e tempestivo pelo processo decisório mais amplo.

Os Princípios de Governança Corporativa da OECD reforçam essa perspectiva ao associarem governança à direção estratégica da companhia, ao monitoramento efetivo da gestão e à accountability do board. Com isso, a estrutura de decisão deixa de aparecer como engrenagem periférica e passa a integrar o núcleo da condução organizacional.

O reporte ocupa posição intermediária entre fluxo e decisão. Sua função não é apenas transmitir dados, mas traduzir tecnicamente o risco em categorias compreensíveis para supervisão e deliberação. Uma organização pode dispor de informação abundante e, ainda assim, falhar decisoriamente quando não consegue converter conteúdo técnico em elementos relevantes para continuidade, reputação, conformidade, exposição e prioridade estratégica. Sem essa tradução, o risco permanece conhecido por

setores específicos, mas não se torna inteligível para a organização como totalidade.

A ausência desses mecanismos formais tende a produzir fragilidades recorrentes: descontinuidade de resposta, perda de informação entre áreas, baixa rastreabilidade decisória, desalinhamento entre supervisão e execução e dependência excessiva de iniciativas individuais. Nesses contextos, a coordenação deixa de ser atributo do sistema organizacional e passa a depender da competência contingente de pessoas ou equipes específicas.

Esse deslocamento reduz a maturidade institucional da segurança. Em vez de operar como dimensão integrada ao governo da organização, ela assume caráter episódico, vulnerável a assimetrias informacionais, falhas de priorização e instabilidade na qualidade das respostas. A governança integrada revela, assim, sua função mais ampla: permitir que a articulação entre áreas se converta em arranjo institucional estável, capaz de sustentar decisão, priorização e resposta ao longo do tempo.

Uma vez estabelecida essa base, o problema já não consiste apenas em conectar funções internas, mas em compreender como a integração entre áreas e ambientes amplia ou limita a maturidade organizacional da segurança. É esse deslocamento que conduz à próxima seção.

3.5 Integração entre áreas e ambientes

A segurança estratégica não se sustenta quando a organização observa o risco por compartimentos estanques. Em contextos organizacionais complexos, as exposições atravessam áreas, processos, sistemas, níveis decisórios e relações externas. Por isso, a governança integrada exige mais do que coordenação localizada. Ela depende de leitura transversal da organização e de seus ambientes de funcionamento.

Esse ponto é decisivo porque o risco não respeita fronteiras funcionais. Uma vulnerabilidade percebida na operação pode produzir impacto regulatório. Uma falha tecnológica pode comprometer continuidade, reputação e decisão de negócio. Um problema inicialmente tratado como questão técnica pode, em curto prazo, deslocar-se para o plano institucional. Quando a organização não reconhece essa transversalidade, tende a responder de modo parcial.

A integração, nesse sentido, não se realiza apenas dentro de cada área isoladamente. Ela requer conexão entre segurança, tecnologia, compliance, jurídico, auditoria, operação, negócio e liderança. Cada uma dessas instâncias observa o risco a partir de recortes específicos. A maturidade organizacional depende, justamente, da capacidade de articular esses recortes em uma leitura institucional coerente.

Essa exigência também alcança os diferentes níveis da organização. O ambiente estratégico, o nível tático e a dimensão operacional não podem funcionar como circuitos paralelos. Quando a decisão superior não dialoga com a execução, ou quando a operação produz informação sem absorção pelos níveis de supervisão, a organização perde continuidade analítica. Com isso, a resposta institucional torna-se descontínua.

A integração também precisa alcançar os ambientes tecnológicos e relacionais. Sistemas, serviços críticos, infraestrutura, fornecedores e parceiros não constituem periferia do risco organizacional. Em muitas estruturas, eles integram a própria condição de funcionamento da atividade principal. Ignorar essas dependências significa preservar pontos cegos no interior da governança.

Isso não significa transformar terceiros em eixo autônomo da seção. O ponto central é outro. A organização precisa compreender que sua capacidade de proteção, resposta e continuidade não se encerra em seus limites formais. Em contextos de alta

interdependência, a maturidade institucional depende de reconhecer que parte relevante do risco se distribui por conexões externas e por relações de dependência tecnológica e operacional.

A integração entre áreas e ambientes também possui dimensão institucional. Exigências regulatórias, controles, supervisão e continuidade organizacional não podem ser tratados como temas paralelos. Quando essas frentes operam sem aproximação suficiente, a organização produz incoerência entre aquilo que protege, aquilo que monitora, aquilo que reporta e aquilo que efetivamente prioriza. A desconexão entre esses planos fragiliza a governança.

Quando essas conexões falham, surgem efeitos recorrentes. Entre eles, destacam-se a visão parcial do risco, a formação de pontos cegos institucionais, a baixa coordenação entre resposta e decisão e a transferência desordenada de responsabilidades. Em vez de operar com leitura integrada, a organização passa a deslocar problemas entre áreas sem consolidar encaminhamentos consistentes.

Essa lógica também produz descontinuidade entre proteção, supervisão e operação. A área técnica pode identificar vulnerabilidades sem que isso gere priorização institucional. A liderança pode demandar controle sem compreender integralmente as exposições envolvidas. A operação pode executar respostas sem alinhamento suficiente com critérios mais amplos de risco, conformidade e continuidade. O efeito agregado é a fragilidade da maturidade organizacional.

A leitura estratégica da segurança exige justamente a superação dessa fragmentação. A segurança só se consolida como dimensão estratégica quando a organização reconhece o risco como fenômeno transversal. Isso significa abandonar a ideia de que cada setor controla apenas sua parcela isolada de exposição. O risco precisa ser compreendido como elemento que atravessa a arquitetura organizacional e exige coordenação entre suas partes.

Nessa perspectiva, a integração não é valor abstrato nem fórmula administrativa genérica. Ela constitui exigência institucional da governança. Sem ela, a organização pode até reunir áreas especializadas, políticas formais e estruturas decisórias. Ainda assim, permanecerá vulnerável à dispersão, porque lhe faltará articulação suficiente para transformar essas partes em sistema coerente.

A maturidade da segurança estratégica depende, portanto, da passagem da fragmentação para a integração institucional. É nesse movimento que governança, risco, conformidade, negócio e decisão deixam de operar como domínios separados e passam a compor uma arquitetura organizacional coerente. Com isso, encerra-se o percurso deste capítulo: a segurança sem governança tende à reatividade, enquanto a governança integrada cria as condições institucionais pelas quais a segurança pode, de fato, operar em chave estratégica.

Considerações Finais

O percurso desenvolvido neste capítulo permitiu demonstrar que a segurança estratégica não se sustenta sem governança integrada. A responsabilidade institucional, embora indispensável, permanece insuficiente quando não é acompanhada por mecanismos capazes de articular áreas, estruturas, fluxos e instâncias de decisão. Em organizações complexas, a segurança deixa de operar como dimensão estratégica quando a coordenação institucional falha.

A análise mostrou, inicialmente, que a falta de governança integrada constitui causa organizacional relevante da fragilidade da segurança. Esse problema não se reduz à ausência de normas ou à deficiência de áreas específicas. Seu núcleo reside na fragmentação institucional que impede a conversão de informações, responsabilidades e capacidades em direção organizacional coerente.

Na sequência, verificou-se que a separação entre estratégia e risco aprofunda essa fragilidade. Quando a formulação estratégica ocorre dissociada da leitura das exposições envolvidas, a organização tende a decidir de forma parcial, a responder de modo reativo e a comprometer a maturidade de sua própria supervisão institucional. O risco, nesse contexto, deixa de orientar a estratégia e reaparece tardiamente como fator de descontinuidade.

O capítulo também evidenciou que segurança, compliance, negócio e liderança não podem operar como campos paralelos. A fragmentação entre essas dimensões empobrece a coordenação organizacional, dificulta a tradução do risco para a decisão e reduz a capacidade de integrar proteção, conformidade, prioridade executiva e continuidade institucional. A segurança só adquire densidade estratégica quando essas instâncias passam a funcionar de forma articulada.

Do mesmo modo, ficou demonstrado que a governança integrada depende de sua materialização em fluxos, políticas e estruturas de decisão. Sem esses suportes formais, a coordenação entre áreas tende a permanecer instável, sujeita a descontinuidades, perdas de informação e dependência excessiva de iniciativas individuais. A maturidade institucional da segurança exige, portanto, arranjos estáveis que sustentem encaminhamento, supervisão e resposta.

Por fim, a análise da integração entre áreas e ambientes permitiu mostrar que o risco atravessa fronteiras funcionais, tecnológicas e organizacionais. Quando a organização o observa de maneira compartimentada, surgem pontos cegos institucionais, baixa coordenação e fragilidade na relação entre proteção, supervisão e operação. A segurança estratégica depende, assim, de uma leitura transversal da organização e de suas dependências.

O ganho conceitual do capítulo está justamente nesse deslocamento. A governança não foi tratada como linguagem genérica de controle nem como repertório abstrato de boas práticas.

Ela apareceu como arranjo institucional de coordenação, capaz de conectar supervisão, decisão, risco, conformidade e objetivos organizacionais em uma arquitetura coerente. É essa coordenação que retira a segurança da periferia e a reinscreve no centro da direção institucional.

Dessa forma, o capítulo demonstrou que a passagem da fragmentação para a integração constitui condição da segurança estratégica. Sem articulação entre estruturas, áreas e ambientes, a organização tende à dispersão, à reatividade e à baixa maturidade institucional. Com governança integrada, ao contrário, torna-se possível transformar responsabilidade dispersa em direção organizacional consistente.

Uma vez estabelecida essa necessidade de coordenação institucional, o passo seguinte consiste em examinar como a organização enfrenta o problema da assunção do risco. Isso porque, depois de demonstrar quem coordena e por quais mecanismos essa coordenação se realiza, torna-se necessário compreender de que modo o risco é delimitado, enfrentado e institucionalmente tratado no interior da decisão organizacional.

CAPÍTULO IV

ASSUNÇÃO DE RISCO: DA PERCEPÇÃO TÉCNICA À DECISÃO ESTRATÉGICA

Introdução

Uma vez demonstrado que a segurança não pode permanecer restrita ao plano técnico, que a responsabilidade decisória requer formalização e que a governança precisa integrar áreas, fluxos e estruturas de supervisão, impõe-se um problema subsequente: de que modo a organização reconhece o risco como objeto legítimo de decisão. Nesse estágio, a maturidade institucional já não depende somente de coordenação ou clareza de papéis. Ela passa a depender da capacidade de avaliar exposições, estabelecer limites, traduzir impactos e assumir escolhas compatíveis com os objetivos organizacionais.

Assumir risco, nesse contexto, não equivale a normalizar falhas nem a admitir vulnerabilidades de modo passivo. O que se afirma é algo distinto: organizações maduras não tratam o risco como anomalia externa ao processo decisório, mas como realidade inerente ao funcionamento institucional, que precisa ser reconhecida, qualificada e enfrentada com critérios consistentes. Essa mudança de estatuto permite converter sinais técnicos dispersos em linguagem executiva, aproximando segurança, continuidade, conformidade, reputação e capacidade de resposta em um mesmo campo decisório.

Nessa direção, o capítulo desenvolve cinco movimentos encadeados. Primeiro, define o risco como categoria de gestão. Em seguida, examina a passagem da ameaça técnica ao risco de negócio. Depois, discute a assunção do risco como dimensão da tomada de decisão. Na sequência, analisa falhas decisórias produzidas pela ausência de avaliação qualificada. Por fim, apresenta a prevenção, a

resiliência e a sustentabilidade como respostas institucionais mais compatíveis com contextos de elevada exposição.

4.1 O risco como categoria de gestão

O risco deixa de ocupar posição periférica quando seus efeitos alcançam objetivos, continuidade e capacidade de execução. Nessa condição, ele deixa de ser percebido como evento isolado e passa a integrar a linguagem da gestão. A ISO 31000:2018 organiza esse entendimento ao tratar o risco como efeito da incerteza sobre os objetivos e ao defender sua integração à governança, à estratégia, ao planejamento, à gestão e à cultura organizacional.

Essa compreensão altera o modo pelo qual a segurança é enquadrada nas organizações. Quando o risco é lido somente pela chave da vulnerabilidade técnica, a tendência é tratá-lo como problema operacional, restrito ao controle de incidentes e à correção de falhas. Entretanto, quando a organização reconhece que exposições relevantes podem comprometer objetivos mais amplos, o risco passa a orientar avaliação, priorização, monitoramento e resposta.

É nesse sentido que os materiais recentes do NIST vinculam o gerenciamento do risco cibernético ao enterprise risk management e destacam o uso de linguagem comum para integrar monitoramento, avaliação e ajuste entre diferentes unidades e programas organizacionais. A consequência mais relevante dessa mudança está no fato de que o risco já não aparece como desvio externo, mas como elemento constitutivo da deliberação institucional.

Por isso, o risco não deve ser concebido como algo a ser integralmente eliminado. Tal expectativa não corresponde ao funcionamento real de organizações complexas. Em vez disso, ele deve ser tratado como condição a ser administrada segundo limites, prioridades e capacidade institucional de resposta. É nesse ponto

que a noção de apetite ao risco ganha relevância, pois permite articular risco, estratégia e objetivos sem confundir prudência com paralisia.

Tratar o risco como categoria de gestão significa, assim, reconhecê-lo como componente normal da deliberação estratégica. Não se trata de abandonar controles, nem de reduzir a segurança a cálculo econômico. Trata-se de admitir que toda organização opera sob incerteza, define prioridades sob restrições e escolhe caminhos em contextos de exposição variável.

4.2 Da ameaça técnica ao risco de negócio

Enquanto a ameaça técnica é percebida como falha localizada, o risco de negócio exige leitura mais ampla. Ele envolve continuidade operacional, reputação, conformidade, finanças e capacidade de resposta. Por isso, sua avaliação não pode permanecer restrita ao vocabulário da tecnologia. Ela precisa ingressar no campo da decisão organizacional.

O NIST CSF 2.0 reforça essa mudança ao incluir a função GOVERN em sua estrutura. Com isso, a gestão do risco cibernético deixa de se concentrar somente em proteção e resposta. Ela passa a envolver contexto organizacional, prioridades, supervisão e integração com a gestão corporativa de riscos.

Essa transição altera o estatuto do problema. Uma vulnerabilidade técnica, isoladamente, pode parecer assunto operacional. Contudo, quando essa exposição alcança ativos críticos, processos essenciais ou compromissos regulatórios, ela assume relevância estratégica. Nesse ponto, o risco já não pertence exclusivamente à área técnica.

O IBGC sustenta essa leitura ao destacar que a cibersegurança deve integrar a agenda do conselho e da alta liderança. A formulação é relevante porque desloca o tema do plano reativo para o plano

deliberativo. O risco passa, então, a ser tratado como matéria de governança e não apenas como questão especializada.

Quando isso não ocorre, a organização tende a fragmentar a percepção da exposição. A área técnica enxerga falhas, mas a direção não percebe seus impactos em valor, continuidade e credibilidade. O resultado é uma assimetria entre a linguagem do evento e a linguagem da decisão.

Converter ameaça técnica em risco de negócio, portanto, não significa ampliar o medo institucional. Significa traduzir a exposição em termos compreensíveis para quem define prioridades, limites e respostas. Sem essa tradução, o risco existe, mas não se torna inteligível para a decisão estratégica.

4.3 Assunção de risco e tomada de decisão

Assumir risco, no plano organizacional, não significa tolerar falhas de forma passiva. Significa reconhecer que a decisão estratégica ocorre sob condições de incerteza. Por isso, a maturidade institucional não se mede pela pretensão de eliminar toda exposição, mas pela capacidade de avaliá-la e delimitá-la com critério.

Nesse contexto, o apetite ao risco exerce função decisória relevante. Ele permite estabelecer até que ponto determinada exposição pode ser aceita sem comprometer objetivos, continuidade e posicionamento institucional. Sua utilidade está em impedir que a organização oscile entre a negação do risco e a reação desproporcional diante dele. A COSO (2020) trata o risk appetite como parte integrante da tomada de decisão e o vincula às estratégias e aos objetivos organizacionais.

Essa formulação é importante porque desloca o risco do plano meramente técnico para o plano da escolha institucional. A questão já não consiste em saber se há exposição, mas em definir qual exposição é aceitável, em quais condições e com quais

contrapartidas. A decisão passa, então, a depender menos de improviso e mais de parâmetros de julgamento.

Crawford e Jabbour (2024) observam que o enterprise risk management tende a qualificar o julgamento gerencial em contextos complexos. O ganho, nesse caso, não está na promessa de previsibilidade total, mas na criação de condições para decisões mais consistentes, sobretudo quando a organização precisa escolher entre prioridades concorrentes, recursos limitados e cenários mutáveis.

Por essa razão, a assunção de risco deve ser compreendida como ato de deliberação estratégica. Ela exige linguagem comum, critérios comparativos e capacidade de traduzir sinais dispersos em decisões justificáveis. Sem esse trabalho de qualificação, o risco pode até ser percebido, mas não se converte em escolha institucional madura.

4.4 Falhas decisórias sem avaliação de risco

As falhas decisórias não decorrem, em primeiro lugar, da mera existência do risco. Elas se agravam quando a organização decide sem avaliação qualificada da exposição que enfrenta. Nessa condição, o problema não está somente no evento adverso, mas na precariedade dos critérios usados para priorizar, comparar e responder.

Quando o risco não é suficientemente avaliado, a organização tende a operar com percepção fragmentada. Alguns sinais são captados pela área técnica, outros permanecem invisíveis para a liderança, e outros ainda não recebem tratamento proporcional à sua materialidade. O resultado costuma ser uma deliberação instável, incapaz de distinguir com clareza o que exige resposta imediata, o que demanda monitoramento e o que pode ser assumido dentro de limites toleráveis.

Essa leitura é coerente com a orientação do NIST (2024), segundo a qual a integração do risco cibernético ao gerenciamento

corporativo exige monitoramento, avaliação e ajuste entre diferentes unidades e programas organizacionais. Sem essa base comum, a decisão passa a depender de leituras parciais, muitas vezes insuficientes para sustentar escolhas consistentes.

A crítica recente de Slapničar, Axelsen e Eulerich (2025) aprofunda essa dificuldade ao mostrar que abordagens ditas baseadas em risco frequentemente enfrentam limitações de mensuração, comparação e priorização. Em outras palavras, a linguagem do risco pode estar presente, mas isso não garante que a organização disponha de um processo decisório capaz de distinguir exposições e definir respostas com precisão.

Nessas circunstâncias, instala-se uma ilusão de controle. A organização acredita que está gerindo o risco porque o nomeia, o reporta ou o classifica, mas não necessariamente o transforma em critério efetivo de deliberação. O efeito prático dessa deficiência aparece na forma de respostas tardias, priorizações imprecisas e dificuldade de sustentar continuidade diante de cenários adversos.

Por isso, a avaliação de risco não constitui etapa acessória do processo decisório. Ela representa a condição pela qual a exposição se torna inteligível para a gestão. Sem essa base, a decisão pode até ocorrer com rapidez, mas dificilmente alcançará consistência estratégica.

4.5 Modelos preventivos, resilientes e sustentáveis

Modelos preventivos, resilientes e sustentáveis partem do reconhecimento de que o risco não desaparece. O que se altera é a capacidade institucional de antecipar impactos, reduzir vulnerabilidades e sustentar continuidade. Nesse sentido, prevenir não significa prometer invulnerabilidade, mas estruturar respostas compatíveis com a exposição existente.

A ISO 22301:2019 oferece base importante para essa compreensão ao tratar a continuidade de negócios como sistema de

gestão. Sua ênfase recai sobre planejamento, implementação, monitoramento, revisão e melhoria contínua, com o objetivo de proteger a organização, reduzir a probabilidade de incidentes disruptivos e assegurar a recuperação quando eles ocorrerem.

Essa perspectiva amplia o tratamento do risco. Em vez de concentrar esforços somente na contenção do evento, a organização passa a estruturar capacidade de resposta antes, durante e depois da disrupção. A prevenção, assim, deixa de ser medida isolada e passa a integrar uma arquitetura institucional orientada à permanência operacional.

Monazzam e Crawford (2024), ao examinarem a relação entre enterprise risk management e resiliência organizacional, mostram que essa capacidade não decorre de improviso. Ela se apoia em elementos como governança de risco, cultura de risco, artefatos de risco e consciência institucional, que tornam a organização mais apta a responder de forma coordenada a contextos adversos.

Esse ponto é relevante porque impede que a resiliência seja tratada como qualidade abstrata. Ela depende de estruturas, rotinas e práticas que tornem o risco inteligível e administrável. Sem esse lastro, a organização pode até reagir a eventos críticos, mas dificilmente sustentará continuidade com consistência.

Marc, Arena e Peljhan (2023) aprofundam essa discussão ao mostrar que a efetividade dos sistemas de gestão de riscos depende também do modo como são utilizados. Não basta dispor de modelos avançados ou de instrumentos formais. É necessário que esses sistemas sejam usados de forma interativa, de modo a informar decisões, circular conhecimento e ajustar respostas diante de mudanças relevantes no ambiente organizacional.

A dimensão da sustentabilidade institucional também se conecta a esse raciocínio. Organizações expostas a cenários voláteis não preservam sua estabilidade por mera repetição de controles. Elas precisam desenvolver capacidade adaptativa, leitura contínua

do ambiente e critérios para recompor prioridades quando a exposição se altera.

O diagnóstico recente do World Economic Forum reforça a atualidade desse problema ao indicar que 84% das empresas se consideram despreparadas para futuras disrupções. Esse dado evidencia que a vulnerabilidade contemporânea não decorre somente da intensidade das ameaças, mas também da dificuldade institucional de convertê-las em prevenção estruturada, resiliência prática e continuidade sustentável.

Por isso, modelos preventivos, resilientes e sustentáveis não representam etapa acessória da gestão do risco. Eles constituem a forma mais desenvolvida de sua assunção estratégica. Quando a organização reconhece limites, prepara respostas e organiza sua continuidade, o risco passa a ser tratado como realidade permanente da decisão institucional.

Considerações finais

O desenvolvimento deste capítulo permitiu demonstrar que o risco, no contexto organizacional contemporâneo, não pode ser reduzido à condição de evento excepcional ou de falha meramente técnica. À medida que afeta objetivos, continuidade, reputação e capacidade de resposta, ele passa a integrar o campo da gestão e da decisão estratégica. Nessa perspectiva, reconhecê-lo constitui exigência de maturidade institucional, e não sinal de fragilidade.

Ao longo das seções, observou-se que a passagem da ameaça técnica ao risco de negócio depende de tradução organizacional, critérios de avaliação e linguagem compatível com a deliberação executiva. O apetite ao risco, tal como indicado pela COSO (2020), permite delimitar exposições aceitáveis e vincular risco, estratégia e objetivos. De modo convergente, Crawford e Jabbour (2024) indicam que estruturas de gestão de riscos tendem a qualificar o

julgamento gerencial em cenários complexos, reforçando a necessidade de decisão fundamentada.

Também se evidenciou que a fragilidade decisória não decorre somente da presença do risco, mas da ausência de avaliação qualificada. Sem critérios de comparação, priorização e monitoramento, a organização pode nomear exposições sem efetivamente convertê-las em base consistente para a escolha. Nesse ponto, a crítica de Slapničar, Axelsen e Eulerich (2025) é elucidativa ao mostrar que abordagens ditas baseadas em risco podem conservar limitações relevantes de mensuração e alinhamento decisório.

Por fim, os modelos preventivos, resilientes e sustentáveis mostraram que a assunção estratégica do risco não se esgota na identificação da exposição. Ela exige preparação institucional para antecipar impactos, sustentar continuidade e reorganizar respostas diante de cenários adversos. A ISO 22301:2019 e os achados de Monazzam e Crawford (2024) reforçam que prevenção e resiliência dependem de estruturas permanentes, e não de improvisação circunstancial. Assim, o risco passa a constituir elemento legítimo da racionalidade organizacional.

CAPÍTULO V

APLICANDO O MÉTODO RGA: DIAGNÓSTICO ESTRATÉGICO, CASOS CRÍTICOS E SOLUÇÕES REPLICÁVEIS

Introdução

Este capítulo tem por finalidade demonstrar a aplicabilidade do Método RGA em situações concretas de risco, falhas de governança e decisões estratégicas mal calibradas. Mais do que um modelo interpretativo, o método se apresenta como ferramenta replicável de diagnóstico, análise causal e orientação decisória, em consonância com o escopo da obra, que reserva ao capítulo final a transformação do modelo em instrumento prático de uso organizacional.

A contribuição do Método RGA reside em sua capacidade de articular, em uma mesma estrutura de leitura, problema, causa organizacional, interpretação estratégica e resposta aplicável. Essa arquitetura permite que eventos críticos deixem de ser tratados como episódios isolados e passem a ser examinados como manifestações de fragilidades institucionais identificáveis, comparáveis e corrigíveis. Nessa perspectiva, o valor do método não se limita à análise retrospectiva. Ele também favorece prevenção, priorização e amadurecimento decisório.

Ao propor uma matriz que integra responsabilidade, governança e assunção de risco em chave operacional, o autor oferece uma contribuição metodológica com utilidade prática e potencial de aplicação em diferentes contextos organizacionais. O diferencial da proposta não está em descrever ferramentas técnicas de segurança, mas em reorganizar o tema em linguagem institucional, estratégica e decisória, convertendo vulnerabilidades dispersas em critérios mais consistentes de avaliação e ação. É com

essa finalidade que o capítulo examina casos críticos, identifica causas recorrentes e extrai soluções replicáveis.

5.1 Como diagnosticar a maturidade estratégica da segurança

O diagnóstico da maturidade estratégica da segurança exige critério que vá além da verificação de controles isolados. O ponto central consiste em identificar se a organização já trata a segurança como tema integrado à governança, ao risco e à decisão. Nessa perspectiva, maturidade não se confunde com quantidade de ferramentas, mas com a qualidade institucional da coordenação, da priorização e da resposta.

O NIST SP 1302 oferece base adequada para esse diagnóstico ao afirmar que os CSF Tiers podem caracterizar o rigor da governança de risco cibernético e dos resultados da gestão. Isso é particularmente útil para o Método RGA porque permite avaliar não só a existência de práticas, mas o grau em que elas já se tornaram consistentes, repetíveis e estrategicamente orientadas.

Nesse sentido, o diagnóstico não deve começar pela pergunta sobre qual tecnologia a organização possui. A questão mais relevante é outra: como o risco é percebido, distribuído, monitorado e incorporado à deliberação. Quando essa leitura é frágil, a segurança tende a permanecer fragmentada, reativa e dependente de respostas episódicas.

A contribuição do Método RGA, aqui, está em transformar essa avaliação em sequência inteligível. Primeiro, identifica-se o problema visível. Em seguida, examinam-se suas causas institucionais. Depois, qualifica-se o risco envolvido e, por fim, definem-se respostas e soluções replicáveis. Com isso, o diagnóstico deixa de ser fotografia estática e passa a funcionar como instrumento de decisão.

Os Cybersecurity Performance Goals da CISA reforçam essa lógica ao se apresentarem como práticas voluntárias de alto impacto,

concebidas tanto como linha de base quanto como referência para medir e melhorar a maturidade cibernética. Para o capítulo, isso é valioso porque fornece parâmetros mínimos de comparação sem transformar a análise em checklist mecânico.

Sob essa ótica, uma organização com baixa maturidade tende a exibir responsabilização difusa, pouca integração entre áreas, resposta tardia e ausência de critérios claros de priorização. Em nível intermediário, já se observam práticas formais, mas ainda com fragmentação entre governança, operação e decisão. Em maior maturidade, a segurança passa a ser tratada como matéria estratégica, com linguagem comum, supervisão consistente e capacidade de ajuste diante de novos cenários.

O NIST SP 800-61r3 fortalece essa leitura ao integrar resposta a incidentes ao gerenciamento do risco cibernético em alinhamento com o CSF 2.0. Essa aproximação é importante porque mostra que maturidade não pode ser medida só pela prevenção. Ela também depende da capacidade de detectar, responder, recuperar e aprender institucionalmente com eventos críticos.

Desse modo, diagnosticar a maturidade estratégica da segurança significa examinar a organização em quatro planos articulados: clareza de responsabilidades, integração de governança, qualidade da avaliação de risco e prontidão de resposta. Essa articulação confere ao Método RGA valor prático elevado, pois permite converter sinais dispersos em leitura estruturada, comparável e orientada à decisão.

5.2 Caso 1: vazamento de dados e responsabilidade difusa

O caso Equifax tornou-se exemplar porque o vazamento de dados não decorreu de uma única falha isolada, mas de uma combinação entre vulnerabilidade conhecida, execução deficiente e responsabilização mal distribuída. A Federal Trade Commission, FTC (2019), sustentou que a empresa deixou de adotar medidas

razoáveis de segurança e não garantiu a correção de uma vulnerabilidade crítica, o que contribuiu para uma violação que afetou aproximadamente 147 milhões de pessoas.

A gravidade institucional do caso aparece com mais nitidez no relatório da House Committee on Oversight and Government Reform (2018). O documento concluiu que a violação era evitável e apontou falta de accountability e ausência de linhas claras de autoridade na estrutura interna de tecnologia da informação. Não se tratava, portanto, de mera insuficiência técnica, mas de um ambiente em que política, comando e execução não operavam de forma coerente.

A decomposição analítica do episódio permite distinguir quatro planos. Primeiro, o evento crítico, isto é, a exposição massiva de dados pessoais. Depois, a causa organizacional, ligada à ausência de linhas claras de autoridade. Em seguida, a leitura estratégica, que revela a distância entre comando formal e efetividade institucional. Por fim, a resposta replicável, que exige atribuição inequívoca de responsabilidades, acompanhamento da execução e mecanismos de verificação compatíveis com a materialidade do risco.

O ganho analítico do método, nesse caso, consiste em impedir que o episódio seja reduzido à narrativa do incidente técnico. O vazamento passa a ser compreendido também como expressão de fragilidade decisória e de baixa maturidade organizacional. Ao reorganizar um evento amplamente conhecido em chave institucional, o RGA evidencia seu potencial de replicação diagnóstica.

5.3 Caso 2: falhas de governança e fragmentação institucional

O caso Marriott-Starwood é particularmente relevante porque evidencia que falhas de segurança podem persistir quando a governança não consegue integrar estruturas, sistemas e responsabilidades. A Federal Trade Commission, FTC (2024a),

afirmou que, após a aquisição da Starwood em 2016, a Marriott passou a responder pelas práticas de segurança das duas marcas, mas falhas relevantes de proteção permaneceram ativas e contribuíram para múltiplas violações de dados.

Segundo a FTC (2024a), as empresas deixaram de implementar controles adequados de senha, acesso, segmentação de rede, atualização de sistemas, registro e monitoramento de ambientes, além de autenticação multifator suficiente. Essas insuficiências não devem ser lidas como lacunas técnicas isoladas. Em conjunto, elas revelam dificuldade de coordenação e baixa capacidade de integrar governança, operação e supervisão em ambiente institucional complexo.

O elemento mais expressivo do episódio está na duração e na extensão dos efeitos da fragmentação. A FTC registrou que uma das violações começou em 2014 e só foi detectada em 2018, com acesso indevido a 339 milhões de registros de hóspedes Starwood em todo o mundo, inclusive 5,25 milhões de números de passaporte não criptografados. Em dezembro de 2024, a Comissão finalizou ordem exigindo programa abrangente de segurança, após concluir que as falhas afetaram mais de 344 milhões de clientes globalmente.

Quando examinado em perspectiva institucional, o caso mostra que o problema visível consiste nas violações reiteradas de dados, ao passo que a causa mais profunda se instala na fragmentação da governança, que impediu a harmonização efetiva de controles, responsabilidades e rotinas de supervisão. O risco, nesse cenário, não se resume ao incidente técnico. Ele se manifesta na incapacidade organizacional de transformar integração formal em coordenação concreta.

O diferencial do método se evidencia ao mostrar que a fragilidade institucional não decorre somente da existência de sistemas herdados. O ponto decisivo está na ausência de estrutura capaz de unificar comando, critérios e monitoramento em uma arquitetura coerente de decisão. Com isso, o episódio deixa de ser

lido como falha pós-aquisição e passa a operar como diagnóstico de maturidade estratégica insuficiente.

5.4 Caso 3: ataque cibernético e decisão tardia

O caso Colonial Pipeline tornou-se paradigmático porque revelou como um ataque cibernético pode ultrapassar o plano técnico e atingir rapidamente a continuidade de serviços essenciais. O Department of Energy registrou que, em 7 de maio de 2021, a empresa desligou proativamente seu sistema de dutos em resposta ao ataque de ransomware e que a retomada integral das operações foi anunciada em 13 de maio de 2021.

A dimensão institucional do episódio não está somente no ataque, mas na forma como ele expôs a dependência sistêmica da infraestrutura crítica. CISA observou, dois anos depois, que o incidente tornou a vulnerabilidade da sociedade altamente conectada uma realidade nacional visível, com efeitos concretos sobre abastecimento e vida cotidiana. O caso, portanto, não pode ser lido como interrupção localizada, mas como falha com repercussão ampliada.

Outro aspecto decisivo do episódio está no peso da prontidão insuficiente diante de ameaças já conhecidas. Em 11 de maio de 2021, CISA e FBI divulgaram advisory conjunto sobre o ransomware DarkSide, a variante usada recentemente contra uma empresa de infraestrutura crítica, enfatizando que a prevenção continua sendo a defesa mais eficaz e recomendando revisão imediata de práticas de fortalecimento da postura cibernética.

Aplicado a esse caso, o método permite distinguir o ataque e a interrupção operacional como manifestação visível de um problema mais profundo: a insuficiência da preparação estratégica para responder com maior robustez a uma exposição de alta criticidade. Quando a resposta depende de interrupção ampla,

pressão externa e reação acelerada, o caso indica que o risco já existia em nível superior ao da mera falha técnica.

A força explicativa do RGA aparece quando a decisão tardia deixa de ser entendida apenas como demora cronológica. O atraso passa a ser percebido como descompasso entre a relevância do risco e o nível prévio de antecipação, integração e prontidão institucional. Com isso, Colonial Pipeline deixa de ser apenas narrativa de ransomware e se converte em leitura de criticidade, dependência sistêmica e maturidade decisória.

5.5 Caso 4: decisão estratégica sem avaliação de risco

O caso Drizly é particularmente expressivo porque evidencia uma decisão organizacional tomada sem avaliação compatível com a exposição já conhecida. A Federal Trade Commission, FTC (2022), afirmou que a empresa e seu CEO, James Cory Rellas, haviam sido alertados para problemas de segurança dois anos antes da violação de 2020, mas não adotaram medidas suficientes para proteger os dados dos consumidores. A falha, portanto, não pode ser compreendida como surpresa absoluta, mas como risco previamente sinalizado e insuficientemente tratado.

Segundo a FTC (2022), a empresa deixou de implementar salvaguardas básicas, como autenticação em dois fatores para o GitHub, limitação adequada de acesso a dados pessoais, políticas escritas de segurança e treinamento correspondente para os empregados. Também manteve credenciais e informações sensíveis em ambiente inadequado, além de não designar supervisão executiva suficiente para assegurar a proteção dos dados. Esses elementos mostram que o problema não estava na ausência total de informação, mas na fragilidade da decisão diante de um risco já conhecido.

A leitura institucional do episódio mostra que a violação, que expôs dados pessoais de cerca de 2,5 milhões de consumidores, foi

precedida por sinais que não foram convertidos em priorização, investimento e ação corretiva. Nessa condição, o risco deixa de ser apenas técnico e passa a revelar falha de julgamento estratégico.

O alcance do caso cresce porque a ordem final da FTC não se limitou à empresa. Em janeiro de 2023, a Comissão finalizou a ordem e vinculou Rellas a obrigações de segurança também em futuras empresas, caso volte a ocupar posições de controle ou liderança em negócios que coletem dados de consumidores em escala relevante. Essa consequência mostra que a omissão decisória pode ultrapassar a organização original e alcançar a própria trajetória executiva de seus dirigentes.

O valor operacional do RGA torna-se nítido quando o episódio é reorganizado em termos de problema, causa, risco qualificado e resposta necessária. Decisões inadequadas deixam de aparecer como recusa explícita e passam a ser compreendidas também como inércia, subestimação ou tratamento insuficiente de alertas prévios. Desse modo, omissões dispersas assumem contorno institucional claro e passível de replicação analítica.

5.6 Síntese executiva do Método RGA

Os casos examinados ao longo deste capítulo demonstraram que o Método RGA possui capacidade consistente de reorganizar eventos críticos em uma estrutura analítica clara. Em vez de limitar a leitura ao incidente visível, o método permite identificar a causa institucional predominante, qualificar o risco em chave estratégica e projetar respostas aplicáveis a contextos distintos. Com isso, situações diversas, como vazamento de dados, fragmentação de governança, resposta tardia e omissão decisória, passam a ser compreendidas por meio de uma lógica comum de diagnóstico.

A principal vantagem prática do RGA está nessa capacidade de converter complexidade em critério de decisão. O método não se limita a descrever falhas nem a enumerar boas práticas. Sua

utilidade reside em oferecer uma sequência de leitura que torna o problema inteligível, comparável e operacionalizável, favorecendo tanto a análise do caso concreto quanto a formulação de soluções replicáveis em outras realidades organizacionais.

É nesse ponto que a contribuição autoral se torna mais evidente. Ao formular uma matriz própria que articula risco, governança e ação em linguagem estratégica, o autor oferece mais do que uma interpretação dos casos analisados. Oferece um instrumento metodológico com valor diagnóstico, aplicabilidade prática e potencial de replicação, capaz de ampliar a maturidade institucional da segurança e de qualificar o tratamento organizacional de eventos críticos.

CONCLUSÃO

Ao longo desta obra, demonstrou-se que a segurança organizacional já não pode ser compreendida como função periférica, confinada ao plano técnico ou subordinada à lógica restrita do suporte operacional. Em ambientes marcados por interdependência digital, pressão regulatória, exposição reputacional e sensibilidade crescente da continuidade institucional, a segurança deixa de ocupar posição acessória e passa a integrar o próprio núcleo da direção organizacional.

O problema central, portanto, jamais residiu unicamente na existência de falhas técnicas. Seu ponto mais profundo sempre esteve na incapacidade de muitas organizações de reconhecer que risco, decisão, responsabilidade e governança pertencem ao mesmo campo institucional. Essa foi a pergunta que orientou o livro desde o início: como transformar a segurança, historicamente tratada como função técnica, operacional ou centro de custo, em eixo estruturante da estratégia organizacional, com governança integrada, responsabilidade formal e decisão orientada por risco.

A resposta construída ao longo dos capítulos conduz a uma afirmação central: a maturidade institucional da segurança emerge quando a organização deixa de administrar vulnerabilidades como episódios fragmentados e passa a tratá-las como matéria de direção, supervisão e escolha estratégica. Essa passagem exigiu demonstrar, em primeiro lugar, que a segurança ultrapassou definitivamente a condição de tema setorial; em seguida, que nenhuma estratégia de proteção se sustenta sem definição objetiva de responsabilidade; depois, que a responsabilidade, por si só, permanece insuficiente quando não é acompanhada por governança integrada; e, por fim, que a própria governança se torna incompleta quando o risco não é traduzido em linguagem executiva e assumido com critério.

O itinerário do livro confirma, assim, a hipótese argumentativa definida no escopo: organizações que mantêm a segurança apartada da estratégia tendem a ampliar vulnerabilidades institucionais, dispersar responsabilidades e comprometer continuidade, reputação e conformidade, ao passo que organizações que integram segurança à governança e à decisão estratégica desenvolvem maior resiliência, capacidade preventiva e maturidade institucional.

É precisamente nesse ponto que o Método RGA se consolida como a principal contribuição autoral da obra. Sua originalidade não decorre de proclamação abstrata, mas da forma pela qual reorganiza o debate sobre segurança em chave institucional, estratégica e decisória, conforme previsto no diferencial competitivo do livro. O método oferece uma matriz própria para examinar problemas organizacionais por meio da articulação entre Responsabilidade, Governança e Assunção de risco, transformando exposições dispersas em estrutura inteligível de diagnóstico, interpretação e resposta. Com isso, a segurança deixa de ser lida como somatório de controles ou de incidentes e passa a ser compreendida como campo de coerência institucional.

O ganho teórico e prático dessa formulação está em reunir, numa mesma arquitetura, aquilo que com frequência aparece dissociado nas organizações: quem responde, como se coordena e em que termos o risco é reconhecido, qualificado e assumido. É por essa via que o Método RGA responde à promessa editorial do livro de oferecer uma estrutura conceitual e prática capaz de deslocar a segurança do campo operacional para o núcleo da decisão organizacional.

Os capítulos finais reforçaram esse argumento ao mostrar que o método conserva potência explicativa e operativa quando aplicado a situações concretas. Os casos analisados evidenciaram que vazamentos de dados, fragmentação institucional, ataques cibernéticos e decisões mal calibradas não devem ser interpretados

como anomalias isoladas, mas como manifestações de fragilidades organizacionais recorrentes. O que o Método RGA torna visível, nesses contextos, é a estrutura profunda que sustenta o evento aparente: responsabilidade difusa, integração insuficiente, leitura precária do risco, resposta tardia ou incapacidade de converter alerta em deliberação.

Essa capacidade de reordenar casos distintos em uma lógica comum de leitura constitui uma das forças mais expressivas da proposta autoral. Nela reside o alto valor de replicação atribuído ao capítulo final no próprio escopo da obra, bem como sua relevância para executivos, conselheiros, gestores, pesquisadores e organizações que buscam maior maturidade em decisões relacionadas a risco e continuidade do negócio.

A conclusão que se impõe, portanto, é que segurança estratégica não se define pela intensidade do aparato técnico empregado, mas pela capacidade institucional de manter nexos claros entre responsabilidade, governança e risco. Quando esses nexos se enfraquecem, a organização tende a converter complexidade em opacidade, especialização em fragmentação e decisão em reação tardia. Quando esses nexos se fortalecem, forma-se uma arquitetura capaz de sustentar continuidade, coerência decisória e aprendizado organizacional. Nesse sentido, a contribuição final deste livro consiste em afirmar que a segurança produz maior valor quando se converte em critério de direção organizacional, e não quando permanece restrita à contenção episódica de ameaças.

O Método RGA foi concebido exatamente para esse deslocamento: oferecer às organizações modernas uma forma mais lúcida, estruturada e replicável de transformar vulnerabilidade dispersa em governança estratégica, responsabilidade inteligível e assunção qualificada do risco. É nessa passagem que a segurança, enfim, deixa de ser setor e se torna decisão.

REFERÊNCIAS BIBLIOGRÁFICAS

AGHION, Philippe; TIROLE, Jean. Formal and real authority in organizations. *Journal of Political Economy*, v. 105, n. 1, p. 1-29, 1997. DOI: 10.1086/262063.

ÅRSTAD, Irene; ENGEN, Ole Andreas. Preventing major accidents: conditions for a functional risk ownership. *Safety Science*, v. 106, p. 57-65, 2018. DOI: 10.1016/j.ssci.2018.03.006.

BOVENS, Mark. Analysing and assessing accountability: a conceptual framework. *European Law Journal*, v. 13, n. 4, p. 447-468, 2007. DOI: 10.1111/j.1468-0386.2007.00378.x.

BOVENS, Mark. Two concepts of accountability: accountability as a virtue and as a mechanism. *West European Politics*, v. 33, n. 5, p. 946-967, 2010. DOI: 10.1080/01402382.2010.486119.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. *Risk Appetite: Critical to Success*. [S.l.]: COSO, 2020.

COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION. *Enterprise Risk Management: Integrating with Strategy and Performance*. [S.l.]: COSO, 2017.

CRAWFORD, Jason; JABBOUR, Mirna. The relationship between enterprise risk management and managerial judgement in decision-making: a systematic literature review. *International Journal of Management Reviews*, v. 26, n. 2, 2024. DOI: 10.1111/ijmr.12337.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. *The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years*. Washington, DC: CISA, 7 maio 2023.

DEPARTMENT OF ENERGY. *Colonial Pipeline Cyber Incident*. Washington, DC: U.S. Department of Energy, 2021.

EL ZEIN, Marwa; BAHRAMI, Bahador; HERTWIG, Ralph. Shared responsibility in collective decisions. *Nature Human Behaviour*, v. 3, p. 554-559, 2019. DOI: 10.1038/s41562-019-0596-4.

FEDERAL TRADE COMMISSION. *Equifax to Pay $575 Million as Part of Settlement with FTC, CFPB, and States Related to 2017 Data Breach*. Washington, DC: FTC, 22 jul. 2019.

FEDERAL TRADE COMMISSION. *FTC Finalizes Order with Marriott and Starwood Requiring Them to Implement a Robust Data Security Program to Address Security Failures*. Washington, DC: FTC, 2024.

FEDERAL TRADE COMMISSION. *FTC Finalizes Order with Online Alcohol Marketplace for Security Failures that Exposed Personal Data of 2.5 million People*. Washington, DC: FTC, 10 jan. 2023.

FEDERAL TRADE COMMISSION. *FTC Takes Action Against Drizly and its CEO James Cory Rellas for Security Failures that Exposed Data of 2.5 Million Consumers*. Washington, DC: FTC, 24 out. 2022.

HIEBL, Martin R. W. The integration of risk into management control systems: towards a deeper understanding across multiple levels of analysis. *Journal of Management Control*, v. 35, p. 1-16, 2024. DOI: 10.1007/s00187-024-00373-6.

HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM. *Committee Releases Report Revealing New Information on Equifax Data Breach*. Washington, DC: U.S. House of Representatives, 10 dez. 2018.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. *10 perguntas que o conselheiro deve fazer sobre cibersegurança*. São Paulo: IBGC, 2021.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO 22301:2019: security and resilience - business continuity management systems - requirements*. 2. ed. Geneva: ISO, 2019.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. *ISO 31000:2018. Risk management — Guidelines*. Geneva: ISO, 2018.

ISO/IEC. *ISO/IEC 27014:2020: information security, cybersecurity and privacy protection — governance of information security*. Geneva: International Organization for Standardization, 2020.

KEAY, Andrew; LOUGHREY, Joan. The framework for board accountability in corporate governance. *Legal Studies*, v. 35, n. 2, p. 252-279, 2015. DOI: 10.1111/lest.12058.

LUNDQVIST, Sara A. Why firms implement risk governance: stepping beyond traditional risk management to enterprise risk management. *Journal of Accounting and Public Policy*, v. 34, n. 5, p. 441-466, 2015. DOI: 10.1016/j.jaccpubpol.2015.05.002.

MARC, Mojca; ARENA, Marika; PELJHAN, Darja. The role of interactive style of use in improving risk management effectiveness. *Risk Management*, 2023. DOI: 10.1057/s41283-023-00114-4.

MONAZZAM, Aynaz; CRAWFORD, Jason. The role of enterprise risk management in enabling organisational resilience: a case study of the Swedish mining industry. *Journal of Management Control*, v. 35, p. 59-108, 2024. DOI: 10.1007/s00187-024-00370-9.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *IR 8286 Rev. 1: integrating cybersecurity and enterprise risk management (ERM)*. Gaithersburg: NIST, 2025. DOI: 10.6028/NIST.IR.8286r1.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *NIST Cybersecurity Framework 2.0: Quick-Start Guide for Using the CSF Tiers*. Gaithersburg, MD: NIST, 2024. Special Publication 1302. DOI: 10.6028/NIST.SP.1302.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *NIST Cybersecurity Framework 2.0: enterprise risk management quick-start guide*. Gaithersburg: NIST, 2024. NIST Special Publication, SP 1303. DOI: 10.6028/NIST.SP.1303.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. *NIST Cybersecurity Framework 2.0: enterprise risk management quick-start guide*. Gaithersburg: NIST, 2024. NIST Special Publication, SP 1303. DOI: 10.6028/NIST.SP.1303.

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

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

OECD. *Digital security risk management for economic and social prosperity: OECD recommendation and companion document*. Paris: OECD Publishing, 2015. DOI: 10.1787/9789264245471-en.

OECD. *Digital security risk management for economic and social prosperity: OECD recommendation and companion document*. Paris: OECD Publishing, 2015. DOI: 10.1787/9789264245471-en.

OECD. *G20/OECD Principles of Corporate Governance 2023*. Paris: OECD Publishing, 2023. DOI: 10.1787/ed750b30-en.

PAPAZAFEIROPOULOU, Anastasia; SPANAKI, Kalliope. Understanding governance, risk and compliance information systems (GRC IS): the experts view. *Information Systems Frontiers*, v. 18, p. 1251-1263, 2016. DOI: 10.1007/s10796-015-9572-3.

SECURITIES AND EXCHANGE COMMISSION. *Cybersecurity risk management, strategy, governance, and incident disclosure*. Washington, DC: SEC, 2023. Release n. 33-11216. File n. S7-09-22.

SECURITIES AND EXCHANGE COMMISSION. *Cybersecurity risk management, strategy, governance, and incident disclosure*. Washington, DC: SEC, 2023. Release n. 33-11216. File n. S7-09-22.

SLAPNIČAR, Sergeja et al. A pathway model to five lines of accountability in cybersecurity governance. *International Journal of Accounting Information Systems*, v. 51, art. 100642, 2023. DOI: 10.1016/j.accinf.2023.100642.

SLAPNIČAR, Sergeja; AXELSEN, Micheal; EULERICH, Marc. Cyber risk management: an illusion of a risk-based approach. *Journal of Management Control*, 2025. DOI: 10.1007/s00187-025-00401-z.

SOOMRO, Zahoor Ahmed; SHAH, Mahmood Hussain; AHMED, Javed. Information security management needs more holistic approach: a literature review. *International Journal of Information Management*, v. 36, n. 2, p. 215-225, 2016. DOI: 10.1016/j.ijinfomgt.2015.11.009.

THE INSTITUTE OF INTERNAL AUDITORS. *The IIA's Three Lines Model: an update of the Three Lines of Defense*. Lake Mary, FL: The IIA, 2020.

WARNER, David; MCKEE, Lisa. Board of directors role in data privacy governance: making the transition from compliance driven to good business stewardship. *Journal of Cybersecurity Education, Research and Practice*, v. 2024, n. 1, art. 14, 2024.

WORLD ECONOMIC FORUM. *Principles for board governance of cyber risk*. Geneva: World Economic Forum, 2021.

WORLD ECONOMIC FORUM. *Principles for board governance of cyber risk*. Geneva: World Economic Forum, 2021.

WORLD ECONOMIC FORUM. *Resilience Pulse Check: Harnessing Collaboration to Navigate a Volatile World*. Geneva: World Economic Forum, 2025.

WORLD ECONOMIC FORUM. *The global risks report 2026*. Geneva: World Economic Forum, 2026. Published: 14 Jan. 2026.

POSFÁCIO

Em um ambiente corporativo cada vez mais exposto, interconectado e pressionado por decisões rápidas, o risco deixou de ser uma variável secundária. Ele passou a influenciar diretamente a continuidade dos negócios, a reputação das organizações e a geração de valor no longo prazo.

Ainda assim, a maioria das empresas continua tratando a segurança como uma função técnica isolada, reativa e desconectada da estratégia. Este livro desafia essa lógica.

Com base em mais de duas décadas de experiência em projetos de alta complexidade, Luiz Henrique de Paula Paiva Apresenta uma nova forma de compreender a segurança: não apenas como proteção, mas como elemento estruturante da decisão organizacional necessária.

Ao longo da obra, o leitor é conduzido por uma abordagem clara, aplicada e orientada à realidade das empresas, por meio do Método RGA: Responsabilidade, Governança e Assunção de Risco. Uma estrutura que conecta o que normalmente está fragmentado, permitindo transformar vulnerabilidades difusas em direcionamento estratégico, clareza decisória e capacidade de resposta.

Mais do que um livro sobre cibersegurança, esta é uma obra sobre liderança, responsabilidade e tomada de decisão em ambientes de incerteza.

Para quem este livro é essencial como leitura e instrumento profissional:

- Executivos e membros de conselho
- Líderes de tecnologia e segurança
- Tomadores de decisão em ambientes complexos

- Empresários que buscam crescimento com sustentabilidade e segurança

Porque, no cenário atual, não se trata apenas de proteger a organização. Trata-se de decidir com consciência antes que o risco cibernético decida pela sua organização.

Em um cenário corporativo marcado por incertezas, transformação digital e riscos cada vez mais complexos, a segurança deixa de ser apenas um conjunto de práticas operacionais para assumir um papel central na estratégia organizacional.

Nesta obra, o leitor é convidado a compreender como a segurança pode — e deve — ser integrada às estruturas de decisão, influenciando diretamente a governança, a distribuição de responsabilidades e a capacidade institucional de പ്രതികരണം diante de vulnerabilidades.

Ao apresentar o Método RGA, o autor propõe uma abordagem inovadora que conecta responsabilidade, governança e assunção de risco em uma lógica estratégica única.

Mais do que um livro técnico, esta é uma leitura essencial para líderes, executivos e tomadores de decisão que reconhecem que sustentar organizações no mundo atual exige mais do que proteger sistemas: exige compreender, interpretar e assumir riscos com clareza, consistência e direção.

ISBN: 978-6-55321-115-5