REVISTA DE GESTÃO E SECRETARIADO

ISSN: 2178-9010
DOI:
http://doi.org/10.7769/gesec.v15i4.3743

Compliance e gestão de riscos em tempos de inovação e disrupção digital

Compliance and risk management in times of innovation and digital disruption

Cumplimiento y gestión de riesgos en tiempos de innovación y disrupción digital

Daniella Campos[1]

Flavia dos Reis Carreiro[2]

Resumo

A evolução dos programas de compliance e gestão de riscos reflete a necessidade vital de adaptabilidade no cenário empresarial contemporâneo, impulsionado pela constante disrupção tecnológica. Dos princípios tradicionais de conformidade regulatória à integração holística de práticas éticas, culturais e de governança, assim como o enfoque estratégico na eficiência, essa transformação é essencial para garantir a resiliência e o sucesso das organizações diante dos desafios e oportunidades do mundo digital. Este artigo analisa a evolução e desafios dos programas de compliance e gestão de riscos nas organizações diante da crescente evolução tecnológica. Com base em uma revisão abrangente da literatura, destacamos como as organizações estão adaptando suas práticas de compliance e gestão de riscos para enfrentar os desafios impostos pelas inovações tecnológicas, como inteligência artificial, blockchain e Internet das Coisas. Analisamos as oportunidades e desafios apresentados por essa evolução e possíveis direcionamentos para garantir a conformidade e a mitigação de riscos em um ambiente empresarial em constante transformação.

Palavras-chave: Compliance. Riscos. Inovação. Disrupção. Privacidade.

Abstract

The evolution of compliance and risk management programs reflects the vital need for

[1] Especialista em Compliance, Gestão de Riscos e Privacidade, Universidade Candido Mendes, Rio de Janeiro, Rio de Janeiro, Brasil. E-mail: daniellacrj@gmail.com Orcid: https://orcid.org/0009-0002-2424-0343

[2] Mestre em Engenharia Mecânica, Universidade Federal do Rio de Janeiro (UFRJ), Rio de Janeiro, Rio de Janeiro, Brasil. E-mail flaviacarreiro1974@gmail.com Orcid: https://orcid.org/0009-0001-7190-0909

adaptability in today's business landscape, driven by constant technological disruption. From traditional regulatory compliance principles to the holistic integration of ethical, cultural, and governance practices, as well as a strategic focus on efficiency, this transformation is essential to ensure the resilience and success of organizations in the face of the challenges and opportunities of the digital world. This article analyzes the evolution and challenges of compliance and risk management programs in organizations in the face of increasing technological evolution. Based on a comprehensive literature review, we highlight how organizations are adapting their compliance and risk management practices to meet the challenges posed by technological innovations such as artificial intelligence, blockchain and the Internet of Things. We discuss the opportunities and challenges presented by this evolution and possible directions to ensure compliance and risk mitigation in an ever-changing business environment.

Keywords: Compliance. Risks. Innovation. Disruption. Privacy.

Resumen

La evolución de los programas de cumplimiento y gestión de riesgos refleja la necesidad vital de adaptabilidad en el panorama empresarial contemporáneo, impulsada por la constante disrupción tecnológica. Desde los principios tradicionales de cumplimiento normativo hasta la integración holística de las prácticas éticas, culturales y de gobernanza, así como el enfoque estratégico en la eficiencia, esta transformación es esencial para garantizar la resiliencia y el éxito de las organizaciones frente a los desafíos y oportunidades del mundo digital. Este artículo analiza la evolución y los desafíos de los programas de cumplimiento y gestión de riesgos en las organizaciones frente a los crecientes desarrollos tecnológicos. A partir de una revisión bibliográfica exhaustiva, destacamos cómo las organizaciones están adaptando sus prácticas de cumplimiento y gestión de riesgos para hacer frente a los desafíos planteados por las innovaciones tecnológicas como la inteligencia artificial, la cadena de bloques y el Internet de las cosas. Analizamos las oportunidades y desafíos que presentan estos desarrollos y las posibles direcciones para garantizar el cumplimiento y la mitigación de riesgos en un entorno empresarial en constante cambio.

Palabras clave: Cumplimiento. Riesgos. Innovación. Interrupción. Privacidad.

Introdução

A evolução dos programas de compliance e gestão de riscos não é só necessária, como também é um tema de extrema relevância em um cenário empresarial cada vez mais influenciado pela disrupção tecnológica.

Ao longo da última década, os programas de compliance evoluíram de simples medidas de conformidade regulatória para abordagens mais holísticas, que incorporam forte gerenciamento de riscos, avaliando não somente considerações éticas, culturais e de governança corporativa, como a busca pela eficiência. Da mesma forma, a gestão de riscos passou por uma transformação significativa, deixando de ser vista como uma função isolada ou específica para alguns negócios, para se tornar parte integrante da estratégia empresarial.

A disrupção tecnológica desempenha um papel fundamental nesse processo de evolução. Por um lado, as novas tecnologias oferecem oportunidades sem precedentes para melhorar a eficiência operacional, otimizar processos e criar novos produtos e serviços. Por outro lado, elas também introduzem grandes desafios em termos de conformidade regulatória, segurança cibernética e privacidade de dados.

Diante desse cenário, este artigo busca analisar como as empresas pensam atualmente e como estão implementando e percebendo essa evolução no cenário atual e futuro. Se as empresas estão revendo e adaptando seus programas de compliance e gestão de riscos para garantir que permaneçam relevantes e eficazes em um ambiente de negócios em constante mudança.

Adota-se para a realização desta pesquisa o método de abordagem teórica, através da revisão bibliográfica, com objetivo de analisar as oportunidades e desafios apresentados por essa evolução e estratégias para manter a conformidade e a mitigação de riscos em um ambiente empresarial em constante transformação.

Embora as inovações tecnológicas ofereçam vantagens inegáveis, oferecem igualmente desafios e novos riscos associados, incluindo questões relacionadas à segurança cibernética, privacidade de dados e governança de algoritmos. Assim, é crucial examinar como as pessoas, tanto especialistas quanto demais atores da organização, estão navegando nesse ambiente em constante transformação, onde a adoção da tecnologia é inevitável, mas os riscos associados demandam uma abordagem estratégica, proativa e tempestiva. Este artigo busca trazer insights sobre como enfrentar esse paradigma, reconhecendo que o caminho para a integração bem-sucedida da tecnologia requer não apenas adaptação, mas também uma compreensão abrangente dos desafios e das oportunidades que ela apresenta.

Fundamentos de Compliance e Gestão de Riscos

2.1 Compliance

O conceito de compliance deriva do verbo "*to comply*", que significa cumprir, e refere-se à conformidade com normas, regulamentos internos, ou decisões de líderes, entre outros (Coimbra & Manzi, 2010). Originou-se das preocupações de empresas norte-americanas, com diretrizes governamentais desde o início do século XX. Embora não seja novo, o tema ganhou destaque devido à atual situação global de corrupção. Em 1970, nos EUA, foram estabelecidas normas para evitar subornos no comércio internacional, levando as empresas a se adaptarem a essas leis, promovendo a criação de departamentos e programas de compliance.

A corrupção não é um fenômeno exclusivo do Brasil; ela está presente em todas as sociedades, manifestando-se de forma mais exacerbada em alguns países e de maneira mais moderada em outros. Para evidenciar essa realidade, a organização *Transparency International* tem publicado anualmente, desde 1995, o Índice de Percepção de Corrupção (IPC) de aproximadamente 180 países e territórios. Mesmo com variações nas percepções sociais, a corrupção persiste como um problema complexo que não tem solução fácil e pode ocorrer em qualquer momento.

Diversos países se reúnem em fóruns para debater a respeito da Corrupção, e dessas reuniões surgem tratados, conforme apontado por Rose-Ackerman (2009). O Brasil é parte de alguns desses tratados e, como resultado da pressão internacional e interna, promulgou em 1º de agosto de 2013 a Lei n. 12.846, conhecida como "Lei Anticorrupção", e seu decreto atualizado 11.129/2022, que estabelece a responsabilização administrativa e civil de pessoas jurídicas por atos contra a administração pública nacional ou estrangeira.

A promulgação da Lei Anticorrupção trouxe à tona no Brasil o conceito de compliance, De acordo com Castro et al. (2019), o combate à corrupção é promovido por meio de controles que desencorajam práticas corruptas, não se limitando à mera existência da legislação, sendo a aplicação do compliance nas empresas através da implementação de um Programa de Integridade, um sistema de gestão da conformidade efetivo na inibição de práticas corruptas bem como demais irregularidades.

Compliance tem sido uma disciplina de destaque no cenário corporativo, sendo vital integrá-lo aos objetivos estratégicos e aos sistemas de gestão de uma empresa, em vez de tratá-lo como uma série de atividades isoladas ou específicas de determinados setores. Em algumas circunstâncias, essa abordagem pode ser percebida como um entrave à inovação ou como um obstáculo ao

desenvolvimento comercial, em detrimento do cumprimento de normas legais e regulatórias (Giovanini, 2014).

Doyle (2019) destaca a respeito da interseção das atividades de compliance -de um Programa de Integridade e Inovação, sendo não só eficiente como sustentável:

> [...] as atividades de compliance, governança, riscos e inovação podem estar diretamente ligados à solidificação dessa estrutura orientada para o crescimento com a finalidade de alcançar vantagem competitiva. Com base nesta proposição, Compliance – inovação é definida como os processos pelos quais as bases de conhecimento do GRC (Governança, Risco e Compliance) e domínios de inovação são integrados para impulsionar a sustentabilidade e exploração comercial através de processos de tomada de decisão.

Não somente a Lei Anticorrupção, mas vários diplomas legais e normativos fazem parte do universo de compliance, regulamentos, frameworks, que englobam regras e boas práticas relacionadas ao Compliance Digital, Trabalhista, Lavagem de Dinheiro, Compliance Ambiental. Temas que tem evoluído no mundo corporativo nos últimos anos.

Como é o caso da Lei Federal nº 13.709/2018 Lei Geral de Proteção de Dados Pessoais (LGPD), que possui o foco na Privacidade e Proteção de Dados Pessoais, sendo base para implementação de uma Governança que permita mitigação dos riscos nas atividades que realizam tratamento de Dados Pessoais, revendo processos, políticas internas, avaliação de impacto e riscos, mecanismos de supervisão de controles internos e monitoramento contínuo.

Em um cenário de rápido desenvolvimento tecnológico e crescente valorização da ética e transparência, tanto em organizações públicas quanto privadas, o compliance e gestão de riscos corporativos, se tornam ferramentas cruciais de governança corporativa.

O papel do compliance evoluiu para além da esfera jurídica, sendo integrado às áreas de gestão, contribuindo para a adoção de melhores práticas. A avaliação do valor do compliance para as partes interessadas é crucial, assim como a adaptação às constantes mudanças regulatórias. Um sistema de gestão de compliance eficaz requer o mapeamento e gestão de riscos, cuja integração é essencial para alcançar os objetivos da organização (Mustapha at al, 2020).

2.2 Gestão de Riscos

A gestão de riscos teve sua origem nos Estados Unidos em 1963, com a publicação do livro "*Risk management in the business enterprise*", escrito por Robert Mehr. A disseminação e adaptação dessa técnica variou entre os países de acordo com as necessidades, sendo introduzida no Brasil a partir da segunda metade da década de 70.

Em 2013, a Lei nº 12.846, conhecida como Lei Anticorrupção, menciona a gestão de riscos e os controles internos, exigindo a existência de mecanismos internos de integridade. Esses requisitos são detalhados no Decreto nº 8.420/215, atualizado 11.129/2022, que lista parâmetros para avaliar programas de integridade, incluindo a gestão adequada de riscos e sua análise periódica.

As organizações enfrentam riscos em suas operações diárias, originados de agentes internos e externos, podendo ser caracterizados pela frequência de ocorrência e extensão de consequências (impacto) (Kasai et al, 2022). Gerenciar riscos não se limita a minimizar o risco total, mas busca também maximizar oportunidades e garantir a realização dos objetivos planejados. O risco, em sua essência, não é apenas negativo, mas pode também representar oportunidades de progresso (Rampini, 2023).

No ambiente complexo e dinâmico das organizações, o gerenciamento de riscos é essencial para alcançar resultados comerciais positivos e cumprir requisitos regulatórios (Hoyt & Liebenberg, 2011).

O padrão ISO 31000:2018 define riscos como a incerteza que pode afetar os objetivos de uma organização, enquanto a gestão de riscos é descrita como o conjunto de ações coordenadas para orientar e controlar a empresa em relação a esses riscos. Por outro lado, o framework COSO ERM (2017) aborda risco como a chance de um evento ocorrer e impactar os objetivos estratégicos e de negócios da organização, com a gestão de riscos sendo definida como a cultura, habilidades e práticas incorporadas à estratégia e ao desempenho para gerenciar riscos e criar valor.

Apesar das nuances nessas definições, os estudos sobre avaliação e gestão de riscos têm avançado consideravelmente, tornando-se uma parte crucial da governança corporativa em organizações de todos os setores. Isso é alcançado por meio do acompanhamento realizado por conselhos, comitês de auditoria ou gestão de riscos. Modelos de referência destinados à avaliação e gestão de riscos compartilham várias semelhanças, concentrando-se em atividades cíclicas que incluem estratégia, identificação, análise, registro, tratamento e monitoramento de riscos.

Além da ISO 31000:2018 e COSO ERM, relacionado ao uso de tecnologia e todo contexto de inovação digital, destacamos o framework NIST (National Institute os Standarts ans Tecnology).

O NIST 800-037 – *Risk Management Framework for Information Systems and Organization* (2021*)*, é específico para a segurança e privacidade de sistemas de informação. Este modelo inclui atividades como preparação, categorização, seleção e implementação de controles, avaliação, autorização e monitoramento de riscos tecnológicos.

Embora esses frameworks tenham diferenças em sua construção e aplicação geográfica, todos desempenham um papel vital na gestão eficaz de riscos. Enquanto a ISO 31000:2018 tem uma abordagem mais ampla e integrada à gestão de riscos, o COSO ERM Framework foca mais na

governança corporativa geral, e o NIST 800-037 se concentra especificamente na segurança de sistemas de informação.

Paralelo as inovações, surgem discussões sobre a necessidade de revisar ou desenvolver regulamentos, diretrizes, taxonomias, recomendações e modelos para a gestão de riscos relacionados à inteligência artificial (IA), já temos a ISO 42001:2023, publicada em 18 dezembro 2023, incorporando ao arcabouço de diretrizes que especifiquem requisitos para estabelecer, implementar, manter e melhorar o Sistema de Gestão de Inteligência Artificial.

2.3 GRC – Governança, Risco e Compliance

Analisando a evolução das disciplinas nos últimos tempos, devido uma sucessão de escândalos corporativos, tem se destacado a incessante busca por resultados imediatos por parte das corporações. Essa prática coloca em xeque a sobrevivência e a credibilidade das empresas perante seus investidores, podendo até mesmo agravar crises financeiras locais ao minar a confiança do mercado. A demanda por conformidade legal e regulatória em relação à Governança, Riscos e Compliance (GRC) tem crescido de maneira acentuada nos últimos anos (Kindleberger, 2011).

Nos Estados Unidos, diversos marcos legais e eventos históricos moldaram esse contexto, como a responsabilização de pessoas jurídicas por atos de corrupção desde a lei FCPA (1977), a implementação de códigos de governança corporativa em 1978 para mitigar conflitos de interesses, os escândalos empresariais de 2001-2002 e a gestão do ambiente de controles internos prevista na lei Sarbanes-Oxley (2002), além da gestão corporativa de riscos (ERM) determinada pela Dodd-Frank-Act (2010).

Na Europa, programas de ética e compliance foram reforçados globalmente por convenções antissuborno da OCDE (Organização para a Cooperação e desenvolvimento Econômico) e da ONU(Organização das Nações Unidas), enquanto marcos referenciais de governança corporativa, como o Cadbury Report no Reino Unido, foram publicados. Além disso, exigências de gestão de riscos e transparência foram reforçadas pelo acordo de Basiléia II e pelo Aviso n°3 do Banco de Portugal.

As áreas de GRC tem passado por uma significativa evolução ao longo dos anos, especialmente impulsionada pela crescente complexidade do ambiente empresarial e regulatório. Inicialmente, as organizações lidavam com essas questões de forma separada e fragmentada, mas com o tempo perceberam a necessidade de uma abordagem mais integrada e holística..

Nesse contexto, o uso de inovação e tecnologias desempenha um papel crucial. Ferramentas de análise de dados, inteligência artificial e automação de processos têm permitido às organizações

não apenas aumentar a eficiência na gestão de riscos e conformidade, mas também alcançar maior maturidade nesses aspectos. (Moeller, 2015), a adoção de tecnologias avançadas possibilita uma abordagem mais proativa na identificação de riscos e na implementação de controles preventivos, reduzindo assim a probabilidade de ocorrência de incidentes ou violações regulatórias.

A evolução da área de GRC na última década é indissociável do uso crescente de inovação e tecnologias. A integração desses elementos não apenas promove eficiência operacional, mas também fortalece a capacidade das organizações de cumprir seus objetivos e enfrentar os desafios do ambiente empresarial atual.

Tecnologia, Inovação e Disrupção Digital

3.1 Tecnologia

A humanidade está em um processo contínuo de evolução. Durante essa jornada, a tecnologia assumiu diferentes significados e representações, em um constante vaivém com a vida social. Em certos momentos, ela é definida, controlada e racionalizada pelas atividades científico-tecnológicas; em outros, é a tecnociência – uma interdisciplinaridade entre ciência e tecnologia – que se destaca. (Levy, 2010).

Por outro lado, a tecnologia, entendida como um conjunto complexo de técnicas de um domínio particular no espaço sociocultural, requer uma reconstrução constante de sua concepção, de modo que o significado de seus efeitos precisa ser examinado em contextos sociais específicos. Ela está intimamente ligada às variáveis comportamentais no desenvolvimento de produtos e serviços, na organização das sociedades e nas relações de produção e consumo, devendo negociar e aceitar os imperativos da sociedade (Levy, 1998).

Hoje, a maioria de nós está envolvida na produção, transformação ou disseminação de informações. Existem várias definições de tecnologia. De uma forma mais superficial, o conceito de tecnologia pode ser aplicado a tudo o que o ser humano inventa para expandir seus poderes, superar suas limitações físicas, tornar seu trabalho mais fácil e sua vida mais agradável. Além disso, a tecnologia não se limita apenas a instrumentos, ferramentas ou equipamentos tangíveis; ela pode também ser composta por elementos intangíveis, como procedimentos, métodos e técnicas (Veloso, 2011).

A sociedade contemporânea é profundamente influenciada pelas transformações sociais impulsionadas pela tecnologia, que se tornou não apenas um meio, mas também um elemento central na construção das identidades individuais e coletivas. (Mendes, 2015).

É crucial compreender que a tecnologia não é apenas uma ferramenta ou um meio de trabalho; ela é uma extensão do próprio ser humano. No entanto, a interação entre tecnologia e sociedade nem sempre segue em harmonia: enquanto a estrutura tecnológica atual luta para acompanhar o ritmo acelerado da inovação, surgem desafios legais decorrentes dessa disparidade. Nesse cenário, os programas de compliance se tornam cada vez mais essenciais nas organizações, uma vez que as inovações tecnológicas frequentemente esbarram em regulamentações que não foram previstas por seus criadores (Rozatti, 2019).

Portanto, fica claro que os programas de compliance e gerenciamento de risco, se tornam ferramentas indispensáveis para lidar com as tecnologias presentes nos ambientes corporativos. Além disso, é evidente a necessidade de uma utilização adequada das ferramentas tecnológicas e dos recursos de TI, sempre respeitando e preservando os princípios éticos e a cultura organizacional.

3.2 Inteligência Artificial

A Inteligência Artificial (IA) é caracterizada como sistemas computacionais que emulam a inteligência e o pensamento humanos, interagindo, interpretando e aprendendo do ambiente, adaptando dinamicamente seu comportamento com base nessas interações (AI Hleg, 2019). Sua presença é multifacetada, aparecendo tanto em software, como agentes inteligentes, sistemas de recomendação e apoio à tomada de decisão, quanto em hardware, como robôs e dispositivos inteligentes. (Ferràs-Hernández, 2018). Esses sistemas têm a habilidade de coletar e interpretar dados, identificar padrões e produzir resultados para auxiliar processos de decisão e alcançar metas específicas. Eles são amplamente empregados para automatizar tarefas, realizar previsões, embasar decisões e interagir com humanos e outros sistemas através de diversos meios e canais, como texto, áudio, imagens e vídeo (Calagna, 2021).

A evolução da IA ao longo das décadas tem sido marcada por avanços significativos, superando falhas e limitações anteriores para alcançar resultados que rivalizam e até mesmo superam as capacidades humanas em diversos campos. Porém, apesar dos impressionantes progressos, a IA ainda enfrenta desafios, como erros primários e resultados sem sentido, especialmente devido ao viés dos conjuntos de dados utilizados no treinamento dos algoritmos. Isso levanta preocupações sobre o impacto da IA na sociedade e na interação entre os indivíduos, bem como sobre sua capacidade de substituir o livre-arbítrio humano.

Para mitigar os riscos associados à IA, é necessário estabelecer práticas de compliance para sistemas digitais e desenvolver legislações adequadas. Além disso, é essencial continuar

pesquisando e desenvolvendo métodos para avaliar e prever o desempenho dos sistemas de IA, garantindo assim sua utilização ética e responsável em benefício da sociedade.

3.3 Disrupção Digital

A Disrupção Digital é um conceito que descreve a transformação radical e abrupta de processos, indústrias e modelos de negócios causada pela rápida adoção e integração de tecnologias digitais inovadoras. Esse fenômeno tem sido amplamente estudado e discutido devido ao seu impacto significativo em organizações, economias e na sociedade em geral.

O termo "disrupção digital" foi popularizado pelo professor Clayton Christensen da Harvard Business School, em seu livro "The Innovator's Dilemma", publicado em 1997. Christensen definiu a disrupção como "um processo pelo qual um produto ou serviço transforma um mercado estabelecido ao oferecer uma solução mais simples, conveniente e acessível, inicialmente atendendo a uma parte negligenciada do mercado".

A disrupção digital é impulsionada por avanços tecnológicos como a Internet, computação em nuvem, inteligência artificial, big data, Internet das Coisas (IoT), blockchain e automação, entre outros. Essas tecnologias permitem novas formas de interação, produção, distribuição e consumo de bens e serviços, alterando fundamentalmente a maneira como as organizações operam e como os consumidores interagem com elas.

Além do impacto nas indústrias e modelos de negócios, a disrupção digital também está mudando a natureza do trabalho, exigindo novas habilidades e competências dos profissionais. Como observado por Klaus Schwab, fundador do Fórum Econômico Mundial, lançou o conceito de Quarta Revolução Industrial: "Na nova economia, os trabalhadores estão competindo com algoritmos e máquinas inteligentes, que estão substituindo muitas das tarefas realizadas por humanos".

Toda revolução, independentemente de sua natureza, traz consigo vantagens e desvantagens, desafios e oportunidades, incertezas e certezas. No contexto da inovação tecnológica, as vantagens são claras: há um aumento da eficiência, na produtividade, qualidade dos processos. Além disso, o uso de ferramentas que permitem decisões baseadas em dados impulsiona a competitividade, facilitando o desenvolvimento de produtos personalizados que atendem às demandas dos consumidores.

Por outro lado, os especialistas destacam alguns inconvenientes, como a velocidade vertiginosa das mudanças e a necessidade de adaptação a elas, os crescentes riscos cibernéticos que

exigem uma atenção redobrada à segurança digital, a alta dependência tecnológica e a exclusão digital, além da escassez de mão de obra qualificada.

Em suma, a disrupção digital é um fenômeno multifacetado e em constante evolução, que está redefinindo a forma como vivemos, trabalhamos e fazemos negócios. O que é um grande desafio também para profissionais de Compliance e Gestão de Riscos que precisam absorver novos conhecimentos para abraçar a mudança e aproveitar as oportunidades oferecidas pela evolução digital, colocando as empresas bem posicionadas para prosperar em um futuro cada vez mais digitalizado.

3.4 Remodelando Riscos e Compliance com Avanço da Tecnologia

As ferramentas digitais têm desempenhado um papel significativo no aprimoramento da capacidade das empresas de monitorar e gerenciar as áreas de GRC, especificamente riscos e compliance, de forma mais eficiente e eficaz. Elas oferecem insights rápidos e precisos, facilitando a tomada de decisões baseadas em dados e proporcionando uma visão abrangente da empresa.

De acordo com a Pesquisa da Revista Compliance ON TOP 2023, pesquisa realizada entre gestores e líderes da área de compliance e Privacidade, as empresas que operam em setores altamente regulamentados ou possuem operações globais complexas estão adotando essas tecnologias de forma mais proeminente, dada a crescente necessidade de gerenciamento de riscos e conformidade regulatória. Embora a implementação dessas ferramentas ainda varie significativamente de acordo com o porte da empresa e o setor de atuação, é cada vez mais comum incorporar tecnologias avançadas na atividade de compliance.

Embora a qualidade da tecnologia utilizada influencie na redução dos prazos, é importante observar que as ferramentas lidam com dados que requerem análise e contextualização, uma área em que a intervenção humana ainda é necessária.

Ainda de acordo com a pesquisa, os profissionais de compliance estão cada vez mais adotando tecnologias como inteligência artificial, big data e blockchain para melhorar a eficiência e a eficácia de seus programas, observando ser o principal tema de atenção nos anos de 2022 e 2023. Essas ferramentas são utilizadas para automatizar processos de monitoramento, aprimorar a análise de dados e oferecer insights mais precisos e em tempo real sobre questões de conformidade. Por exemplo, sistemas baseados em IA são empregados para detectar padrões anômalos em transações financeiras que podem indicar lavagem de dinheiro ou fraude.

Embora a adoção dessas tecnologias enfrente restrições, como limitações de orçamento, a pesquisa aponta que falta de expertise técnica e preocupações com privacidade e segurança de dados,

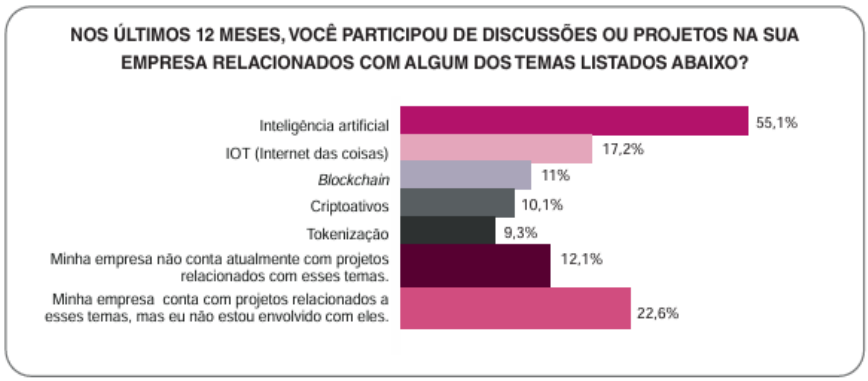
é uma realidade crescente que está moldando a abordagem das empresas em relação ao compliance. A integração de tecnologias avançadas é fundamental não apenas para aumentar a eficiência, mas também para lidar com a complexidade do ambiente regulatório atual.

Por exemplo, a inteligência artificial e a *big data* permitem análises detalhadas de grandes volumes de dados, facilitando a identificação de padrões e tendências que podem indicar riscos de não conformidade. A Internet das Coisas oferece a capacidade de coletar dados em tempo real, crucial para identificar rapidamente desvios nas operações da empresa. O blockchain proporciona um nível de segurança e transparência sem precedentes, especialmente valioso em setores onde a integridade dos registros é crítica. Os criptoativos representam oportunidades para desenvolver sistemas de pagamento mais seguros e transparentes. Importante destacar que a adoção dessas tecnologias no compliance não é apenas uma questão de eficiência, mas também de necessidade, dada a complexidade e impacto do ambiente regulatório atual.

Apesar de todo avanço e benefício a pesquisa aponta a necessidade de, ao adotar essas tecnologias, as empresas devem estar atentas às questões éticas, de privacidade e proteção de dados, além das fraudes e ataques cibernéticos. É essencial garantir que as decisões tomadas por sistemas baseados em IA sejam explicáveis e que haja responsabilidade por suas ações. O viés nos algoritmos de IA deve ser monitorado e corrigido para garantir a justiça e evitar discriminação. Além disso, as empresas devem considerar o impacto social e ambiental das tecnologias que utilizam e implementar uma gestão de riscos eficaz para avaliar e mitigar os riscos associados ao seu uso.

Figura 1

Pesquisa realizada pela Revista Compliance On Top (2023)



Fonte: Compliance on top (2023)

3.5 Cenário Atual da Gestão de Riscos – O Que as Organizações Pensam Atualmente

O cenário em constante evolução do mercado e a crescente complexidade das questões relacionadas aos riscos obrigam as organizações a aprimorar continuamente suas estruturas de governança. No caso das empresas que já possuem práticas ou áreas estruturadas de gerenciamento de riscos, a utilização de ferramentas ou atividades está cada vez mais consolidada.

O emprego de soluções e ferramentas tecnológicas, aliado ao desenvolvimento de profissionais qualificados na compreensão dos riscos em toda a organização, emerge como um elemento fundamental para potencializar a eficácia na identificação e monitoramento de riscos, fortalecendo, assim, a capacidade das empresas em enfrentá-los.

Conforme constatado pela pesquisa realizada pela Deloitte Consultoria sobre o Futuro do Processo da Gestão de Riscos Empresariais, divulgada em abril de 2024, mais da metade das organizações participantes ainda não incorpora ferramentas ou softwares para coletar, gerenciar ou consolidar indicadores para a gestão de riscos. No entanto, tal adoção se torna essencial, uma vez que soluções preditivas, como o *'risk sensing'*, possibilitam uma detecção ativa de riscos emergentes e tendências, propiciando a identificação de oportunidades e contribuindo para a adoção de práticas mais estratégicas e alinhadas aos objetivos da organização. Isso evita que as ações sejam tomadas unicamente em resposta aos riscos materializados.

A pesquisa mostra que as organizações participantes ainda enfrentam desafios relacionados à evolução do processo de gestão de riscos, buscando alcançar maior maturidade. As ferramentas de soluções de Analytics e Inteligência Artificial, por exemplo, são exploradas de maneira inicial e direcionadas principalmente à automação de relatórios e à coleta ou monitoramento de dados. No que diz respeito à IA, em particular, a adoção dessa ferramenta ainda é incipiente nas empresas participantes, mas espera-se que cresça substancialmente nos próximos anos. Isso se dá em virtude do reconhecimento pelo mercado da necessidade de uma maior familiarização com o uso dessas tecnologias, a fim de alcançar ganhos de escalabilidade.

Na figura 4, observa-se o resultado da pesquisa, em que a crise sanitária em 2020 destacou a importância da transformação digital e intensificou a necessidade de investimento em segurança cibernética, devido ao surgimento de novas vulnerabilidades e à descentralização das operações, com o advento do trabalho remoto, visando a proteção das pessoas e a continuidade das atividades. Durante a crise, questões regulatórias e estratégicas cederam lugar a medidas de contingência para manter as operações, com foco nos riscos cibernéticos, devido às mudanças significativas como o aumento do trabalho remoto, o uso de dados fora dos ambientes físicos das empresas, a expansão do e-commerce, a migração para a nuvem e a sofisticação dos ataques cibernéticos. Com a

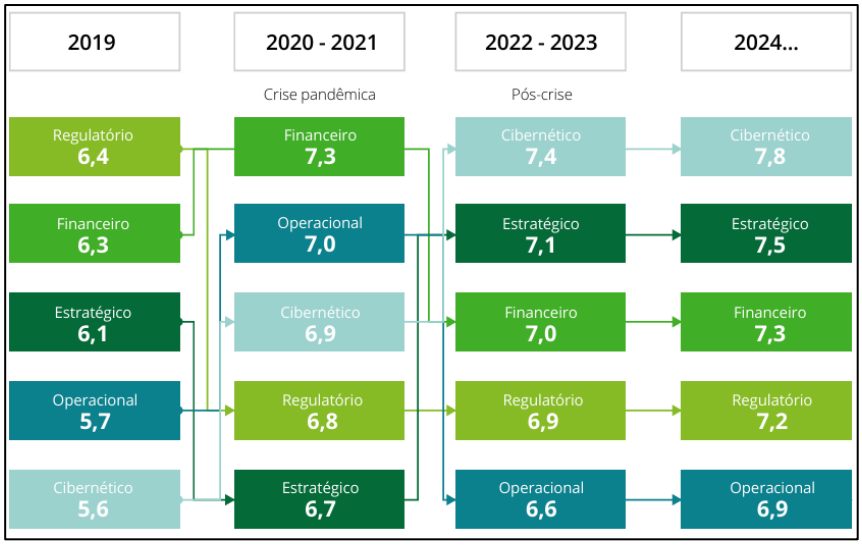
recuperação gradual após o fim da crise em maio de 2023, as empresas começaram a repensar suas estratégias, priorizando o planejamento de médio e longo prazo. Os riscos cibernéticos, que ganharam destaque durante a pandemia devido às novas demandas do mercado, consolidaram-se ainda mais em 2022 e 2023. Para 2024, espera-se que o cenário anterior se repita, com os riscos cibernéticos e estratégicos permanecendo elevados, embora os demais (financeiro, regulatório e operacional) também estejam em níveis superiores ao pré-crise.

Se não nos arriscarmos, não progredimos. A gestão inteligente dos riscos é fundamental para a reinvenção e transformação das empresas, permitindo-lhes sobreviver, criar valor e prosperar em tempos de incerteza, ao mesmo tempo em que desenvolvem a resiliência para proteger seu valor diante de riscos complexos e em constante mutação.

Analisando a pesquisa Global de Riscos 2023, realizada pela PwC Consultoria, "Da ameaça à oportunidade", traz uma avaliação de liderança entre as empresas que estão revolucionando sua abordagem em relação aos riscos, ao abraçarem o potencial transformador da tecnologia e dos dados em busca de oportunidades e criação de valor (Figura 3).

Figura 2

Nível de classificação das categorias de riscos mensuradas pelas organizações, por período.



No questionário, foi solicitado aos respondentes que classificassem, em uma escala de 1 a 10, sendo 1 a mais baixa e 10 a mais alta, qual seria a nota atribuída para cada categoria de risco, considerando os quatro períodos indicados ao lado. Os índices se referem às médias consolidadas da amostra, para cada tipo de riscos, dentro do período apontado.
Fonte: Deloitte (2024)

Entrevistando 3.910 líderes executivos e de risco, desde membros do conselho de administração até o C-Level, em diversas áreas, como tecnologia, operações, finanças, riscos e

auditoria, a pesquisa evidencia o papel cada vez mais crucial da tecnologia na proteção do valor das organizações, mitigando e gerenciando eficazmente os riscos.

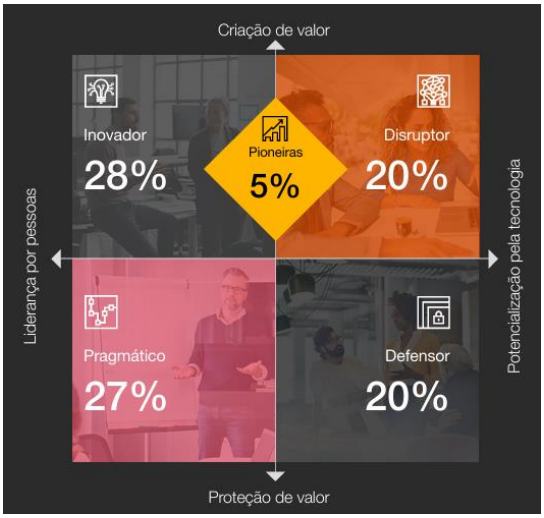
A pesquisa mostra que os líderes brasileiros demonstram um forte impulso para investir em tecnologia como forma de repensar seu cenário de riscos. No Brasil, por exemplo, a inteligência artificial generativa (GenAI) é vista mais como uma oportunidade do que como um risco.

A pesquisa revela um grupo de empresas, representando 5% do total (figura 3), que têm o melhor desempenho em todos os setores da indústria - identificadas como "pioneiras" - estão avançando na busca por oportunidades.

Sustentadas por uma resiliência estratégica que permeia toda a organização, guiadas por uma abordagem de gestão de risco liderada por pessoas e potencializada pela tecnologia, essas empresas pioneiras estão muito mais propensas do que outras a aprimorar suas equipes internas e a fazer um uso mais amplo de análises avançadas (analytics), modelos preditivos, ferramentas de cibersegurança e computação em nuvem para gerenciar riscos. Elas também têm uma probabilidade maior de considerar tecnologias emergentes, como a GenAI, como uma oportunidade em vez de um risco.

Figura 3

Pesquisa Global de Riscos



Fonte: PwC, 2023

Esses comportamentos e os resultados superiores das pioneiras destacam uma lacuna que outras organizações precisam preencher se desejarem utilizar a tecnologia de forma mais eficaz e criar oportunidades e valor a partir dos riscos.

3.6 Ameaças

A penetração da transformação digital nos diversos setores corporativos atingiu um estágio em que a tecnologia está sendo empregada para remodelar fundamentalmente todos os tipos de negócios. A estrutura de uma empresa que busca adotar a transformação digital deve encorajar a tomada de riscos, promover a inovação e cultivar um ambiente de trabalho propício (Nascimento, 2019).

Atualmente, os dados corporativos das organizações estão dispersos em uma variedade de ambientes, incluindo servidores internos, nuvem, dispositivos móveis e aplicativos online, tanto para fins corporativos quanto pessoais. (Jimene,2019). Nas palavras de Pierre Lévy:

> "O volume de informações armazenadas cresce em ritmo acelerado e, portanto, os conhecimentos e habilidades necessários a entender a esfera da "tecnociência" igualmente evoluem na mesma velocidade, a ponto de não mais haver dissociação entre memória pessoal e saber, perante essa escala crescente de dados."

Diante dessas reflexões, torna-se evidente a dimensão que a proteção de dados adquiriu, devido ao volume de dados utilizados em diversas ferramentas tecnológicas, sendo notável a necessidade garantias legais para a privacidade de dados– existentes hoje - especialmente diante das revelações sobre o monitoramento de cidadãos e governos, como as feitas por Edward Snowden no Wikileaks (Pereira, 2019) e os grandes vazamentos e manipulações de dados, incluindo questões eleitorais, como o caso da empresa Cambridge Analytica- Facebook (Pozzi, 2019). Tais acontecimentos têm gerado preocupações na sociedade quanto à rápida circulação de dados e, principalmente, quanto ao seu destino e uso (Silva, 2019).

Com o avanço na capacidade de processamento de dados pelos computadores, e o surgimento do fenômeno da Big Data, que se refere à capacidade computacional de coletar e processar grandes volumes de dados. Isso tem impulsionado a economia compartilhada e o capitalismo de vigilância, que se baseiam na análise das informações geradas pelos usuários para impulsionar o desenvolvimento econômico (Nascimento, 2019).

Os algoritmos de inteligência artificial (IA) estão cada vez mais presentes em uma variedade de áreas, como medicina, educação, indústria, finanças, agricultura, entre outras. Entender o comportamento desses sistemas é crucial para controlar suas ações, aproveitar seus benefícios e mitigar possíveis danos e riscos. Métodos como "Human-in-the-loop" (HITL) - que é um subconjunto de inteligência artificial que utiliza inteligência humana e de máquina para desenvolver modelos de aprendizado de máquina- são recomendados para otimizar essas tecnologias (Cuofano, 2024) (Bannister at al, 2020).

No entanto, diversos incidentes envolvendo algoritmos foram relatados nos últimos anos. Desde algoritmos de recrutamento enviesados, como utilização de critérios não-neutros de gênero, até chatbots que emitiram recomendações perigosas e racistas durante consultas simuladas, como o caso da utilização de um algoritmo de reconhecimento facial da Amazon que classificou incorretamente 28 membros do Congresso como criminosos, esses casos destacam a importância de uma abordagem cautelosa e ética no desenvolvimento e uso de tecnologias de IA (Dastin, 2018) (Farinaccio, 2018).

Os benefícios derivados do uso da tecnologia para processar grandes volumes de dados, identificar padrões e oferecer soluções são amplamente reconhecidos. No entanto, o risco emerge quando a responsabilidade pela tomada de decisões, que normalmente seria atribuída a seres humanos, é delegada a algoritmos (Bradley, 2020).

Yuval Noah Harari, ilustra essa questão ao descrever o cenário em que um algoritmo, e não um humano, avalia a concessão de empréstimos bancários. Esse algoritmo analisa uma vasta quantidade de dados sobre o solicitante e estatísticas de milhões de outros indivíduos para determinar se ele é suficientemente confiável para receber o empréstimo. Embora muitas vezes o algoritmo desempenhe essa função de forma mais eficiente do que um gerente humano, o problema surge quando ocorre discriminação injusta. Se o banco nega o empréstimo a alguém e é questionado sobre os motivos, a resposta muitas vezes é simplesmente "O algoritmo disse não". Isso evidencia e exemplifica a falta de transparência e compreensão sobre as decisões algorítmicas (Unisinus, 2023).

Os algoritmos podem ser tendenciosos, refletindo preconceitos e discriminações existentes na sociedade. A falta de dados de qualidade pode levar a vieses que resultam em decisões incorretas, levantando questões sobre a responsabilidade nessas circunstâncias. Decisões baseadas em bancos de dados históricos podem perpetuar vieses do passado, mesmo que esses vieses não sejam mais aceitáveis pela sociedade atual.

Portanto, apesar dos benefícios trazidos com os avanços tecnológicos, a capacidade avançada de processamento da inteligência artificial (IA), ela carece da capacidade humana de compreender a realidade a partir de perspectivas históricas e ideológicas. A existência de vieses é inegável. Essas preocupações ressaltam a importância da transparência nas decisões automatizadas e a conformidade com regulamentações como a Lei Geral de Proteção de Dados (LGPD) no Brasil que protege os direitos dos titulares de dados e estabelece limites para o uso de informações pessoais (EY, 2023).

Considerações Finais

O avanço tecnológico ocorrido no último século, especialmente nas últimas décadas, tem trazido benefícios reconhecidos pela sociedade, como a otimização de processos, a velocidade das análises e a economia de tempo em tarefas repetitivas.

No entanto, a atividade de Compliance responsável por garantir o cumprimento de normas legais e regulamentares, enfrenta o desafio de abraçar a nova tecnologia enquanto zela pela transparência, segurança e responsabilização. Como conciliar a pregação da privacidade de dados com o uso de uma tecnologia que pode não garantir esse quesito? Como realizar análises de riscos eficientes, preditivas com erros de análise de dados massivos e direcionamentos equivocados? Como promover práticas ambientais sustentáveis quando a tecnologia em questão emite mais carbono que outras atividades econômicas? Como defender a diversidade e a inclusão quando dados falhos podem levar à discriminação?

O uso responsável da IA, inclusive no compliance e gerenciamento de risco, requer abordagens que garantam transparência, segurança e responsabilização desde a concepção das ferramentas. Além disso, é fundamental estabelecer claramente as responsabilidades sobre as decisões tomadas por essa tecnologia.

O crescente uso das tecnologias de IA oferece um campo vasto e promissor para pesquisas futuras sobre seu impacto para indivíduos, organizações e sociedade. No entanto, muitos desafios ainda precisam ser explorados para se atingir uma IA confiável e responsável, dada a complexidade do tema e a evolução vertiginosa dos algoritmos de IA.

Apesar dos desafios, as empresas que agem com coragem e rapidez podem obter vantagem competitiva ao adotar as tecnologias emergentes. A tecnologia revela seu verdadeiro valor quando risco e oportunidade são compreendidos e integrados em todos os aspectos do negócio, promovendo precisão, consistência, confiança e credibilidade. Usar uma tecnologia flexível e escalável permite que as organizações sigam um roteiro gerenciável de mudança.

Podemos observar nas pesquisas realizadas, que o futuro do gerenciamento de riscos empresariais está se movendo em direção a uma integração mais profunda com a estratégia e a cultura organizacional, dentro de um contexto de revolução digital e redefinição das estruturas e responsabilidades dos órgãos de governança.

A sobrevivência e o crescimento sustentável das empresas dependem crucialmente da capacidade de adaptação, mudança e reinvenção em meio às constantes transformações e incertezas. Utilizar o potencial da tecnologia e dos dados de formas inovadoras, juntamente com o desenvolvimento de habilidades multidisciplinares mais diversificadas em toda a

organização, serão essenciais para transformar o risco em um catalisador de mudança e crescimento.

Apontar como melhor estratégia a não atualização e utilização de inovações tecnológicas, como IA, parece tão absurdo quanto investir e decidir na sua utilização sem a preparação adequada aos riscos associados, o equilíbrio, com conhecimento e preparação à frente de uma liderança disruptiva, essa combinação representa uma grande chance de sucesso aos desafios futuros.

Por fim, é importante estabelecer uma cultura organizacional que valorize a ética e a responsabilidade na utilização de novas tecnologias. Isso requer liderança comprometida em priorizar a integridade e a conformidade em todas as decisões relacionadas ao uso de Inovações Tecnológicas, e incentivar uma cultura de questionamento e melhoria contínua.

Referências

Agência EY, (2023), São Paulo. Disponível em https://www.ey.com/pt_br/agencia ey/noticias/compliance-inteligencia-artificial-requer-supervisao-humana.

AI Hleg. (2019a). A Definition of AI: Main Capabilities and Disciplines. In European Commission. Disponível em: https://ec.europa.eu/digital-single-

Bannister, F., & Connolly, R. (2020). Administration by algorithm: A risk management framework. Information Polity, 25(4), 471–490. Disponível em: https://doi.org/10.3233/IP-200249

Bradley, P. (2020). Risk management standards and the active management of malicious intent in artificial superintelligence. AI and Society, 35(2), 319–328.Disponível em: https://doi.org/10.1007/s00146-019-00890-2.

Brandão, C.A. (2022) São Paulo. Um Framework para Gestão de Riscos de Inteligência Artificial nas Organizações. Disponível em : https://repositorio.fgv.br/items/fd71f8f4-8391-4037-8833-b7208120ab7e.

Castro, P. R., Amaral, J. V., & Guerreiro, R. (2019). Aderência ao programa de integridade da lei anticorrupção brasileira e implantação de controles internos. Revista Contabilidade & Finanças, 30(80), 186-201.Disponível em: https://doi.org/10.1590/1808-057x201806780

Cavalari, A.P.F (2019). O Compliance Digital como Tecnologia de Gestão, Disponível em: https://mediacaodesatandonos.org.br/.

Christensen, C. M. (1997). The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail. Harvard Business Review Press.

Coimbra, M. A; Manzi, V.A (Orgs.). (2010) São Paulo. Manual de compliance: preservando a boa governança e a integridade das organizações.

Compliance on top (2023) São Paulo. Disponível em:: https://complianceontop.com.br/wp-content/uploads/2023/12/COMPLIANCE-ON-TOP-2023_web_v3.pdf.

COSO. (2017). Enterprise Risk Management Integrating with strategy and performance. Committee of Sponsoring Organizations of the Treadway Commission, 16. Disponível em: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf.

Cuofano, G. (2024, 1 de abril) Human-in-the-loop AI em poucas palavras, Disponível em: https://fourweekmba.com/pt/humano-no-loop-ai/.

Dastin, J. (2018). Amazon scraps secret AI recruiting tool that showed bias against women | Reuters. Disponível em: https://www.reuters.com/article/us-amazon-com-jobs-automation insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women idUSKCN1MK08G.

Decreto nº. 11.129, de 11 de julho de 2022. Regulamenta a Lei nº 12.846, de 1º de agosto de 2013 [...]. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2022/Decreto/D11129.htm.

Deloitte (2024) Brasil, Disponível em: https:// www2.deloitte.com/content/dam/Deloitte/br/Documents/risk/Os-Cinco-Pilares-dos-Riscos-Empresariais-Deloitte.pdf

Dias, C.C; Ferreira, R.V., (2023). O uso da Inteligência Artificial na atividade de Compliance : Riscos e

DODD-FRANK ACT.(2010). United States House of Representatives. Dodd Frank Wall Street Reform Consumer Protection Act. Disponível em: https://www.cftc.gov/sites/default/files/idc/groups/public/@swaps/documents/file/hr4173_enrolledbill.pdf.

Doyle, E. et al. (2019). Compliance-innovation: A quality-based route to sustainability. Journal of the Cleaner Production Chemical, v. 210, p. 266-275.

Farinaccio, R. (2018) *Reconhecimento facial da Amazon confundiu políticos dos EUA com criminosos.* Disponível em: https://www.tecmundo.com.br/seguranca/132630-reconhecimento-facial-amazon-confundiu-politicos-eua-criminosos.htm

FCPA. United States House of Representatives (1977). Disponível em : https://www.justice.gov/criminal-fraud/foreign-corrupt-practices-act.

Ferràs-Hernández, X. (2018). The Future of Management in a World of Electronic Brains. Journal of Management Inquiry, 27(2), 260–263. Disponível em : https://doi.org/10.1177/1056492617724973

Giovanini, W. (2014). Compliance a excelência na prática. São Paulo.

Hout, R. E.; Liebenberg, A. P. (2011). The value of enterprise risk management. Journal of Risk and Insurance, v. 78, n. 4, p. 795–822.

Instituto Brasileiro de Governança Corporativa, IBGC, (2023). Código das Melhores Práticas de Governança Corporativa, 6ª edição.

ISO (2018). ISO/IEC 31000:2018, Risk management — Guidelines. Disponível em: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1

ISO (2023) ISO/IEC 42001:2023, Information Tecnology Artificial Intelligence Management System. Disponível em : https://www.iso.org/standard/81230.html.

Jimene, C. V. Vainzof, R. (2018) Compliance digital para o seu Programa de Compliance. Ebook Gratuito. São Paulo.. Disponível em: http://www.lecnews.com.br/blog/entenda-mais-sobre compliance-digital/

Kasay, M. Y. et al. (2022) Implantação do processo de gestão de riscos no setor público: estudo de caso em organizações militares. Brazilian Journal of Business, v. 4, n. 2, p. 827–844.

Kindleberger, C.P, Aliber, R.Z.(2011). Manias, Panics and Crashes - A History of Financial Crises. Palgrave Macmillan (St. Martin's Press LLC).

Lei nº. 12.846, de 1º de agosto de 2013. Dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira, e dá outras providências. Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12846.htm.

Lei nº. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015 2018/2018/lei/L13709.htm.

Lévy, Pierre. (2010) Cibercultura: tecnologia e vida social na cultura contemporânea. 5. ed. Porto Alegre: Sulina.

Lévy, Pierre (2014). As Tecnologias da Inteligência. Trad. Carlos Irineu da Costa. 3. ed. São Paulo: Editora 34, 2014. p. 121.

Manyika, J. Lund, S. Chui, M. Bughin, J. Woetzel, L. Batra. P. Ko, R. Sanghvi, S. (2017, 28 de novembro). *O futuro do mercado de trabalho: impacto em empregos, habilidades e salários*. Recuperado de https://www.mckinsey.com/featured-insights/future-of-work/jobs-lost-jobs-gained-what-the-future-of-work-will-mean-for-jobs-skills-and-wages/pt-BR

Mendes, G. Sarlet, I. Wolfgang, C. Alexandre Z. P. (2015) Direito, inovação e tecnologia. São Paulo. Saraiva. p. 94.

Moeller, R. R. (2015)"Brink's Modern Internal Auditing: A Common Body of Knowledge"

Mustapha, A. M. et al. (2020). A systematic literature review on compliance requirements management of business processes. International Journal of System Assurance Engineering and Management, v. 11, n. 3, p. 561–576.

Nascimento, F. A. (2018) Os desafios do Processo de Transformação Digital: Um Estudo de Caso na Indústria Química. Tese de Dissertação de Mestrado. INSPER – Instituto de

Ensino e Pesquisa. São Paulo. p. 18. Disponível em http://dspace.insper.edu.br/xmlui/handle/11224/2155 Acesso em 04 de jul. 2019

NIST. (2021a). Comments Received for RFI on Artificial Intelligence Risk Management Framework. NIST. https://www.nist.gov/itl/ai-risk-management-framework/comments

NIST. (2021c). Summary Analysis of Responses to the NIST Artificial Intelligence Risk Management Framework (AI RMF) - Request for Information (RFI). NIST, 1–10

OCDE.(1997). OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions. Disponível: http://www.oecd.org/corruption/

Pereira, J. P. Snowden, o senhor que seguiu a Assange. Disponível em: https://www.publico.pt/

Pozzi, S. EUA multam Facebook em 5 bilhões de dólares por violar privacidade dos usuários. Disponível em:https://brasil.elpais.com/brasil/2019/07/12/economia/1562962870_283549.html

Price-Westinghouse, PwC, Brasil (2023). Pesquisa Global de Riscos. Disponível em: https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2024/pesquisa-global-de-riscos-2023.html

Rampini, G. H. S. (2023) Impacto da gestão de riscos nos resultados das organizações. 1. ed. Curitiba: Editora Appris. v. 1

Rozatti, J. V. Faleiros Junior. J. L. M. (2019). Estudos Essenciais de Direito Digital. 1 ed. Uberlânida. LAECC. p.311

Silva, F. O. B. (2019). A Responsabilidade do Compliance Officer na Proteção de Dados Pessoais. Revista de Direito e Novas Tecnologias. vol. 3| Abr - Jun 1 2019 DTR\2019\35399.

Transparency International (UK), Disponível em : https://www.transparency.org.uk/?gad_source=1&gclid=CjwKCAjwoa2xBhACEiwA1sb1BIWO2YsMD_s5hqq0bmwzqvMMSCNkpTWHUPTw6yacQCGv-0GKQayDwxoC5ncQAvD_BwE

Veloso, R. Tecnologia da informação e comunicação: desafios e perspectivas. São Paulo. Saraiva, 2011, p. 3

Received: 03.29.2024

Accepted: 04.19.2024