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

Ano V, v.2 2024 | submissão: 16/02/2024 | aceito: 19/02/2024 | publicação: 22/02/2024

Governança corporativa da informação: segurança, privacidade de dados e gestão executiva na era da inteligência artificial

Corporate information governance: security, data privacy and executive management in the age of artificial intelligence

Gobernanza de la Información Corporativa: Seguridad, Privacidad de Datos y Gestión Ejecutiva en la Era de la Inteligencia Artificial

Ricardo Saddi Becker
Bacharelado em Ciência da Computação pela Universidade Federal de Mato Grosso (2009).
Especialista certificado pelo DRII em continuidade de negócios

RESUMO

A informação consolidou-se como um dos principais ativos estratégicos das organizações contemporâneas, assumindo papel determinante na geração de valor, inovação e competitividade. Paralelamente ao crescimento exponencial do volume de dados e à incorporação de tecnologias baseadas em Inteligência Artificial (IA), ampliaram-se os desafios relacionados à segurança da informação, à privacidade dos titulares de dados e à governança corporativa. Nesse contexto, este estudo analisa a integração entre governança da informação, proteção de dados, gestão executiva e segurança cibernética, discutindo como esses elementos contribuem para a construção de organizações mais resilientes, transparentes e orientadas por dados. A pesquisa foi desenvolvida por meio de revisão bibliográfica de caráter exploratório e descritivo, fundamentada em literatura científica, normas internacionais e referenciais de governança amplamente adotados no ambiente corporativo. Os resultados evidenciam que a proteção das informações deixou de representar apenas uma responsabilidade operacional das áreas de Tecnologia da Informação para tornar-se uma atribuição estratégica compartilhada entre executivos, conselhos de administração e lideranças organizacionais. Conclui-se que modelos integrados de governança, aliados à adoção de práticas estruturadas de segurança, privacidade e gestão de riscos, constituem fatores essenciais para assegurar conformidade regulatória, sustentabilidade dos negócios e confiança institucional em um cenário caracterizado pela crescente digitalização das relações econômicas e sociais.

PALAVRAS-CHAVE: Governança da Informação; Segurança da Informação; Privacidade de Dados; Inteligência Artificial; Gestão Executiva.

ABSTRACT

Information has become one of the most valuable strategic assets of contemporary organizations, playing a decisive role in value creation, innovation and competitiveness. Simultaneously with the exponential growth of data volumes and the incorporation of Artificial Intelligence (AI) technologies, challenges related to information security, data privacy and corporate governance have intensified. This study examines the relationship between information governance, data protection, executive management and cybersecurity, discussing how these elements contribute to the development of resilient, transparent and data-driven organizations. The research was conducted through an exploratory and descriptive literature review based on scientific publications, international standards and recognized governance frameworks. The findings demonstrate that information protection is no longer solely an operational responsibility of Information Technology departments, becoming instead a strategic concern shared by executives, boards of directors and organizational leadership. The study concludes that integrated governance models, combined with structured practices in security, privacy and risk management, are fundamental to ensuring regulatory compliance, business sustainability and institutional trust in an increasingly digital economy.

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

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

Ano V, v.2 2024 | submissão: 16/02/2024 | aceito: 19/02/2024 | publicação: 22/02/2024

KEYWORDS: Information Governance; Information Security; Data Privacy; Artificial Intelligence; Executive Management.

INTRODUÇÃO

A economia digital transformou profundamente a maneira como organizações produzem conhecimento, tomam decisões e estabelecem vantagens competitivas. A expansão dos ambientes conectados, da computação em nuvem, das plataformas digitais e da Inteligência Artificial ampliou significativamente o valor estratégico dos dados, tornando a informação um recurso indispensável para a inovação, o desenvolvimento de novos modelos de negócios e o fortalecimento da competitividade empresarial.

Entretanto, o mesmo cenário que impulsiona oportunidades também amplia a complexidade da gestão corporativa. O crescimento exponencial do volume de informações, a circulação contínua de dados pessoais, a integração entre diferentes ecossistemas tecnológicos e a crescente dependência de serviços digitais elevaram os riscos relacionados à privacidade, à segurança cibernética, à conformidade regulatória e à governança dos ativos informacionais. Como consequência, a administração desses recursos deixou de representar uma atribuição exclusivamente técnica para assumir dimensão estratégica nas organizações.

Nos últimos anos, legislações voltadas à proteção de dados pessoais, como a Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral sobre a Proteção de Dados (GDPR) na União Europeia, reforçaram a necessidade de mecanismos capazes de assegurar transparência, responsabilidade e controle sobre o tratamento das informações. Paralelamente, a rápida evolução das soluções baseadas em Inteligência Artificial introduziu novos desafios relacionados à utilização ética dos dados, à transparência dos algoritmos e à responsabilidade pelas decisões automatizadas. Nesse contexto, a governança da informação emerge como disciplina responsável por estabelecer políticas, processos e responsabilidades que assegurem a utilização segura, ética e estratégica dos ativos informacionais. Mais do que garantir conformidade normativa, sua finalidade consiste em promover qualidade dos dados, fortalecer a tomada de decisões, reduzir riscos corporativos e ampliar a capacidade de geração de valor a partir da informação.

A participação das lideranças executivas assume importância crescente nesse processo. Conselhos de administração, diretores executivos, gestores de tecnologia e responsáveis pela proteção de dados passam a compartilhar responsabilidades relacionadas à definição das estratégias de governança, ao

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

Ano V, v.2 2024 | submissão: 16/02/2024 | aceito: 19/02/2024 | publicação: 22/02/2024

gerenciamento dos riscos digitais e ao estabelecimento de uma cultura organizacional orientada pela proteção da informação e pela utilização responsável da Inteligência Artificial.

Diante desse cenário, este estudo tem como objetivo analisar a relação entre governança da informação, segurança da informação, privacidade de dados e gestão executiva, discutindo como esses elementos se complementam na construção de organizações capazes de conciliar inovação tecnológica, conformidade regulatória e sustentabilidade dos negócios em um ambiente caracterizado por crescente complexidade digital.

METODOLOGIA

A presente pesquisa caracteriza-se como um estudo de natureza exploratória e descritiva, desenvolvido por meio de revisão bibliográfica. Conforme Gil (2019), esse procedimento metodológico permite reunir, organizar e analisar criticamente diferentes perspectivas teóricas sobre determinado fenômeno, favorecendo a compreensão das transformações conceituais e práticas observadas em contextos organizacionais contemporâneos.

O levantamento bibliográfico contemplou livros, artigos científicos, normas internacionais, publicações institucionais e referenciais de governança relacionados à segurança da informação, proteção de dados pessoais, governança corporativa, Inteligência Artificial, gestão de riscos e transformação digital. Foram priorizadas obras reconhecidas pela comunidade acadêmica e técnica, bem como documentos produzidos por organismos internacionais dedicados ao desenvolvimento de boas práticas em governança da informação.

As fontes selecionadas foram submetidas à análise qualitativa, buscando identificar convergências conceituais, modelos de gestão amplamente adotados e tendências observadas na evolução das práticas de governança corporativa da informação. Para favorecer uma abordagem sistemática, o conteúdo foi organizado em cinco eixos temáticos: fundamentos da governança da informação; privacidade de dados e conformidade regulatória; Inteligência Artificial e gestão de riscos; segurança da informação sob a perspectiva executiva; e liderança estratégica orientada por dados.

Além da literatura clássica sobre governança e gestão da informação, foram considerados referenciais recentes relacionados à regulamentação da Inteligência Artificial, aos princípios internacionais de ética digital e às normas voltadas à proteção da privacidade e da segurança dos ativos informacionais. Essa abordagem possibilita integrar fundamentos consolidados da literatura com os desafios

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

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

Ano V, v.2 2024 | submissão: 16/02/2024 | aceito: 19/02/2024 | publicação: 22/02/2024

emergentes decorrentes da rápida evolução tecnológica e das novas exigências regulatórias impostas às organizações.

1. FUNDAMENTOS DA GOVERNANÇA DA INFORMAÇÃO

A transformação digital modificou substancialmente a forma como as organizações produzem valor, tornando a informação um dos principais ativos estratégicos do ambiente corporativo. Dados gerados por operações, clientes, fornecedores, dispositivos conectados e plataformas digitais passaram a sustentar decisões de negócio, impulsionar iniciativas de inovação e orientar estratégias de crescimento. Nesse contexto, a governança da informação deixa de representar uma atividade restrita à Tecnologia da Informação para assumir papel transversal, envolvendo diferentes áreas da organização e níveis de liderança.

A governança da informação pode ser compreendida como o conjunto de políticas, processos, responsabilidades e mecanismos de controle destinados a assegurar que os ativos informacionais sejam administrados de forma consistente ao longo de todo o seu ciclo de vida. Seu propósito não se limita à proteção dos dados, mas busca garantir que as informações sejam confiáveis, íntegras, acessíveis, utilizadas de maneira ética e alinhadas aos objetivos estratégicos da instituição. Dessa forma, qualidade, segurança, conformidade e geração de valor tornam-se dimensões indissociáveis da gestão da informação.

A consolidação dessa disciplina decorre da percepção de que decisões organizacionais são diretamente influenciadas pela qualidade dos dados disponíveis. Informações incompletas, inconsistentes ou desatualizadas comprometem análises gerenciais, dificultam o atendimento às exigências regulatórias e podem produzir impactos financeiros, operacionais e reputacionais relevantes. Sob essa perspectiva, a governança da informação estabelece critérios para padronização, classificação, retenção, compartilhamento e descarte dos ativos informacionais, reduzindo ambiguidades e fortalecendo a confiabilidade das decisões corporativas.

Entre os pilares mais relevantes desse modelo destaca-se a definição clara de papéis e responsabilidades. Organizações com maior grau de maturidade costumam distinguir atribuições entre executivos patrocinadores, proprietários dos dados (*Data Owners*), gestores responsáveis pela qualidade das informações (*Data Stewards*) e equipes técnicas encarregadas da administração dos ambientes tecnológicos. Essa segregação favorece maior responsabilização institucional, amplia a transparência dos processos e reduz conflitos relacionados à utilização dos dados.

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

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

Ano V, v.2 2024 | submissão: 16/02/2024 | aceito: 19/02/2024 | publicação: 22/02/2024

Outro elemento essencial refere-se à gestão do ciclo de vida da informação. Desde sua criação ou coleta até o arquivamento e descarte definitivo, os dados percorrem diferentes etapas que exigem controles específicos. A inexistência de políticas de retenção, classificação documental ou descarte seguro aumenta a exposição a riscos regulatórios e compromete a eficiência da gestão documental. Por essa razão, modelos modernos de governança estabelecem critérios objetivos para cada fase desse ciclo, conciliando requisitos legais, necessidades operacionais e interesses estratégicos da organização.

A qualidade dos dados também ocupa posição central nas práticas de governança. Dimensões como precisão, consistência, completude, atualidade e unicidade influenciam diretamente a confiabilidade das análises realizadas pelas áreas de negócio. A expansão de iniciativas de Business Intelligence, Analytics e Inteligência Artificial tornou ainda mais evidente que modelos analíticos produzem resultados apenas na medida em que utilizam bases de dados confiáveis. Assim, investimentos em tecnologias avançadas tendem a apresentar desempenho limitado quando não são acompanhados por programas estruturados de qualidade da informação.

Além dos aspectos operacionais, a governança da informação fortalece a capacidade de adaptação das organizações diante de mudanças regulatórias e tecnológicas. A existência de políticas institucionalizadas, responsabilidades formalmente definidas e processos documentados facilita a incorporação de novos requisitos legais, reduz impactos decorrentes de transformações organizacionais e amplia a previsibilidade na administração dos ativos informacionais.

Nesse cenário, observa-se uma evolução conceitual importante: a informação deixa de ser tratada apenas como recurso operacional para consolidar-se como patrimônio estratégico da organização. Sua adequada governança influencia diretamente a capacidade de inovar, competir, atender exigências regulatórias e estabelecer relações de confiança com clientes, parceiros, investidores e órgãos de fiscalização. Em organizações orientadas por dados, a maturidade da governança informacional tornou-se indicador relevante da própria capacidade institucional de gerar valor de forma sustentável.

2. PRIVACIDADE DE DADOS E CONFORMIDADE REGULATÓRIA

A intensificação da coleta, do compartilhamento e do processamento de informações pessoais transformou a privacidade em um dos principais desafios da governança corporativa contemporânea. O crescimento dos serviços digitais, da computação em nuvem, das plataformas colaborativas e das aplicações baseadas em Inteligência Artificial ampliou significativamente a circulação de dados entre

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

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

Ano V, v.2 2024 | submissão: 16/02/2024 | aceito: 19/02/2024 | publicação: 22/02/2024

organizações, fornecedores e usuários, exigindo mecanismos capazes de assegurar tratamento responsável das informações e respeito aos direitos dos titulares.

A evolução desse cenário impulsionou o fortalecimento dos marcos regulatórios voltados à proteção de dados pessoais. A entrada em vigor da Lei Geral de Proteção de Dados (LGPD), no Brasil, e do Regulamento Geral sobre a Proteção de Dados (GDPR), na União Europeia, consolidou uma mudança de paradigma ao estabelecer que a utilização de dados pessoais deve observar princípios relacionados à finalidade, necessidade, transparência, segurança, responsabilização e prestação de contas. Essas legislações não representam apenas instrumentos jurídicos de fiscalização, mas referenciais capazes de orientar modelos mais maduros de governança da informação.

Sob essa perspectiva, conformidade regulatória não deve ser compreendida como atividade limitada ao atendimento de exigências legais. Organizações que tratam a proteção de dados exclusivamente como obrigação normativa tendem a adotar medidas pontuais e reativas. Em contrapartida, instituições que incorporam a privacidade à estratégia organizacional desenvolvem políticas permanentes de gestão dos dados, fortalecendo a confiança dos titulares e reduzindo riscos associados à utilização inadequada das informações.

Um dos princípios mais relevantes nesse contexto é o conceito de *Privacy by Design*, segundo o qual requisitos de privacidade devem ser considerados desde as fases iniciais de concepção de produtos, serviços e processos organizacionais. Em vez de implementar controles apenas após a identificação de problemas, essa abordagem incentiva a integração preventiva da proteção de dados ao desenvolvimento das soluções tecnológicas, reduzindo custos de adequação e ampliando a efetividade dos mecanismos de segurança.

Complementarmente, o princípio do *Privacy by Default* estabelece que as configurações padrão dos sistemas devem privilegiar o menor tratamento possível de dados pessoais, limitando a coleta e o compartilhamento às informações estritamente necessárias para cada finalidade. Essa diretriz reforça a ideia de que a proteção da privacidade não depende exclusivamente do comportamento do usuário, mas também das decisões arquiteturais adotadas durante o desenvolvimento e a operação dos sistemas.

A implementação de programas estruturados de privacidade exige ainda mecanismos permanentes de governança. Inventários de dados, mapeamento dos fluxos informacionais, registros das atividades de tratamento, avaliações de impacto à proteção de dados e processos formais para atendimento aos direitos dos titulares constituem instrumentos fundamentais para assegurar conformidade contínua.

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

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

Ano V, v.2 2024 | submissão: 16/02/2024 | aceito: 19/02/2024 | publicação: 22/02/2024

Essas práticas também favorecem maior transparência perante autoridades reguladoras e reduzem o tempo necessário para responder a incidentes envolvendo informações pessoais.

Outro aspecto de crescente relevância refere-se à gestão dos riscos decorrentes do compartilhamento de dados com terceiros. Cadeias complexas de fornecedores, serviços terceirizados, plataformas em nuvem e ecossistemas digitais ampliam a necessidade de avaliação permanente das práticas adotadas pelos parceiros comerciais. A conformidade organizacional deixa, portanto, de depender apenas dos controles internos e passa a incorporar mecanismos de due diligence, cláusulas contratuais específicas, auditorias periódicas e critérios objetivos para seleção e monitoramento de operadores de dados.

A figura do Encarregado pelo Tratamento de Dados Pessoais, conhecido internacionalmente como *Data Protection Officer* (DPO), reforça esse modelo de governança ao atuar como elemento de integração entre organização, titulares e autoridades de fiscalização. Mais do que desempenhar função consultiva, esse profissional contribui para disseminar a cultura de proteção de dados, apoiar decisões estratégicas e orientar programas de conformidade alinhados às exigências regulatórias e às melhores práticas internacionais.

À medida que a economia digital evolui, a privacidade deixa de ser percebida apenas como requisito legal para consolidar-se como diferencial competitivo e elemento essencial da reputação institucional. Organizações capazes de demonstrar transparência, responsabilidade e compromisso com a proteção dos dados fortalecem relações de confiança com clientes, parceiros e investidores, transformando a conformidade regulatória em componente estratégico da sustentabilidade e da governança corporativa.

3. INTELIGÊNCIA ARTIFICIAL, GOVERNANÇA ALGORÍTMICA E GESTÃO DE RISCOS

A incorporação da Inteligência Artificial (IA) aos processos organizacionais representa uma das transformações mais significativas da atualidade. Sistemas capazes de analisar grandes volumes de dados, identificar padrões complexos e apoiar decisões em tempo real vêm sendo empregados em setores como saúde, finanças, indústria, logística, educação e administração pública. Embora essas tecnologias ampliem a eficiência operacional e a capacidade analítica das organizações, sua adoção também introduz desafios relacionados à governança, à transparência das decisões automatizadas e à gestão dos riscos associados aos modelos algorítmicos.

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

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

Ano V, v.2 2024 | submissão: 16/02/2024 | aceito: 19/02/2024 | publicação: 22/02/2024

Diferentemente dos sistemas tradicionais, aplicações baseadas em aprendizado de máquina apresentam comportamento dinâmico, condicionado à qualidade dos dados utilizados no treinamento, às características dos algoritmos empregados e às alterações ocorridas no ambiente operacional. Como consequência, decisões produzidas por esses modelos podem sofrer degradação de desempenho ao longo do tempo, reproduzir vieses estatísticos presentes nas bases de dados ou gerar resultados cuja lógica não seja plenamente compreendida pelos próprios usuários. Essa característica reforça a necessidade de mecanismos específicos de governança para assegurar confiabilidade, rastreabilidade e supervisão humana.

Nesse contexto, a governança algorítmica emerge como disciplina voltada ao estabelecimento de políticas, responsabilidades e controles aplicáveis ao ciclo de vida dos modelos de Inteligência Artificial. Seu objetivo consiste em garantir que sistemas automatizados sejam desenvolvidos, implementados e monitorados de forma compatível com princípios éticos, requisitos legais e objetivos estratégicos da organização. A governança não busca limitar a inovação tecnológica, mas assegurar que sua utilização ocorra de maneira transparente, responsável e alinhada ao interesse institucional.

Entre os principais desafios encontra-se a qualidade das bases de dados utilizadas para treinamento e validação dos modelos. Informações incompletas, desatualizadas ou estatisticamente desequilibradas comprometem a capacidade preditiva dos algoritmos e ampliam o risco de decisões inconsistentes. Em aplicações relacionadas à concessão de crédito, recrutamento de pessoas, diagnóstico médico ou análise de risco, pequenas distorções nos dados podem produzir impactos relevantes sobre indivíduos e organizações. Dessa forma, programas de governança da IA dependem diretamente da maturidade da governança da informação discutida nos capítulos anteriores.

Outro aspecto de crescente relevância refere-se à explicabilidade dos modelos (*Explainable Artificial Intelligence – XAI*). Em aplicações críticas, decisões automatizadas não devem ser avaliadas apenas pela precisão estatística, mas também pela capacidade de fornecer justificativas compreensíveis para seus resultados. A transparência favorece auditorias independentes, fortalece a confiança dos usuários e possibilita identificar fatores que influenciam o comportamento dos algoritmos, especialmente em setores sujeitos a elevada regulação.

A supervisão humana permanece igualmente indispensável. Embora modelos avançados sejam capazes de automatizar atividades complexas, a responsabilidade pelas decisões organizacionais continua pertencendo às pessoas e às instituições que utilizam essas tecnologias. A participação de especialistas na validação dos resultados, na revisão periódica dos modelos e na definição de limites

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

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

Ano V, v.2 2024 | submissão: 16/02/2024 | aceito: 19/02/2024 | publicação: 22/02/2024

para automação reduz a probabilidade de decisões inadequadas e preserva princípios relacionados à responsabilidade corporativa.

A rápida evolução das soluções de IA também ampliou a importância do gerenciamento contínuo dos riscos tecnológicos. Organizações maduras estabelecem processos permanentes para monitorar desempenho dos modelos, identificar deriva estatística (*model drift*), revisar parâmetros de treinamento e avaliar impactos decorrentes de alterações nos conjuntos de dados. Essa abordagem permite detectar degradações antes que produzam consequências relevantes para os processos de negócio.

Nos últimos anos, organismos internacionais passaram a estruturar referenciais específicos para governança da Inteligência Artificial. Destacam-se iniciativas voltadas à gestão de riscos, princípios éticos para utilização responsável da IA e diretrizes para transparência algorítmica, refletindo uma tendência global de fortalecimento dos mecanismos regulatórios aplicáveis às tecnologias emergentes. Essas iniciativas reforçam que inovação e responsabilidade devem evoluir de maneira integrada, evitando que ganhos de eficiência sejam obtidos à custa da redução da confiança institucional.

Sob essa perspectiva, a Inteligência Artificial deixa de representar apenas uma ferramenta de automação para tornar-se objeto permanente da governança corporativa. Sua utilização responsável depende da integração entre qualidade dos dados, supervisão humana, avaliação contínua de riscos e mecanismos capazes de assegurar transparência, conformidade regulatória e responsabilidade nas decisões automatizadas.

4. SEGURANÇA DA INFORMAÇÃO COMO INSTRUMENTO DE GOVERNANÇA E VALOR ORGANIZACIONAL

Durante muitos anos, a segurança da informação foi tratada predominantemente como uma função técnica, concentrada na administração de controles computacionais destinados à proteção dos ambientes tecnológicos. A evolução dos modelos de negócios digitais, entretanto, ampliou significativamente sua relevância estratégica. Atualmente, incidentes envolvendo vazamento de informações, comprometimento da integridade dos dados ou interrupção de serviços produzem impactos que extrapolam a esfera tecnológica, afetando reputação institucional, desempenho financeiro, conformidade regulatória e confiança de clientes, investidores e parceiros comerciais.

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

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

Ano V, v.2 2024 | submissão: 16/02/2024 | aceito: 19/02/2024 | publicação: 22/02/2024

Essa transformação modificou a forma como organizações estruturam seus programas de segurança. A responsabilidade pela proteção da informação deixou de estar restrita às equipes técnicas e passou a integrar a agenda dos conselhos de administração e da alta liderança. O gerenciamento dos riscos cibernéticos passou a ser compreendido como componente da governança corporativa, influenciando decisões relacionadas à expansão dos negócios, à inovação tecnológica, à gestão de terceiros e à sustentabilidade organizacional.

Nesse contexto, a cultura organizacional assume papel determinante. A efetividade dos controles de segurança depende não apenas da adoção de tecnologias especializadas, mas também do comportamento das pessoas que produzem, compartilham e utilizam informações diariamente. Programas permanentes de conscientização, capacitação e desenvolvimento de competências fortalecem a percepção dos riscos associados ao tratamento inadequado dos dados e reduzem a ocorrência de incidentes decorrentes de falhas humanas, ainda responsáveis por parcela significativa dos eventos de segurança registrados em organizações públicas e privadas.

Outro aspecto relevante refere-se à integração entre segurança da informação e gestão de riscos corporativos. Em vez de atuar de maneira isolada, os programas de segurança devem participar dos processos de planejamento estratégico, avaliando impactos potenciais sobre objetivos institucionais, continuidade das operações, conformidade regulatória e reputação organizacional. Essa integração favorece decisões mais equilibradas quanto à priorização de investimentos, à aceitação de riscos residuais e à definição de controles compatíveis com o contexto de cada organização.

A crescente dependência de fornecedores especializados também ampliou a importância da gestão dos riscos associados às cadeias de suprimentos digitais. Serviços em nuvem, plataformas terceirizadas, provedores de software, parceiros tecnológicos e empresas responsáveis pelo processamento de dados passaram a integrar ecossistemas altamente conectados, nos quais vulnerabilidades externas podem produzir impactos significativos sobre a organização contratante. Dessa forma, processos estruturados de avaliação de fornecedores, auditorias periódicas e monitoramento contínuo tornaram-se elementos essenciais da governança da segurança.

Sob a perspectiva executiva, indicadores de desempenho assumem função estratégica. Métricas relacionadas à maturidade dos controles, tempo de resposta a incidentes, aderência às políticas corporativas, resultados de auditorias, conformidade regulatória e evolução do nível de risco fornecem informações relevantes para subsidiar decisões da alta administração. Diferentemente dos indicadores operacionais tradicionalmente utilizados pelas equipes técnicas, esses instrumentos

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

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

Ano V, v.2 2024 | submissão: 16/02/2024 | aceito: 19/02/2024 | publicação: 22/02/2024

permitem traduzir riscos tecnológicos em informações compreensíveis para gestores responsáveis pelo direcionamento estratégico da organização.

A evolução dos ambientes digitais também fortaleceu a necessidade de abordagens baseadas em melhoria contínua. Avaliações periódicas de maturidade, revisões de políticas institucionais, exercícios de gestão de crises, auditorias independentes e processos sistemáticos de aprendizagem organizacional contribuem para aperfeiçoar continuamente os programas de segurança, tornando-os mais adaptáveis às transformações tecnológicas e regulatórias.

Por fim, observa-se que a segurança da informação passou a exercer papel relevante na geração de valor institucional. Organizações capazes de demonstrar elevado grau de maturidade na proteção de seus ativos informacionais tendem a fortalecer relações de confiança com clientes, investidores e parceiros estratégicos, ampliando sua capacidade competitiva em mercados cada vez mais orientados por dados. Nesse cenário, a segurança deixa de representar exclusivamente um centro de custos para consolidar-se como investimento estratégico capaz de sustentar inovação, conformidade e crescimento sustentável.

5. LIDERANÇA EXECUTIVA E TOMADA DE DECISÃO ORIENTADA POR DADOS

A consolidação da economia digital alterou significativamente o papel da liderança nas organizações. A crescente disponibilidade de informações, associada ao avanço das plataformas analíticas e da Inteligência Artificial, ampliou a capacidade das empresas de compreender seu ambiente de negócios e responder com maior rapidez às mudanças do mercado. Nesse contexto, a tomada de decisão baseada em dados (*data-driven decision making*) deixou de representar uma vantagem competitiva circunstancial para tornar-se componente essencial da estratégia corporativa.

Essa transformação exige que executivos desenvolvam competências que ultrapassam o domínio tradicional da administração. A compreensão dos princípios relacionados à governança da informação, proteção de dados, segurança cibernética e Inteligência Artificial passa a integrar o conjunto de habilidades necessárias para orientar investimentos, avaliar riscos e estabelecer prioridades organizacionais. O papel da liderança deixa de concentrar-se exclusivamente na gestão financeira e operacional, incorporando responsabilidades relacionadas à utilização ética, segura e estratégica dos ativos informacionais.

A maturidade digital das organizações está diretamente associada à capacidade de integrar dados provenientes de diferentes áreas de negócio em processos decisórios consistentes. Informações

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

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

Ano V, v.2 2024 | submissão: 16/02/2024 | aceito: 19/02/2024 | publicação: 22/02/2024

produzidas por sistemas corporativos, plataformas de relacionamento com clientes, indicadores financeiros, sensores industriais e ambientes digitais permitem construir uma visão mais abrangente do desempenho institucional. Entretanto, a simples disponibilidade desses dados não assegura melhores decisões. Sua efetividade depende da existência de mecanismos de governança capazes de garantir qualidade, confiabilidade e contexto para interpretação das informações.

Nesse cenário, Business Intelligence, Analytics e Inteligência Artificial desempenham funções complementares. Enquanto as plataformas analíticas oferecem suporte à identificação de tendências e padrões de comportamento, modelos de IA ampliam a capacidade preditiva das organizações e auxiliam na simulação de cenários complexos. Contudo, a utilização dessas tecnologias deve permanecer subordinada aos objetivos estratégicos definidos pela liderança, evitando que decisões automatizadas substituam a análise crítica necessária à gestão organizacional.

A atuação integrada entre Conselho de Administração, Chief Executive Officer (CEO), Chief Information Officer (CIO), Chief Information Security Officer (CISO) e Encarregado pelo Tratamento de Dados Pessoais (DPO) tornou-se um dos principais indicadores de maturidade da governança corporativa. A articulação entre essas funções favorece maior alinhamento entre inovação tecnológica, gestão de riscos, conformidade regulatória e objetivos institucionais, reduzindo a fragmentação das decisões relacionadas à transformação digital.

Outro elemento relevante refere-se ao estabelecimento de indicadores capazes de traduzir informações técnicas em métricas compreensíveis para a alta administração. Indicadores-chave de desempenho (kpis) e indicadores-chave de risco (kris) relacionados à qualidade dos dados, conformidade regulatória, maturidade da governança, proteção da privacidade e eficiência operacional fornecem subsídios objetivos para acompanhamento da evolução institucional e para a definição de prioridades estratégicas.

A sustentabilidade das organizações digitais também depende da consolidação de uma cultura orientada por dados. Essa transformação não decorre exclusivamente da adoção de novas tecnologias, mas da capacidade institucional de incorporar evidências objetivas aos processos de planejamento, inovação e tomada de decisão. Ambientes organizacionais que estimulam transparência, compartilhamento responsável das informações e aprendizagem contínua apresentam maior capacidade de adaptação às mudanças regulatórias, tecnológicas e mercadológicas.

Por fim, observa-se que a liderança contemporânea passa a exercer função integradora entre tecnologia, governança e estratégia. A capacidade de transformar dados em conhecimento confiável, promover inovação de forma responsável e equilibrar oportunidades com riscos tornou-se fator

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

Ano V, v.2 2024 | submissão: 16/02/2024 | aceito: 19/02/2024 | publicação: 22/02/2024

determinante para organizações que buscam competitividade em um ambiente caracterizado pela rápida evolução tecnológica e pela crescente dependência dos ativos informacionais.

CONCLUSÃO

A crescente centralidade da informação nas atividades econômicas e institucionais redefiniu a forma como as organizações estruturam seus processos de gestão, inovação e geração de valor. Em um ambiente marcado pela intensificação da transformação digital, pela expansão da Inteligência Artificial e pelo fortalecimento das exigências regulatórias relacionadas à proteção de dados, a governança da informação consolida-se como elemento estratégico para a sustentabilidade organizacional.

A análise desenvolvida neste estudo evidencia que segurança da informação, privacidade de dados, governança corporativa e gestão executiva constituem dimensões interdependentes de um mesmo sistema de gestão. A efetividade dessas iniciativas não depende exclusivamente da implementação de tecnologias especializadas, mas da construção de estruturas organizacionais capazes de integrar políticas institucionais, processos decisórios, responsabilidades claramente definidas e mecanismos permanentes de monitoramento e melhoria contínua.

Observou-se que a qualidade da informação exerce influência direta sobre a capacidade das organizações de desenvolver modelos analíticos confiáveis, implementar soluções baseadas em Inteligência Artificial e atender às crescentes exigências relacionadas à transparência e à conformidade regulatória. Nesse contexto, programas de governança da informação deixam de possuir caráter meramente administrativo para assumir papel determinante na geração de valor institucional e na redução dos riscos associados à utilização dos ativos digitais.

A evolução das tecnologias de Inteligência Artificial introduz novos desafios relacionados à transparência algorítmica, à mitigação de vieses, à supervisão humana e à responsabilização pelas decisões automatizadas. Esses aspectos demonstram que a inovação tecnológica precisa ser acompanhada por mecanismos robustos de governança capazes de assegurar equilíbrio entre eficiência operacional, proteção dos direitos fundamentais e responsabilidade corporativa.

Outro aspecto evidenciado ao longo deste trabalho refere-se à importância da participação da alta administração na condução das estratégias de governança da informação. A integração entre conselhos de administração, executivos, áreas de tecnologia, segurança da informação e proteção de dados

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

Ano V, v.2 2024 | submissão: 16/02/2024 | aceito: 19/02/2024 | publicação: 22/02/2024

fortalece a capacidade institucional de responder às transformações do ambiente digital, promovendo maior alinhamento entre objetivos estratégicos, inovação e gestão de riscos.

Embora este estudo tenha sido desenvolvido por meio de revisão bibliográfica, os referenciais analisados demonstram convergência quanto à necessidade de tratar a informação como patrimônio estratégico das organizações. A maturidade da governança informacional passa a refletir não apenas o nível de conformidade regulatória alcançado pela instituição, mas também sua capacidade de inovar, preservar a confiança dos diferentes públicos e sustentar decisões fundamentadas em dados confiáveis.

Como perspectivas para pesquisas futuras, recomenda-se aprofundar investigações relacionadas aos impactos da Inteligência Artificial Generativa sobre a governança corporativa, à regulamentação internacional dos sistemas inteligentes, aos modelos de governança para ecossistemas digitais distribuídos e à utilização de métricas capazes de mensurar o retorno estratégico dos investimentos em governança da informação e proteção da privacidade.

Entendemos, portanto, que a governança corporativa da informação representa um dos principais pilares das organizações orientadas por dados. Ao integrar segurança da informação, privacidade, Inteligência Artificial, gestão de riscos e liderança executiva, torna-se possível construir ambientes mais transparentes, resilientes, inovadores e preparados para enfrentar os desafios tecnológicos, regulatórios e competitivos que caracterizam a economia digital contemporânea.

REFERÊNCIAS

- GIL, A. C. *Como Elaborar Projetos de Pesquisa*. 6. Ed. São Paulo: Atlas, 2019.

Governança da Informação e Dados

- DAMA INTERNATIONAL. *DAMA-DMBOK: Data Management Body of Knowledge*. 2. Ed. Bradley Beach: Technics Publications, 2017.
- WEILL, P.; ROSS, J. W. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*. Boston: Harvard Business School Press, 2004.
- DAVENPORT, T. H. *Competing on Analytics: The New Science of Winning*. Boston: Harvard Business School Press, 2007.
- REDMAN, T. H. *Data Driven: Profiting from Your Most Important Business Asset*. Boston: Harvard Business Review Press, 2008.

Segurança da Informação e Gestão

- WHITMAN, M. E.; MATTORD, H. J. *Principles of Information Security*. 7. Ed. Boston: Cengage Learning, 2022.
- ISACA. *COBIT 2019 Framework: Governance and Management Objectives*. Schaumburg: ISACA, 2019.

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

Ano V, v.2 2024 | submissão: 16/02/2024 | aceito: 19/02/2024 | publicação: 22/02/2024

- ISO/IEC 27001:2022. *Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements*.
- ISO/IEC 27701:2019. *Privacy Information Management*.
- ISO/IEC 38500:2015. *Governance of IT for the Organization*.

Privacidade e Inteligência Artificial

- NIST. *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*. Gaithersburg: National Institute of Standards and Technology, 2023.
- NIST. *Cybersecurity Framework (CSF 2.0)*. Gaithersburg: National Institute of Standards and Technology, 2024.
- OECD. *Recommendation of the Council on Artificial Intelligence*. Paris: Organisation for Economic Co-operation and Development, 2019.
- BRASIL. Lei nº 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados Pessoais (LGPD)*.
- REGULAMENTO (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. *General Data Protection Regulation (GDPR)*.

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