Gestão de Riscos Emergentes

Tácito Augusto Silva Leite

A contribuição da ISO 31050 para o Setor de Segurança

Brasil • 2026

Resumo

Este eBook complementa a apresentação realizada por Tácito Augusto Silva Leite durante o 6º World Security Congress, em São Paulo, nos dias 22 e 23 de abril de 2026. Tácito apresentou a palestra intitulada: Gestão de riscos emergentes: A contribuição da ISO 31050 para o setor de segurança.

Este eBook explora como a norma ISO 31050 contribui para a gestão de riscos emergentes no setor de segurança. Por meio de uma abordagem estruturada e adaptativa, a ISO 31050 fornece diretrizes específicas para identificar e gerenciar riscos emergentes, caracterizados por sua incerteza, complexidade e falta de padrões históricos. O conteúdo abrange a importância de uma gestão proativa de riscos emergentes, sua integração com os objetivos estratégicos das organizações e a comparação com a abordagem de Enterprise Security Risk Management (ESRM) da ASIS, destacando como ambas as abordagens podem ser complementares para alcançar uma gestão holística e eficaz.

O eBook também aborda os desafios culturais e operacionais na implementação da ISO 31050, bem como a importância de superar as limitações de dados e o viés de percepção para alcançar uma gestão eficaz. Com exemplos práticos e estudos de caso, ilustra-se como a antecipação de riscos emergentes pode ser transformada em uma vantagem competitiva, melhorando a resiliência e a sustentabilidade organizacional. Finalmente, são oferecidas recomendações práticas para aplicar a ISO 31050 no contexto de segurança, complementando as práticas atuais e fortalecendo a capacidade organizacional para enfrentar um ambiente em mudança.

Summary

This eBook complements the presentation given by Tácito Augusto Silva Leite during the 6th World Security Congress, in São Paulo, on April 22nd and 23rd, 2026. Tácito delivered the lecture titled: Emerging Risk Management: The Contribution of ISO 31050 to the Security Sector.

This eBook explores how ISO 31050 contributes to the management of emerging risks in the security sector. Through a structured and adaptive approach, ISO 31050 provides specific guidelines for identifying and managing emerging risks, characterized by their uncertainty, complexity, and lack of historical patterns. The content covers the importance of proactive management of emerging risks, their integration with the strategic objectives of organizations, and a comparison with the Enterprise Security Risk Management (ESRM) approach by ASIS, highlighting how both approaches can be complementary to achieve holistic and effective management.

The eBook also addresses cultural and operational challenges in the implementation of ISO 31050, as well as the importance of overcoming data limitations and perception bias to achieve effective management. With practical examples and case studies, it illustrates how anticipating emerging risks can be transformed into a competitive advantage, improving organizational resilience and sustainability. Finally, practical recommendations are offered for applying ISO 31050 in the security context, complementing current practices and strengthening organizational capacity to face a changing environment.

Palavras-chave

ISO 31050; ISO 31000; Gestão de riscos emergentes; Setor de segurança; Incerteza e complexidade; Gestão proativa; Enterprise Security Risk Management (ESRM); Resiliência organizacional; Vantagem competitiva; Riscos e oportunidades.

Sobre o autor

tacitoleite@totalrisk.com.br

www.linkedin.com/in/tacitoleite

http://lattes.cnpq.br/6763601233758573

Tácito Augusto Silva Leite, MSc

DSE, C31000, ASE

Mestre em Gestão de Riscos pela EALDE Business School e UCAM Universidade Católica San Antonio de Murcia, autor do livro Gestão de Riscos na Segurança Patrimonial - consultoriadeseguranca.com.br, Criador da Plataforma t-Risk - totalrisk.com.br, Pós-graduado em Segurança Empresarial pela Universidade Pontifícia Comillas de Madrid, MBA em Gestão de Segurança Empresarial pela Universidade Anhembi-Morumbi (Laureate), MBA em Sistemas de Informação pela Universidade UnP com especialização em Segurança da Informação, Curso de Gestão de Recursos de Defesa pela Escola Superior de Guerra no Brasil, Curso de Formação em Gestão de Riscos e Auditoria baseada em Riscos ISO 31000 pelo QSP, Curso de Terrorismo e Contraterrorismo pela Universiteit Leiden nos Países Baixos e Oficial da Reserva do Exército Brasileiro. Atua desde 1994 na área de gestão de riscos, segurança corporativa e segurança da informação. CEO da plataforma t-Risk e Diretor da ABSEG – Associação Brasileira de Profissionais de Segurança.

Licença de Distribuição

Clique na imagem abaixo para acessar.

Creative Commons License Deed

Atribuição-NãoComercial 4.0 Internacional (CC BY-NC 4.0)

This is a human-readable summary of (and not a substitute for) the license.

Você tem o direito de:

Compartilhar — copiar e redistribuir o material em qualquer suporte ou formato

Adaptar — remixar, transformar, e criar a partir do material

O licenciante não pode revogar estes direitos desde que você respeite os termos da licença.

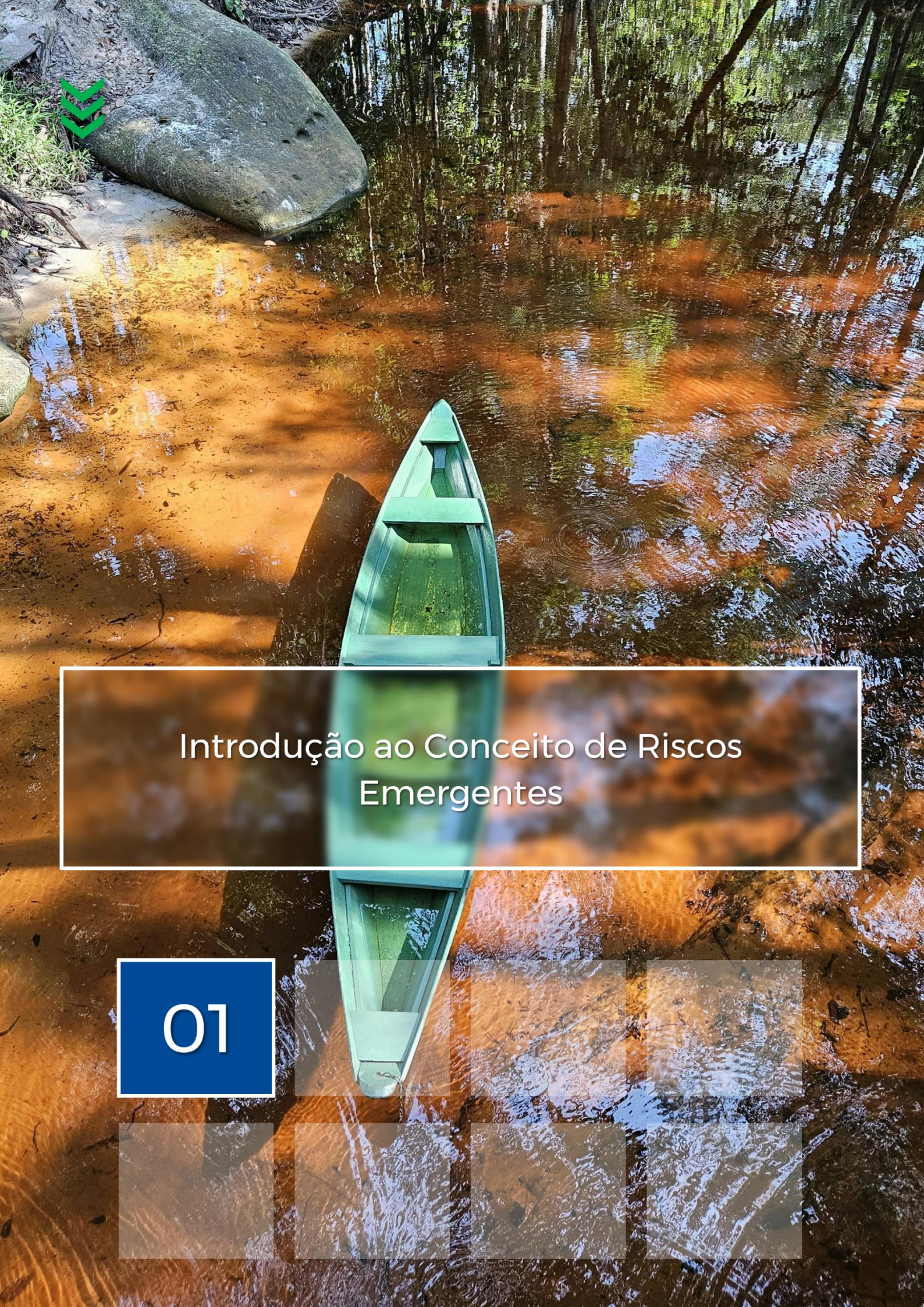
De acordo com os termos seguintes:

Atribuição — Você deve dar o crédito apropriado, prover um link para a licença e indicar se mudanças foram feitas. Você deve fazê-lo em qualquer circunstância razoável, mas de nenhuma maneira que sugira que o licenciante apoia você ou o seu uso.

NãoComercial — Você não pode usar o material para fins comerciais.

Sem restrições adicionais — Você não pode aplicar termos jurídicos ou medidas de caráter tecnológico que restrinjam legalmente outros de fazerem algo que a licença permita.

SUMÁRIO



Introdução ao Conceito de Riscos Emergentes

01

Capítulo 1 – Introdução ao Conceito de Riscos Emergentes

1.1. Breve introdução sobre a ISO no mundo e os comitês técnicos (ABNT/CEE-063)

A Organização Internacional de Normalização (ISO) está presente em mais de 170 países e é uma entidade internacional de normalização que se dedica à criação e padronização de normas técnicas aplicáveis em diversos setores, incluindo a gestão de riscos. A ISO contribui para a harmonização global de práticas, promovendo a eficiência e a segurança em vários campos.

O Comitê Técnico ISO/TC 262 (Global) é responsável pelo desenvolvimento das normas ISO relacionadas à gestão de riscos, com uma ampla contribuição de mais de 70 comitês em todo o mundo, como a ABNT/CEE-063 no Brasil. Este comitê é uma referência em termos de inovação na gestão de riscos, com a participação ativa de profissionais de diversas indústrias.

1.2. Definição e características dos riscos emergentes (baseado na ISO 31050)

A ISO 31050 define os riscos emergentes como fenômenos que não são completamente compreendidos ou previstos devido à sua complexidade e à rapidez com que surgem. Esses riscos estão associados a incertezas que emergem de mudanças dinâmicas nos contextos sociais, tecnológicos, econômicos, ambientais e políticos. Diferentemente dos riscos tradicionais, que podem ser medidos e previstos a partir de dados históricos, os riscos emergentes têm uma natureza disruptiva e, muitas vezes, originam-se de forças externas, desafiando as abordagens convencionais de gestão. A falta de um histórico consolidado torna sua identificação e avaliação mais complexas, exigindo uma abordagem adaptativa e inovadora.

Os riscos emergentes podem ser classificados em várias categorias, dependendo de suas origens e impactos potenciais. Entre as principais categorias encontram-se os riscos tecnológicos, que surgem do desenvolvimento e implementação de novas tecnologias, como a inteligência artificial e a automação avançada. Também se destacam os riscos ambientais, especialmente devido ao impacto das mudanças e eventos climáticos extremos. Além disso, existem riscos sociais, relacionados às mudanças nas expectativas da sociedade, como a maior demanda por práticas ESG, enquanto os riscos regulatórios e políticos referem-se à constante evolução dos marcos legais. Por fim, os riscos econômicos, como crises financeiras e instabilidade nos mercados, também representam um desafio constante para as organizações.

Os riscos emergentes possuem características que os tornam desafiadores para a gestão de riscos convencional. Em primeiro lugar, envolvem um alto grau de incerteza e complexidade, resultado das interações entre múltiplos fatores que não são bem compreendidos. Além disso, sua evolução é rápida e dinâmica, o que torna as estratégias tradicionais de avaliação e tratamento obsoletas. Têm um impacto potencial amplo e sistêmico, afetando não apenas partes específicas da organização, mas também toda a cadeia de valor e até setores inteiros. Outra característica crítica é a falta de dados históricos, o que dificulta a utilização de métodos quantitativos tradicionais na avaliação desses riscos.

Para identificar e gerenciar eficazmente os riscos emergentes, a ISO 31050 propõe o uso de uma combinação de técnicas qualitativas e quantitativas, destacando métodos como a exploração de cenários futuros, que considera variáveis econômicas, sociais, tecnológicas e ambientais. Além disso, as consultas com especialistas são fundamentais, assim como a análise de tendências e sinais fracos no contexto externo, que permitem detectar mudanças em um estágio inicial. O *crowdsourcing* e a inovação aberta também são técnicas úteis, já que a colaboração com diversos *stakeholders* pode revelar informações importantes sobre possíveis mudanças e riscos futuros.

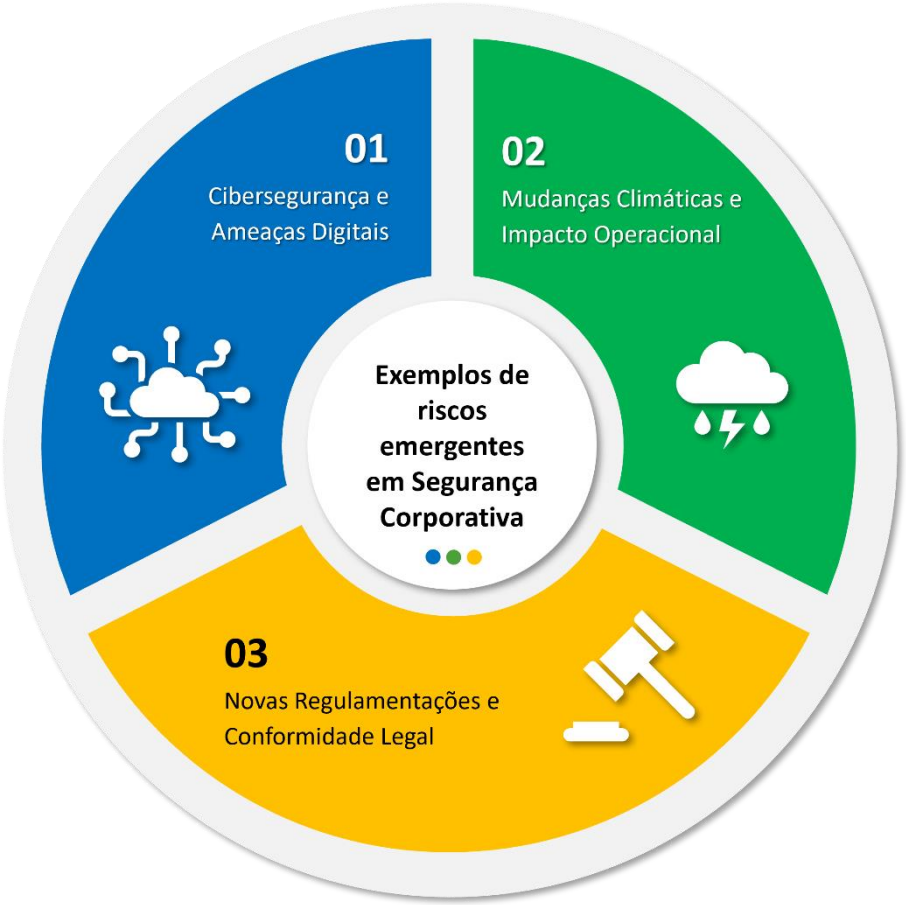
A gestão adequada dos riscos emergentes traz numerosos benefícios estratégicos para as organizações. As empresas que conseguem antecipar e reagir rapidamente aos riscos emergentes fortalecem sua resiliência, minimizando as perdas e adaptando-se mais facilmente às mudanças. Além disso, a gestão proativa desses riscos pode transformar a incerteza em oportunidades, fomentando a inovação e criando vantagens competitivas. Finalmente, demonstrar uma sólida capacidade para gerenciar riscos emergentes reforça a reputação da organização e a confiança dos *stakeholders*, clientes, investidores e parceiros, garantindo a estabilidade e a segurança das operações, mesmo em situações de incerteza.

1.3. Exemplos de riscos emergentes em segurança corporativa

- **Cibersegurança e Ameaças Digitais:** Com o aumento da digitalização, surgiram novos riscos relacionados a ataques cibernéticos, sequestro de dados e violações de privacidade. Esses riscos impactam diretamente a segurança corporativa, pois ameaçam a integridade dos sistemas e os ativos de informação.

- **Mudanças Climáticas e Impacto Operacional:** Os eventos climáticos extremos, como inundações, secas e tempestades, estão aumentando em frequência e intensidade, criando riscos que afetam diretamente as operações e a resiliência das empresas.

- **Novas Regulamentações e Conformidade Legal**: A velocidade das mudanças regulatórias, especialmente em áreas como proteção de dados e ESG *(Environmental, Social and Governance)*, também representa riscos emergentes que as empresas precisam monitorar.



1.4. A importância de antecipar e gerenciar riscos emergentes

Gerenciar os riscos emergentes é essencial para assegurar a continuidade das operações e proteger os ativos das organizações, especialmente no contexto atual, caracterizado pelas dinâmicas descritas nos mundos VUCA e BANI. O mundo VUCA (Volátil, Incerto, Complexo e Ambíguo) descreve um cenário no qual as mudanças são rápidas e imprevisíveis, a incerteza é uma constante, e a complexidade e a ambiguidade desafiam os processos tradicionais de tomada de decisão. Esse ambiente faz com que os riscos emergentes, que não possuem padrões históricos previsíveis, sejam muito mais difíceis de antecipar e controlar.

Por outro lado, o conceito de mundo BANI (Frágil, Ansioso, Não linear e Incompreensível) considera características ainda mais desafiadoras do ambiente atual, como a fragilidade

das estruturas diante de crises inesperadas, a ansiedade gerada pela imprevisibilidade, a não linearidade dos impactos e a dificuldade de compreender a inter-relação entre os eventos. Esses aspectos fazem com que os riscos emergentes não sejam apenas mais frequentes, mas também mais ameaçadores, já que pequenas mudanças podem desencadear efeitos desproporcionais e, muitas vezes, incompreensíveis para as organizações.

Nesse contexto, a antecipação dos riscos emergentes torna-se uma vantagem estratégica fundamental. As empresas que conseguem identificar sinais fracos e antecipar mudanças são capazes de se adaptar rapidamente a novos cenários, garantindo uma maior resiliência diante de mudanças abruptas e eventos disruptivos. A ISO 31050 oferece uma abordagem estruturada para a gestão desses riscos, integrando conhecimento coletivo, tecnologias avançadas e estratégias adaptativas. Esta norma enfatiza a importância de uma gestão proativa, capaz de explorar cenários, envolver os *stakeholders* e utilizar técnicas qualitativas para reconhecer e mitigar riscos antes que se materializem.

Assim, a capacidade de gerenciar riscos emergentes em um mundo BANI e VUCA requer que as empresas não apenas se adaptem, mas que também sejam ágeis, flexíveis e criativas na maneira como respondem aos desafios. Isso inclui o desenvolvimento de uma cultura organizacional que fomente a inovação, a colaboração e o aprendizado contínuo. A gestão eficaz desses riscos permite que as organizações transformem a incerteza em uma oportunidade de crescimento, reforçando sua posição no mercado e garantindo a sustentabilidade de suas operações em um ambiente de constantes mudanças.

ISO 31050: Perspectivas e Contribuições

02

Capítulo 2 – ISO 31050: Perspectivas e Contribuições

2.1. Visão geral da norma ISO 31050:2023 e seu contexto de aplicação

A ISO 31050:2023 é uma extensão importante dos conceitos e práticas estabelecidos pela ISO 31000, especificamente orientada para a identificação e gestão de riscos emergentes em um ambiente global cada vez mais dinâmico e complexo. Esta norma foi desenvolvida para atender às necessidades de organizações que enfrentam desafios sem precedentes, como crises ambientais, avanços tecnológicos disruptivos, mudanças sociais e desafios regulatórios. A ISO 31050 fornece diretrizes detalhadas para o reconhecimento e tratamento de riscos que não apresentam padrões tradicionais ou históricos previsíveis, ajudando as organizações a identificar sinais emergentes e tomar decisões antecipadas.

O contexto de aplicação da ISO 31050 inclui empresas de diferentes portes e setores, já que o risco emergente é transversal e impacta todas as áreas organizacionais. Desde o setor financeiro, que enfrenta crescentes ameaças cibernéticas, até o setor manufatureiro, que deve lidar com questões climáticas que afetam suas cadeias de suprimentos, a norma é uma ferramenta adaptável para mitigar riscos que surgem em ambientes incertos. Além disso, a ISO 31050 é aplicável tanto às operações internas quanto às interações com *stakeholders* externos, promovendo uma visão holística e integrada da gestão de riscos.

2.2. Diferenças e semelhanças entre ISO 31050 e ISO 31000:2018

A ISO 31050 e a ISO 31000 têm objetivos complementares, mas diferem em seu escopo e abordagem. A ISO 31000:2018 é a norma de referência para a gestão de riscos de maneira ampla, aplicável a qualquer tipo de risco em qualquer setor. Estabelece uma estrutura geral para identificar, analisar, avaliar e tratar riscos de maneira sistemática e repetível, sendo amplamente utilizada para a criação de processos e políticas de gestão de riscos.

Por outro lado, a ISO 31050 concentra-se especificamente nos riscos emergentes. Enquanto a ISO 31000 aborda os riscos de maneira geral, a ISO 31050 destaca-se por sua ênfase em antecipar e gerenciar riscos que são novos, incertos e altamente imprevisíveis. A ISO 31050 fornece diretrizes específicas para lidar com riscos emergentes em um ambiente que é volátil, incerto, complexo e ambíguo (VUCA), e que muitas vezes possui características associadas ao mundo BANI (Frágil, Ansioso, Não linear, Incompreensível). Uma das diferenças fundamentais é que a ISO 31050 promove uma abordagem mais exploratória e adaptativa, enquanto a ISO 31000 foca em uma estrutura estruturada e cíclica.

Apesar das diferenças, ambas as normas compartilham a mesma filosofia de que a gestão de riscos é essencial para a criação e proteção de valor em uma organização. Ambas destacam a importância da liderança e o comprometimento da alta direção, bem como a integração da gestão de riscos na governança e na cultura organizacional. Além disso, ambas as normas reforçam a necessidade de um processo de melhoria contínua, o que garante a adaptação constante dos sistemas de gestão de riscos às mudanças no ambiente.

2.3. Como a ISO 31050 complementa a ISO 31000 na gestão de riscos emergentes

A ISO 31050 complementa a ISO 31000 ao fornecer uma abordagem específica nos riscos que surgem como resultado de eventos inesperados e dinâmicas de mudança acelerada. Enquanto a ISO 31000 estabelece a estrutura básica de governança para o processo de gestão de riscos, a ISO 31050 avança, permitindo que as organizações sejam mais proativas e resilientes em relação aos riscos emergentes. A ISO 31050 sugere abordagens que incluem o uso de técnicas prospectivas, como análise de cenários, identificação de sinais fracos e mapeamento de tendências, que permitem às organizações detectar sinais de riscos antes que se materializem.

Além disso, a ISO 31050 reforça a importância de uma cultura organizacional adaptativa, onde a capacidade de aprendizado contínuo e a colaboração são essenciais. Fomenta a

integração de informações obtidas de diversas fontes, incluindo *stakeholders* externos, especialistas e o uso de ferramentas de inteligência artificial para a análise de dados. Dessa forma, a ISO 31050 fortalece os processos estabelecidos pela ISO 31000, fornecendo às organizações as ferramentas necessárias para se prepararem para o inesperado e serem resilientes diante de crises e mudanças.

2.4. Aplicação dos princípios da ISO 31050 no aumento da resiliência organizacional

A resiliência organizacional é um dos principais objetivos da aplicação da ISO 31050. A norma fornece uma série de princípios e metodologias que ajudam as organizações a se adaptarem e se prepararem para mudanças súbitas e riscos emergentes, fortalecendo a capacidade de resistir, adaptar-se e prosperar. Entre os princípios mais importantes destaca-se a necessidade de uma abordagem sistêmica e holística, que abranja não apenas as operações internas, mas também toda a cadeia de valor e os *stakeholders* externos.

A ISO 31050 também destaca a importância da flexibilidade e da adaptabilidade como componentes-chave da resiliência. Isso inclui a adoção de planos de contingência que sejam ágeis e adaptáveis às mudanças no contexto operacional, bem como o desenvolvimento de competências internas para a detecção rápida de riscos emergentes. A norma fomenta a adoção de práticas como o desenvolvimento de cenários e a exploração de incertezas para prever possíveis impactos e preparar respostas adequadas, além de promover uma cultura organizacional que priorize a comunicação aberta e a resposta rápida a crises.

Adotar os princípios da ISO 31050 permite às organizações desenvolver uma postura mais proativa frente ao risco, aumentando sua resiliência e a capacidade de transformar desafios em oportunidades. Ao promover o uso de tecnologias avançadas para o monitoramento e análise de riscos, e integrar o conhecimento dos *stakeholders* no processo de gestão de riscos, a ISO 31050 ajuda a fortalecer a capacidade de adaptação e a resiliência das organizações diante de um ambiente cada vez mais incerto e desafiador.

Processo de Gestão de Riscos emergentes com ISO 31050

03

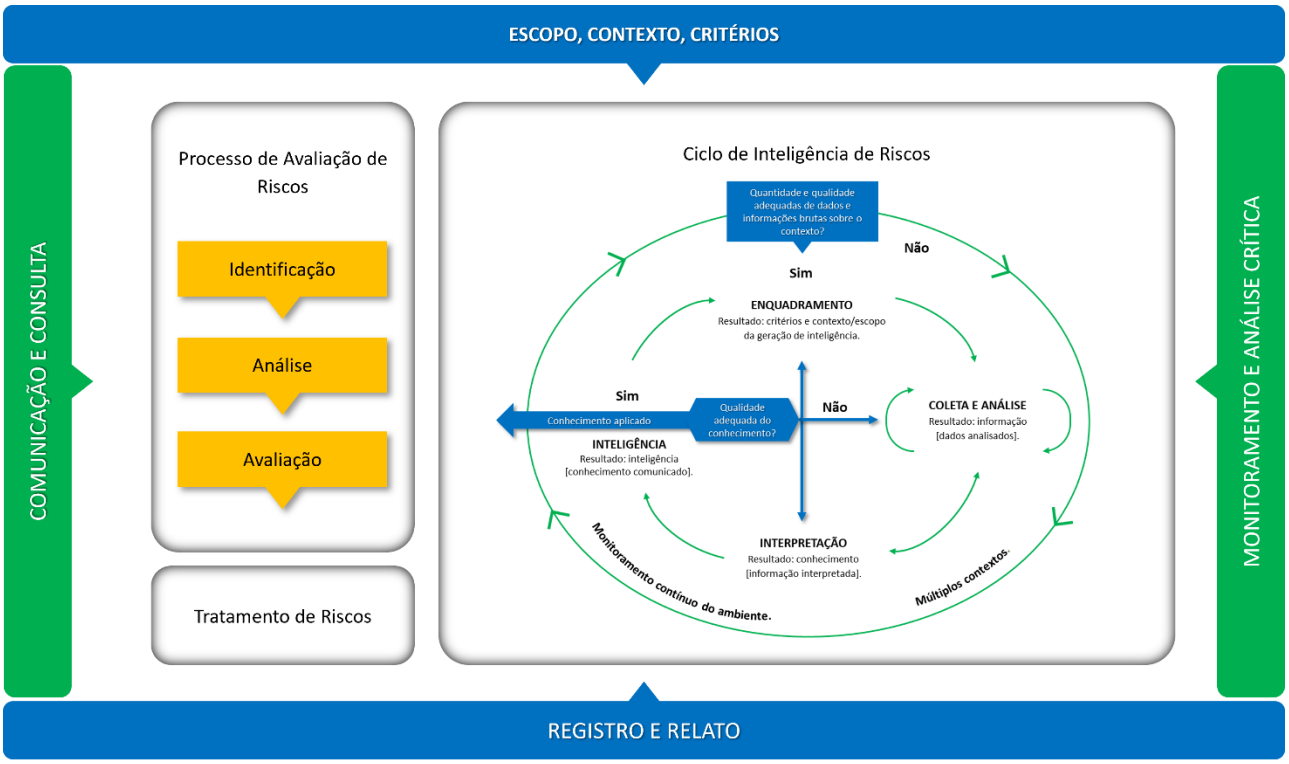
Capítulo 3 – Processo de gestão de riscos emergentes com ISO 31050

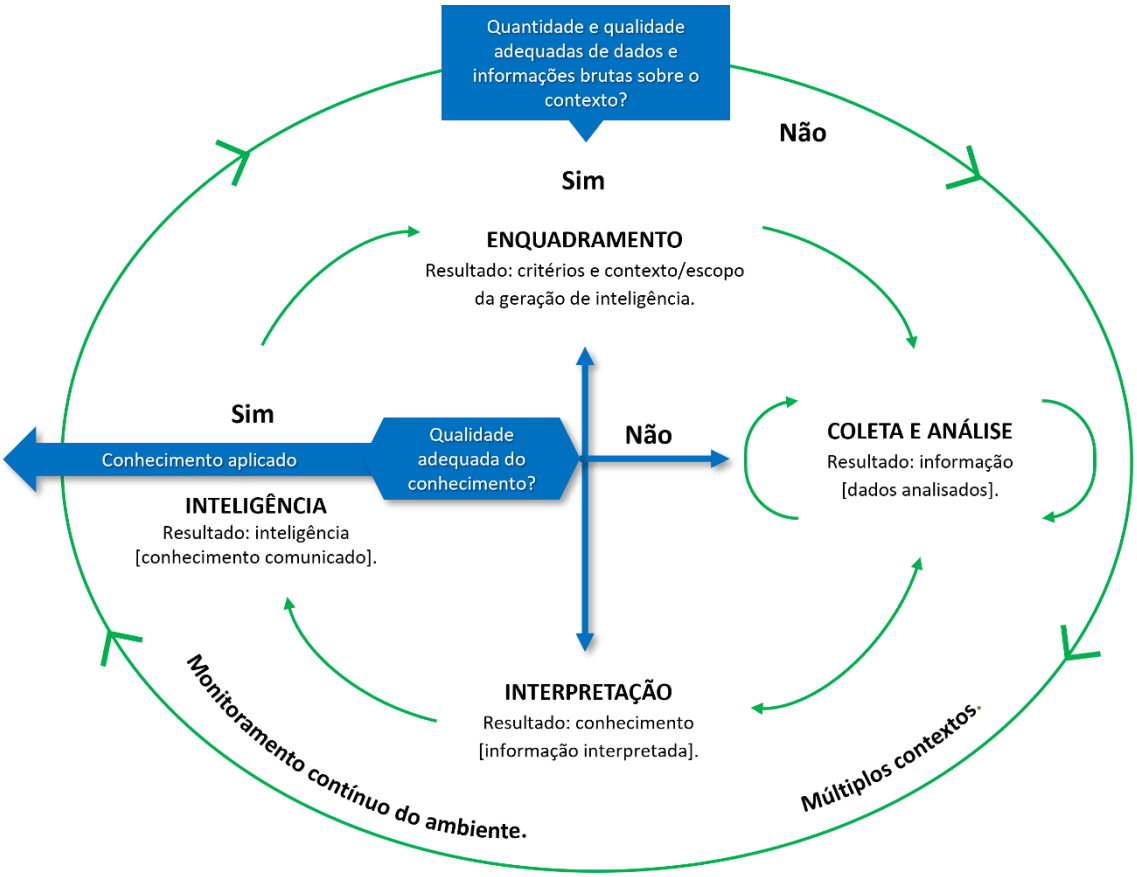
3.1. Ciclo de inteligência de risco: conceitos e aplicação

O ciclo de inteligência de risco é um conceito fundamental introduzido pela ISO 31050 para lidar com a incerteza associada aos riscos emergentes. Este ciclo é composto por várias etapas que buscam monitorar, identificar, avaliar e tratar riscos de forma contínua e adaptativa. O conceito de "inteligência de risco" implica a coleta sistemática de informações relevantes, a análise dessas informações e a disseminação do conhecimento obtido para apoiar as decisões estratégicas.

O processo começa com a identificação de sinais fracos, que são indicadores iniciais de mudanças no ambiente que, de maneira isolada, podem parecer insignificantes, mas que, ao serem analisados em conjunto, podem sinalizar o surgimento de um risco significativo. A análise de tendências e sinais fracos é uma ferramenta essencial para detectar riscos emergentes antes que se manifestem de maneira prejudicial. Posteriormente, a informação coletada é avaliada com o objetivo de determinar sua relevância e o possível impacto na organização, integrando diferentes perspectivas para garantir uma análise abrangente.

O ciclo de inteligência de risco também inclui a etapa de análise preditiva, na qual são utilizados cenários futuros para explorar os possíveis impactos dos riscos emergentes. Com base na análise preditiva e na avaliação dos dados coletados, as organizações podem desenvolver estratégias proativas para tratar os riscos de maneira eficiente. A aplicação do ciclo de inteligência de risco permite que a gestão de riscos emergentes seja uma atividade contínua, que utiliza o aprendizado obtido ao longo do processo para melhorar continuamente a resposta da organização.





Fonte: ISO 31050.

3.2. Adoção de uma abordagem integrada e holística para a gestão de riscos

A ISO 31050 enfatiza a importância de uma abordagem integrada e holística na gestão de riscos emergentes, reconhecendo que os riscos emergentes raramente afetam apenas uma parte da organização de maneira isolada. Esses riscos são multifatoriais e podem impactar diversas áreas simultaneamente, exigindo uma visão ampla e integrada do contexto organizacional para gerenciá-los adequadamente. A abordagem integrada considera as interdependências entre diferentes tipos de riscos, sejam eles estratégicos, operacionais, financeiros, ambientais ou sociais.

A integração dos processos de gestão de riscos com as áreas-chave da organização, incluindo a governança corporativa, operações, planejamento estratégico e comunicação, é fundamental para garantir que todos os aspectos do risco sejam considerados e abordados de maneira coordenada. Essa abordagem também inclui a colaboração entre diferentes *stakeholders*, tanto dentro quanto fora da organização, como parceiros, fornecedores, reguladores e a comunidade. Um aspecto importante da abordagem holística é a coordenação transversal, que permite que diferentes departamentos compartilhem informações e cooperem na identificação e mitigação de riscos.

Além disso, a abordagem holística fomenta a integração da gestão de riscos no dia a dia da organização, fazendo com que todos os níveis hierárquicos, desde a alta direção até os colaboradores da linha de frente, participem do processo de identificação e resposta a riscos emergentes. Essa abordagem não apenas aumenta a eficácia da gestão de riscos, mas também fortalece a cultura organizacional de resiliência e adaptabilidade.

3.3. A necessidade de acumulação de conhecimento verificável e a tomada de decisão sob incerteza

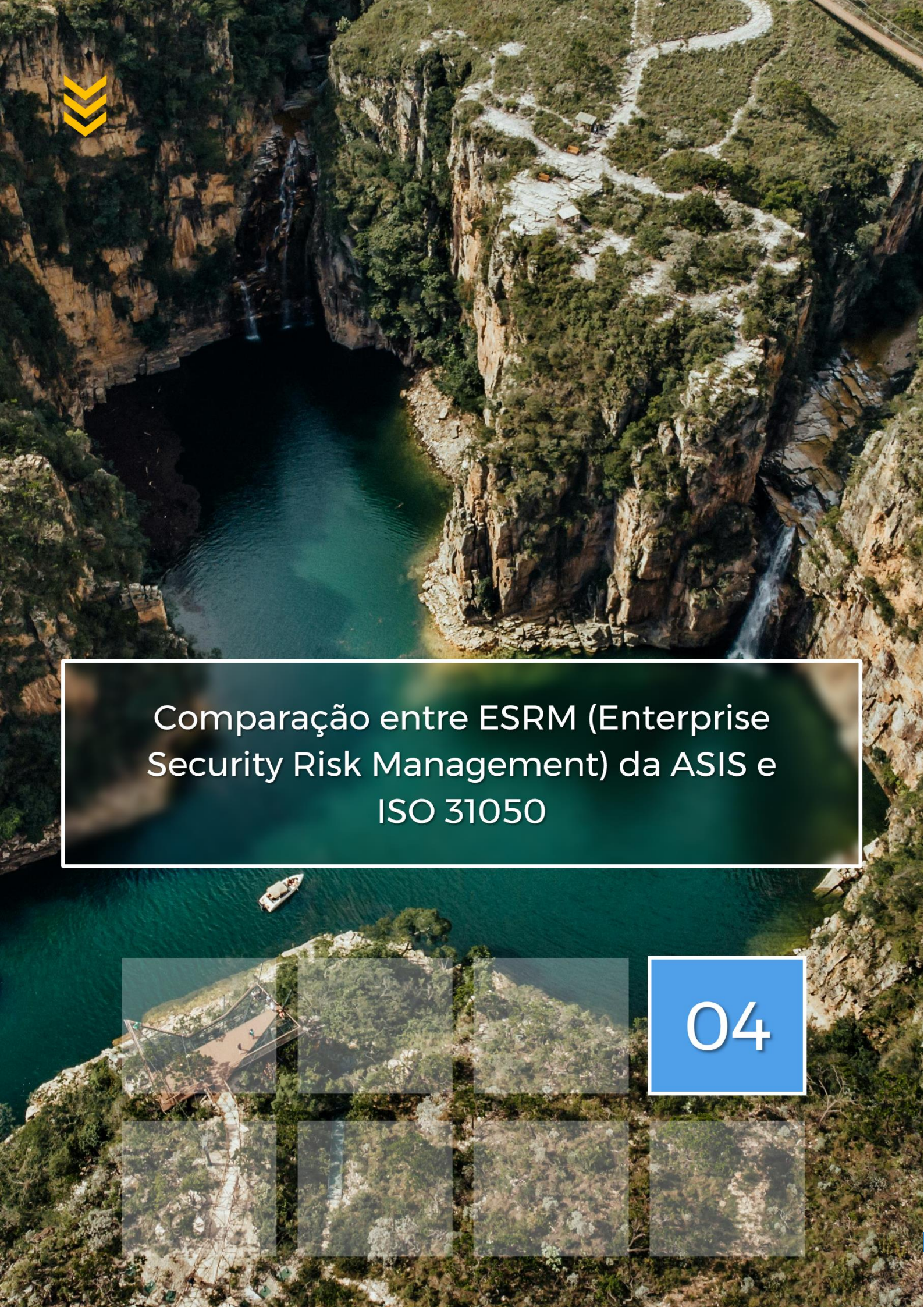
Uma das principais contribuições da ISO 31050 para a gestão de riscos emergentes é o reconhecimento da importância da acumulação de conhecimento verificável como base para a tomada de decisão sob incerteza. Diferentemente dos riscos tradicionais, os riscos emergentes não possuem um histórico consistente que possa ser utilizado para prever comportamentos futuros, o que torna os dados tradicionais insuficientes para uma avaliação precisa. Portanto, a coleta e verificação de informações, através de fontes confiáveis e diversificadas, são fundamentais para construir uma base de conhecimento que apoie decisões informadas.

A acumulação de conhecimento deve ser contínua, utilizando fontes internas e externas, como análise de tendências, pesquisas acadêmicas, relatórios de mercado e consultas com especialistas. Recomenda-se frequentemente o uso de ferramentas de análise de

dados e inteligência artificial para identificar padrões emergentes e fornecer insights sobre possíveis riscos. A utilização de metodologias que permitam a verificação do conhecimento, como a validação cruzada com especialistas e a análise de evidências históricas, é essencial para reduzir a incerteza e aumentar a confiança nas decisões tomadas.

A tomada de decisão sob incerteza requer que as organizações sejam flexíveis e capazes de ajustar suas estratégias conforme novas informações e ideias são obtidas. A ISO 31050 fomenta o uso de cenários prospectivos e a análise de múltiplas alternativas para permitir que as organizações estejam preparadas para uma variedade de futuros possíveis. A experimentação controlada, como a realização de simulações e exercícios de resposta a crises, também é uma prática recomendada para testar diferentes abordagens e validar as melhores estratégias antes que os riscos se materializem. Dessa forma, as decisões podem ser adaptadas e refinadas com base no aprendizado contínuo e na evolução das circunstâncias.

Fonte: ISO 31050.



Comparação entre ESRM (Enterprise Security Risk Management) da ASIS e ISO 31050

04

Capítulo 4 – Comparação entre ESRM (Enterprise Security Risk Management) da ASIS e ISO 31050

4.1. Introdução ao conceito de ESRM e sua relevância para a segurança corporativa

O conceito de *Enterprise Security Risk Management* (ESRM) foi desenvolvido pela ASIS para fornecer uma estrutura de gestão de riscos de segurança corporativa que abranja todos os níveis de uma organização, com um foco prioritário na segurança. O ESRM concentra-se em identificar, analisar, avaliar, controlar e gerenciar os riscos relacionados à segurança dos ativos, sejam eles físicos, digitais ou humanos, sempre alinhando as práticas de segurança com os objetivos estratégicos da organização. Esse conceito adota uma abordagem centrada no negócio, buscando integrar a segurança no planejamento estratégico e assegurando que todos os *stakeholders* compreendam o papel da segurança na proteção do valor organizacional.

A relevância do ESRM no contexto da segurança corporativa reside em sua capacidade de integrar as funções de segurança em todos os níveis da organização, promovendo uma visão clara e compartilhada dos riscos de segurança. O ESRM enfatiza o papel da segurança como facilitador do sucesso empresarial, em vez de ser vista apenas como um custo ou uma atividade isolada. Fornece uma estrutura que abrange desde a análise de ameaças e vulnerabilidades até a implementação de medidas de mitigação, garantindo que a segurança seja uma responsabilidade compartilhada e que os riscos sejam gerenciados de maneira eficaz e contínua.

ESRM - Enterprise Security Risk Management

4.2. Princípios da avaliação de riscos de segurança no contexto do ESRM e da ISO 31050

O processo de avaliação de riscos descrito no ESRM é idêntico ao processo descrito na ISO 31000, que, por sua vez, é a base para o desenvolvimento da ISO 31050. Tanto o ESRM quanto a ISO 31000 compartilham a estrutura fundamental da gestão de riscos, que inclui etapas de identificação, análise, avaliação e tratamento de riscos, sempre alinhadas com os objetivos estratégicos da organização. Essa estrutura permite que a avaliação de riscos seja realizada de maneira sistemática e repetível, integrando-se às operações organizacionais e garantindo que todos os riscos sejam considerados adequadamente.

No contexto do ESRM, a avaliação de riscos de segurança é realizada com o objetivo principal de proteger os ativos mais importantes da organização, que podem incluir pessoas, propriedades físicas, informações e reputação. O ESRM busca avaliar não apenas as ameaças identificáveis, mas também a vulnerabilidade dos ativos e o impacto potencial em caso de incidentes. Com isso, é possível priorizar ações de segurança que gerem maior valor para o negócio, assegurando que a gestão de riscos esteja diretamente conectada com os objetivos organizacionais e a proteção do valor da empresa.

Por outro lado, a ISO 31050 expande a perspectiva da avaliação de riscos para abranger os riscos emergentes, aqueles que surgem de mudanças inesperadas e, muitas vezes, disruptivas no ambiente organizacional ou externo. A ISO 31050 foca em identificar riscos que são complexos, voláteis e incertos, promovendo uma abordagem mais ampla que transcende a segurança física ou digital. Assim, enquanto o ESRM tem um foco específico na proteção dos ativos atuais contra ameaças concretas, a ISO 31050 enfatiza a importância de antecipar novos riscos, analisar tendências e preparar a organização para desafios futuros. Esta norma abrange um espectro mais amplo de riscos, incluindo aspectos operacionais, financeiros e estratégicos, além dos riscos de segurança.

Em resumo, tanto o ESRM quanto a ISO 31050 compartilham a estrutura de avaliação de riscos da ISO 31000, mas divergem em seus focos específicos. Enquanto o ESRM prioriza a mitigação de ameaças à segurança dos ativos e a continuidade das operações, a ISO 31050 foca na antecipação e preparação para riscos emergentes, ajudando a organização a se adaptar e responder a um ambiente em constante transformação.

4.3. Comparação entre os princípios do ESRM e a abordagem da ISO 31050

A comparação entre os princípios do ESRM e a abordagem da ISO 31050 revela tanto convergências quanto diferenças importantes que enriquecem a gestão de riscos corporativos. O ESRM e a ISO 31050 compartilham o princípio de que a gestão de riscos deve estar integrada aos objetivos estratégicos da organização, promovendo uma abordagem proativa e participativa. Ambas as estruturas reconhecem que a gestão de riscos deve ser parte integrante da cultura organizacional e deve envolver todas as áreas e níveis hierárquicos da empresa.

Uma diferença fundamental reside no escopo e na forma de aplicação. O ESRM tem um foco mais específico na segurança corporativa, abordando riscos que afetam diretamente a integridade dos ativos e a proteção contra ameaças identificáveis. Está orientado a garantir que as funções de segurança se alinhem com as prioridades do negócio, mitigando as vulnerabilidades que possam impactar diretamente a continuidade das operações e a proteção dos ativos. A ISO 31050, por outro lado, é mais ampla e preocupa-se em abordar riscos emergentes e pouco conhecidos, promovendo uma abordagem exploratória que envolve a análise de tendências, a identificação de sinais fracos e o desenvolvimento de estratégias adaptativas.

Enquanto o ESRM adota uma abordagem de “proteção de ativos”, a ISO 31050 adota uma abordagem mais orientada à resiliência organizacional. Isso significa que o ESRM prioriza a redução de vulnerabilidades e a segurança imediata dos ativos, enquanto a ISO 31050 foca em preparar a organização para enfrentar um ambiente incerto e em constante mudança, capacitando-a não apenas para mitigar riscos, mas também para encontrar oportunidades de crescimento em meio à incerteza.

4.4. Ponto de convergência: como alinhar ESRM com ISO 31050 para uma gestão estratégica

Os pontos de convergência entre o ESRM e a ISO 31050 oferecem uma oportunidade única para alinhar ambas as abordagens e criar uma estrutura robusta de gestão de riscos e segurança. Integrar o ESRM e a ISO 31050 permite que a organização não apenas proteja seus ativos de maneira eficiente, mas que também esteja preparada para se adaptar a mudanças e responder a riscos emergentes. Esse alinhamento cria um sistema de gestão que é tanto reativo, na proteção contra ameaças e vulnerabilidades já conhecidas, quanto proativo, na antecipação e preparação para novos desafios.

Um ponto-chave de alinhamento é o foco compartilhado em integrar a gestão de riscos com os objetivos estratégicos da organização. Ambas as estruturas enfatizam que as

atividades de segurança e de gestão de riscos não devem ser realizadas de maneira isolada, mas devem estar conectadas com os objetivos de crescimento, inovação e sustentabilidade do negócio. Assim, ao implementar uma estratégia combinada, a organização é capaz de proteger seus ativos mais importantes enquanto constrói resiliência para enfrentar os riscos do futuro.

Outro ponto de convergência é a ênfase na colaboração entre *stakeholders* e na difusão da responsabilidade da gestão de riscos por todos os níveis da organização. Utilizando os princípios do ESRM, é possível garantir que as funções de segurança sejam reconhecidas como parte integrante do processo de criação de valor. Ao aplicar a ISO 31050 em conjunto, as organizações podem assegurar o monitoramento contínuo do ambiente externo, identificando sinais de mudança e ajustando suas estratégias para lidar tanto com ameaças iminentes quanto com riscos emergentes. Dessa forma, a integração do ESRM com a ISO 31050 proporciona uma visão holística da segurança e da gestão de riscos, que fortalece a capacidade organizacional de responder a desafios complexos e incertos de maneira estratégica e resiliente.

Transformação de Incertezas em Oportunidades

05

Capítulo 5 – Transformação de Incertezas em Oportunidades

5.1. Como a ISO 31050 facilita a transformação de riscos em vantagens competitivas

A ISO 31050 fornece um guia prático para transformar os riscos emergentes, que frequentemente se apresentam como incertezas complexas e imprevisíveis, em oportunidades estratégicas para a organização. A norma facilita essa transformação ao fomentar uma abordagem proativa e adaptativa para a gestão de riscos, integrando ferramentas como a análise preditiva e a exploração de cenários futuros. A identificação antecipada de riscos emergentes permite que as organizações se preparem para responder rapidamente e se posicionem de forma vantajosa frente aos seus concorrentes.

Por exemplo, a ISO 31050 incentiva o desenvolvimento de estratégias que não apenas minimizem os impactos dos riscos, mas também maximizem as oportunidades que possam surgir. Quando se detecta um risco emergente, a organização tem a oportunidade de inovar e se adaptar antes das outras, criando novas linhas de produtos ou serviços, ajustando processos internos para uma maior eficiência ou até estabelecendo alianças estratégicas que aproveitem as condições do mercado. Dessa maneira, ao abordar os riscos emergentes como fontes potenciais de inovação, as empresas podem reforçar sua posição competitiva e explorar novos mercados, promovendo o crescimento sustentável e a criação de valor a longo prazo.

5.2. Estudos de caso e exemplos de aplicação no setor de segurança

Para ilustrar como a ISO 31050 pode transformar riscos em oportunidades, podemos considerar alguns estudos de caso. Um exemplo é o de uma empresa de segurança que, ao adotar a ISO 31050, conseguiu identificar e se preparar para o aumento das ameaças cibernéticas, impulsionadas pela crescente digitalização dos serviços de segurança. Essa empresa não apenas implementou medidas de proteção aprimoradas, mas também desenvolveu novos serviços focados em cibersegurança, como consultoria em proteção de dados e auditorias de segurança digital. Como resultado, criou uma nova linha de negócios altamente demandada por seus clientes. Um exemplo prático é Prosegur/SegurPro – https://www.prosegur.com/sobre-nosotros . No Brasil, a média do ROI (retorno sobre o investimento) é de aproximadamente 5% em vigilância tradicional, 25% em segurança eletrônica e mais de 50% em cibersegurança.

Um exemplo que demonstra a criticidade dos riscos emergentes é o de uma grande empresa de logística que opera em um porto internacional e enfrentou uma combinação

de riscos relacionados à cibersegurança, às mudanças climáticas e a novas regulamentações. Imagine que um evento climático extremo, como uma inundação significativa, afetou a infraestrutura do porto, causando a interrupção do fornecimento de energia e dos sistemas de comunicação. Durante a crise, hackers aproveitaram as vulnerabilidades criadas para lançar um ataque cibernético direcionado, sequestrando dados críticos e exigindo um resgate. Simultaneamente, a empresa enfrentava pressões regulatórias para garantir a conformidade com novas normas de ESG e proteção de dados, que exigiam transparência sobre as ações tomadas em resposta à crise climática e seus impactos nos dados dos clientes.

Este cenário mostra como a combinação de diferentes tipos de riscos emergentes pode resultar em uma situação complexa e sistêmica, na qual os impactos se multiplicam devido à interação entre eventos climáticos extremos, ameaças cibernéticas e exigências regulatórias. A incapacidade da empresa de responder adequadamente a cada uma dessas dimensões resultou em uma série de desafios operacionais, financeiros e de reputação que poderiam ter efeitos duradouros.

A aplicação dos princípios da ISO 31050 seria fundamental para mitigar os efeitos desse tipo de risco emergente. A ISO 31050 recomenda uma abordagem integrada e adaptativa para a gestão de riscos, que inclui a identificação de sinais fracos, a antecipação de possíveis ameaças e o desenvolvimento de planos de contingência sólidos. No caso dessa empresa de logística, adotar as práticas da ISO 31050 poderia ter levado a uma preparação antecipada para cenários de crise climática, ao fortalecimento das defesas cibernéticas e ao estabelecimento de mecanismos para garantir a conformidade normativa mesmo em situações adversas. Dessa forma, a abordagem integrada da ISO 31050 permitiria não apenas a mitigação dos riscos individuais, mas também a coordenação efetiva entre diferentes áreas, garantindo uma resposta coesa e minimizando os impactos negativos.

Esses exemplos ilustram como a antecipação e a preparação proativas para riscos emergentes permitem que as organizações não apenas resistam aos desafios, mas que também se adaptem e cresçam em meio às mudanças, transformando possíveis ameaças em oportunidades de inovação e diferenciação.

5.3. Benefícios da gestão de riscos emergentes para a resiliência e a sustentabilidade organizacional

A gestão de riscos emergentes traz uma série de benefícios que são fundamentais para fortalecer a resiliência e a sustentabilidade organizacional. Em primeiro lugar, ao implementar as diretrizes da ISO 31050, as empresas conseguem antecipar riscos e responder de maneira ágil e coordenada, minimizando os impactos negativos e garantindo a continuidade de suas operações. Essa capacidade de resposta rápida, especialmente em um contexto de mudanças abruptas e imprevisíveis, é um dos principais pilares da resiliência organizacional.

Além disso, a ISO 31050 promove uma visão estratégica a longo prazo que considera as incertezas do ambiente e fomenta a inovação como resposta adaptativa aos riscos. Dessa maneira, as empresas estão capacitadas não apenas para reagir às ameaças, mas também para moldar seu futuro, identificando e aproveitando oportunidades para crescer de forma sustentável. A abordagem orientada para o futuro da ISO 31050 reforça a sustentabilidade organizacional, já que considera não apenas a sobrevivência imediata, mas também a capacidade de se adaptar continuamente e prosperar em um ambiente em constante transformação.

A gestão eficaz dos riscos emergentes também contribui para a criação de uma cultura organizacional resiliente, na qual a identificação de riscos e a tomada de decisão sob incerteza são percebidas como oportunidades de aprendizado e crescimento. Essa cultura promove a comunicação aberta, a participação de todos os níveis da organização na gestão de riscos e a criação de estratégias que valorizem tanto a mitigação de riscos quanto a exploração de novas oportunidades. Dessa forma, a ISO 31050 ajuda a transformar a gestão de riscos emergentes em uma ferramenta essencial para o fortalecimento da resiliência e da sustentabilidade a longo prazo.

Integração da Gestão de Riscos Emergentes com os Objetivos Corporativos

06

Capítulo 6 – Integração da Gestão de Riscos Emergentes com os Objetivos Corporativos

6.1. A importância da integração com os objetivos estratégicos da organização

A integração da gestão de riscos emergentes com os objetivos estratégicos da organização é fundamental para garantir que a gestão de riscos não seja uma atividade isolada, mas sim uma parte essencial do planejamento corporativo. Em um ambiente de negócios cada vez mais volátil e incerto, gerenciar riscos emergentes de maneira alinhada com os objetivos estratégicos permite que a empresa esteja preparada para se adaptar e responder rapidamente às mudanças, protegendo sua sustentabilidade e fortalecendo sua posição competitiva.

Quando a gestão de riscos está alinhada com os objetivos estratégicos, as decisões relacionadas aos riscos são tomadas com uma visão clara do impacto nas metas organizacionais. Isso permite que as ações de mitigação sejam direcionadas para proteger as áreas mais críticas para o sucesso da organização. Além disso, a integração permite que a gestão de riscos atue como facilitadora da inovação e do crescimento sustentável, já que identificar e gerenciar riscos emergentes também pode revelar novas oportunidades alinhadas com as ambições da empresa.

6.2. Contribuições da ISO 31050 para o alinhamento das estratégias de segurança com as metas corporativas

A ISO 31050 fornece diretrizes para alinhar a gestão de riscos emergentes com os objetivos corporativos, promovendo uma abordagem holística e adaptativa que contribui para a sustentabilidade a longo prazo. A norma enfatiza a importância de incorporar a avaliação de riscos emergentes no processo de definição estratégica, considerando os cenários futuros e as incertezas que podem impactar o ambiente empresarial. Ao integrar os princípios da ISO 31050, as organizações conseguem adaptar suas estratégias de segurança para não apenas proteger seus ativos e operações, mas também apoiar a execução de suas metas e objetivos.

Uma das principais contribuições da ISO 31050 é a abordagem prospectiva na gestão de riscos, que incentiva as organizações a analisar tendências e sinais fracos para identificar riscos que possam afetar o futuro. Isso permite que a empresa adote uma postura proativa, desenvolvendo estratégias de segurança que estão diretamente vinculadas ao sucesso corporativo. Além disso, a norma promove uma cultura de resiliência organizacional, que é fundamental para alinhar a gestão de riscos com as metas estratégicas, garantindo que a empresa seja capaz de se adaptar a mudanças abruptas e inesperadas.

Outro ponto importante é o ciclo de inteligência, muito bem documentado e estruturado na ISO 31050, que orienta as organizações a coletar, analisar e disseminar informações de maneira contínua. Este ciclo permite a antecipação de riscos emergentes e uma tomada de decisão fundamentada, reforçando a postura proativa e adaptativa frente aos desafios futuros.

6.3. Exemplos práticos de alinhamento e resultados obtidos

Um exemplo prático de integração entre a gestão de riscos emergentes e os objetivos corporativos pode ser observado em uma empresa do setor de energia que, ao adotar a ISO 31050, conseguiu alinhar suas estratégias de segurança com suas metas de crescimento sustentável. A empresa identificou que os riscos emergentes relacionados às mudanças climáticas e à transição energética poderiam impactar suas operações e seus planos de expansão. Com base nos princípios da ISO 31050, a organização realizou uma análise prospectiva dos riscos climáticos, desenvolvendo planos de adaptação que incluíam a modernização de sua infraestrutura e a adoção de tecnologias verdes.

Essa abordagem não apenas mitigou os riscos associados a eventos climáticos extremos, mas também criou novas oportunidades de crescimento para a empresa, que se

posicionou como líder na transição para fontes de energia mais limpas e sustentáveis. Outro exemplo pode ser visto em uma empresa do setor financeiro que, ao integrar a gestão de riscos emergentes com suas metas de inovação tecnológica, adotou medidas proativas de cibersegurança que permitiram o desenvolvimento seguro de novos serviços digitais. Essa integração não apenas minimizou os riscos cibernéticos, mas também contribuiu para a expansão de sua base de clientes e para o fortalecimento da confiança no mercado.

Esses exemplos demonstram como a aplicação da ISO 31050 na gestão de riscos emergentes pode fortalecer a conexão entre segurança, inovação e crescimento estratégico, garantindo que as iniciativas de mitigação de riscos estejam sempre em sintonia com os objetivos corporativos.

Desafios na Implementação da ISO 31050 no Setor de Segurança

07

Capítulo 7 – Desafios na Implementação da ISO 31050 no Setor de Segurança

7.1. Principais barreiras culturais e operacionais

A implementação da ISO 31050 no setor de segurança enfrenta uma série de barreiras culturais e operacionais que devem ser abordadas para que o processo seja eficaz. Em termos culturais, uma das maiores dificuldades é promover uma mudança de mentalidade dentro da organização, que frequentemente está acostumada a lidar com os riscos de maneira reativa, gerenciando as consequências apenas quando os riscos se materializam. Essa cultura reativa contrasta com a abordagem proativa proposta pela ISO 31050, que requer a identificação antecipada e a antecipação de riscos emergentes antes que causem danos significativos. Para muitos colaboradores e gestores, essa mudança implica abandonar práticas tradicionais, o que pode gerar resistência, especialmente em indústrias onde a gestão de riscos é percebida como uma responsabilidade exclusiva de departamentos especializados, como segurança patrimonial, segurança do trabalho e cibersegurança.

Outra barreira cultural é a dificuldade de integrar a gestão de riscos como uma responsabilidade compartilhada por toda a organização. Em muitos casos, a gestão de riscos é percebida como uma função periférica e não como um elemento central da estratégia corporativa. Mudar essa percepção e promover a conscientização sobre a importância dos riscos emergentes em todos os níveis da empresa — desde a alta direção até os colaboradores da linha de frente — é essencial para a adoção efetiva da norma. Isso requer esforços de comunicação interna, treinamentos e, sobretudo, o comprometimento dos líderes para fomentar a adoção dessa nova cultura que valoriza a vigilância constante e a resposta antecipada aos sinais de mudança.

Do ponto de vista operacional, a integração da ISO 31050 nos processos organizacionais pode ser particularmente desafiadora devido à complexidade e à necessidade de coordenação entre diferentes áreas da empresa. A norma propõe uma abordagem holística e integrada que requer a participação de equipes multidisciplinares, o que pode ser difícil de implementar em empresas com estruturas organizacionais compartimentadas, onde os departamentos funcionam de forma isolada e têm pouca comunicação entre si. Para superar esses desafios operacionais, é necessário desenvolver processos claros de colaboração e estabelecer canais eficientes de comunicação interna que fomentem a troca de informações sobre possíveis riscos emergentes. Além disso, a abordagem da ISO 31050 exige a capacitação das equipes com novas competências, desde o uso de ferramentas tecnológicas de monitoramento até a análise de dados qualitativos. A formação e o desenvolvimento de habilidades são

fundamentais, mas também podem ser desafiadores para empresas que não têm um histórico de programas estruturados de capacitação em gestão de riscos.

7.2. Superando limitações de dados e o viés de percepção

Um dos principais desafios na implementação da ISO 31050 é superar as limitações de dados e os vieses de percepção que dificultam a gestão eficaz dos riscos emergentes. Diferentemente dos riscos tradicionais, os riscos emergentes geralmente não possuem dados históricos suficientes que permitam uma análise quantitativa precisa. A falta de um histórico consolidado faz com que a avaliação desses riscos seja um desafio, já que a maioria dos métodos convencionais de gestão de riscos depende de uma base de dados robusta para a análise preditiva. Para superar essa limitação, a ISO 31050 recomenda o uso de técnicas qualitativas, como a exploração de cenários, a análise de tendências e as consultas com especialistas, que são ferramentas valiosas para abordar a incerteza e a complexidade dos riscos emergentes.

Outro aspecto importante a considerar é o viés de percepção, que pode influenciar negativamente a forma como os riscos emergentes são avaliados e priorizados. As pessoas tendem a subestimar riscos menos conhecidos que não se materializaram no passado, enquanto superestimam riscos que já ocorreram ou que parecem mais tangíveis e iminentes. Esse viés pode levar os riscos emergentes a serem negligenciados até que seja tarde demais para uma resposta eficiente. Superar esse desafio requer não apenas técnicas analíticas robustas, mas também uma mudança cultural que valorize o pensamento crítico e a tomada de decisão baseada em evidências, e não apenas em experiências passadas.

Para enfrentar as limitações de dados e o viés de percepção, é fundamental investir em tecnologias de coleta e análise de informações, como a análise preditiva e a inteligência artificial, que ajudam a identificar padrões e sinais fracos que podem ser indícios de riscos emergentes. A criação de uma base de conhecimento contínua, onde as informações de múltiplas fontes sejam atualizadas e analisadas constantemente, é fundamental para aumentar a capacidade da organização de antecipar riscos. Além disso, fomentar uma cultura de aprendizado contínuo, onde todas as lições derivadas da experiência da organização e das análises prospectivas sejam integradas nos processos de tomada de decisão, é essencial para eliminar preconceitos e aumentar a eficácia na gestão de riscos emergentes.

Programas de capacitação destinados a sensibilizar os colaboradores sobre a importância dos riscos emergentes, combinados com ferramentas analíticas avançadas, são estratégias essenciais para superar esses desafios e garantir a implementação bem-sucedida da ISO 31050.

Conclusão e Recomendações Estratégicas

08

Capítulo 8 – Conclusão e Recomendações Estratégicas

8.1. A importância de uma abordagem proativa para os riscos emergentes

Em um cenário cada vez mais volátil e imprevisível, a importância de uma abordagem proativa para a gestão de riscos emergentes não pode ser subestimada. Diferentemente dos riscos tradicionais, os riscos emergentes caracterizam-se por sua complexidade, incerteza e rápida evolução. Esses riscos podem surgir repentinamente e ter impactos sistêmicos em toda a organização, afetando as operações, as finanças, a reputação e até a viabilidade do negócio. A abordagem reativa, na qual as organizações respondem apenas após a materialização dos riscos, é ineficaz e perigosa no contexto atual, onde as mudanças são rápidas e os impactos podem ser devastadores.

A ISO 31050 promove a adoção de uma postura proativa, na qual a organização não apenas reage aos riscos, mas se antecipa a eles. Isso implica a identificação antecipada de sinais de mudança, a análise contínua do ambiente externo e o desenvolvimento de estratégias adaptativas. A abordagem proativa ajuda a transformar os riscos emergentes em oportunidades de crescimento e inovação, permitindo que as organizações não apenas mitiguem ameaças, mas também explorem oportunidades e novas possibilidades de diferenciação no mercado. Quando os riscos emergentes são gerenciados de maneira antecipada, a empresa está em uma posição mais favorável para minimizar os impactos negativos, proteger seus ativos e, ao mesmo tempo, fortalecer a confiança de seus *stakeholders*.

8.2. Recomendações para a aplicação prática da ISO 31050 no setor de segurança

Para aplicar a ISO 31050 de maneira eficaz no setor de segurança, é essencial seguir algumas recomendações estratégicas que assegurem uma implementação robusta e integrada. Em primeiro lugar, é necessário que a alta direção esteja totalmente comprometida com a adoção da norma. Sem o apoio da liderança, é improvável que a cultura organizacional mude para valorizar a identificação e a antecipação de riscos emergentes. Portanto, o primeiro passo deve ser o comprometimento dos líderes, demonstrando que a gestão de riscos emergentes é uma prioridade estratégica.

Outro ponto fundamental é a capacitação dos colaboradores e o desenvolvimento de competências específicas para lidar com riscos emergentes. Isso inclui formação sobre os princípios da ISO 31050, além do uso de técnicas qualitativas, como a análise de cenários e a identificação de sinais fracos, e o uso de tecnologias avançadas, como a inteligência artificial e a análise preditiva. Criar uma base de conhecimento dentro da organização e capacitar os colaboradores para monitorar e analisar riscos emergentes são passos essenciais para garantir que todos os níveis hierárquicos estejam alinhados com a abordagem proposta pela ISO 31050.

A integração da gestão de riscos emergentes nos processos de negócio existentes é outra recomendação crítica. Isso requer incorporar a análise de riscos emergentes em todas as fases do planejamento estratégico e da tomada de decisão, garantindo que a gestão de riscos não seja um processo isolado, mas uma parte integrante das operações e do planejamento corporativo. Para facilitar essa integração, é importante desenvolver uma comunicação eficaz entre os departamentos e criar estruturas que promovam a colaboração entre áreas, de modo que todos estejam envolvidos na identificação e resposta a riscos emergentes.

Finalmente, recomenda-se o uso de um ciclo contínuo de inteligência de riscos, conforme descrito na ISO 31050. Este ciclo implica a coleta contínua de informações, a análise dessas informações para identificar riscos potenciais e a disseminação do conhecimento obtido para os tomadores de decisão. Implementar um ciclo de inteligência robusto ajudará a garantir que a organização esteja sempre preparada para responder a riscos emergentes e ajustar suas estratégias conforme necessário, aumentando sua resiliência diante de mudanças inesperadas.

8.3. Fortalecendo a segurança corporativa com ISO 31050

A implementação da ISO 31050 oferece uma oportunidade única para fortalecer a segurança corporativa, convertendo a gestão de riscos emergentes em um elemento central da estratégia organizacional. A norma fornece uma estrutura abrangente e integrada que permite às empresas antecipar-se aos riscos, ser proativas em sua mitigação e utilizar esses riscos como oportunidades para o crescimento e a inovação. Ao integrar os princípios da ISO 31050, as organizações conseguem transformar uma abordagem tradicionalmente reativa em um processo dinâmico e proativo, que contribui para a construção de uma cultura de resiliência e adaptabilidade.

No setor de segurança, a ISO 31050 destaca-se por seu foco na identificação e gestão de riscos complexos que não possuem um histórico bem definido, como as ameaças cibernéticas, as mudanças climáticas e os desafios regulatórios. Adotar esta norma significa não apenas estar preparado para enfrentar riscos emergentes, mas também estar em posição de aproveitar as oportunidades que estes trazem, como a inovação em processos, a melhoria dos serviços oferecidos e o fortalecimento da confiança dos *stakeholders*. A ISO 31050 ajuda a promover uma visão holística, onde a segurança é considerada um facilitador do sucesso estratégico, contribuindo diretamente para a criação e proteção de valor dentro da organização.

Portanto, ao fortalecer suas práticas de gestão de riscos emergentes com a ISO 31050, as organizações estarão mais bem preparadas para enfrentar as incertezas do ambiente empresarial atual, garantir a continuidade de suas operações e alcançar um desempenho superior a longo prazo. A adoção desta norma representa um passo importante para converter a gestão de riscos em um verdadeiro diferencial competitivo, assegurando não apenas a proteção contra ameaças, mas também a capacidade de evoluir e prosperar em um mundo em constante mudança.

8.4. Passos para implementar a ISO 31050 em complemento ao processo atual de gestão de riscos de segurança

A implementação da ISO 31050 no setor de segurança pode ser integrada ao processo de *Enterprise Security Risk Management* (ESRM) da ASIS para criar um sistema robusto e dinâmico de gestão de riscos emergentes.

Aqui são apresentados 10 passos para realizar essa implementação de maneira eficaz:

1) **Comprometimento da liderança e definição de objetivos estratégicos:** O primeiro passo é garantir o comprometimento da alta direção. A liderança deve

reconhecer a importância dos riscos emergentes e definir objetivos estratégicos que alinhem a gestão de riscos emergentes com as metas corporativas. Isso inclui comunicar claramente como a ISO 31050 complementa o processo atual de ESRM e como ambas as estruturas podem ajudar a alcançar os objetivos da organização.

2) **Análise do sistema atual de gestão de riscos:** Antes de começar a implementação, é essencial analisar o sistema atual de gestão de riscos de segurança para identificar lacunas e oportunidades. Isso implica revisar como o ESRM é aplicado atualmente e determinar quais elementos da ISO 31050 podem ser adicionados para melhorar a abordagem dos riscos emergentes, especialmente aqueles que transcendem as ameaças e vulnerabilidades físicas e operacionais.

3) **Desenvolvimento de competências e capacitação**: Capacitar a equipe é fundamental para implementar a ISO 31050. Isso inclui formar os colaboradores sobre as diferenças entre a abordagem tradicional e a abordagem para riscos emergentes, conforme descrito na ISO 31050. Os treinamentos específicos devem incluir a identificação de sinais fracos, técnicas qualitativas como a análise de cenários e o uso de tecnologias como a inteligência artificial para a previsão de riscos.

4) **Criação de um ciclo de inteligência de risco:** Estabelecer um ciclo de inteligência de risco robusto é essencial. Este ciclo, descrito pela ISO 31050, deve ser implementado para identificar, coletar, analisar e disseminar informações relevantes sobre riscos emergentes. No contexto do ESRM, isso pode significar um aumento na frequência das avaliações de riscos, o monitoramento de tendências e uma maior colaboração entre as áreas de TI, segurança e gestão de riscos corporativos.

5) **Integração com o ESRM alinhamento com a gestão de ativos**: A ISO 31050 deve ser integrada ao ESRM para garantir uma abordagem abrangente. O ESRM está focado na proteção dos ativos mais importantes da organização, e a ISO 31050 pode complementar essa abordagem ajudando a antecipar riscos emergentes que possam impactar esses ativos. Essa integração assegura que a avaliação de riscos emergentes seja realizada de forma coordenada, considerando tanto ameaças/vulnerabilidades conhecidas quanto riscos emergentes.

6) **Identificação e análise de sinais fracos**: Adotar práticas de identificação de sinais fracos é um passo fundamental. Utilizando ferramentas de análise de dados e monitoramento, a organização deve começar a detectar padrões ou

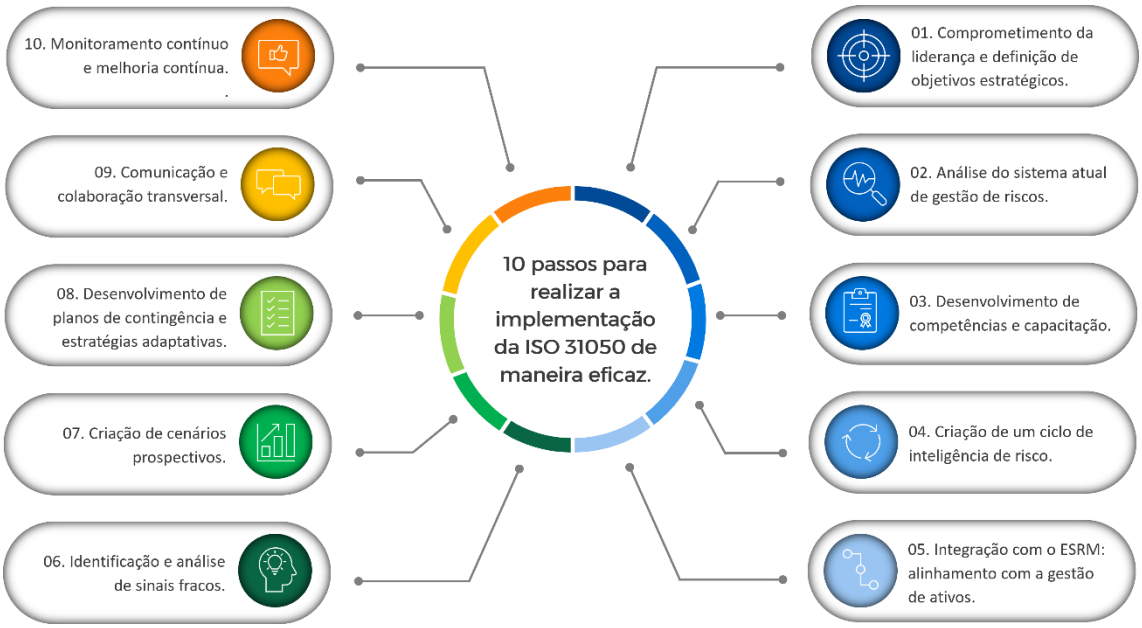
mudanças no ambiente interno e externo que possam indicar a possibilidade de um risco emergente. No contexto do ESRM, isso pode incluir monitorar a segurança cibernética de maneira mais ampla, incluindo vulnerabilidades que possam ser exploradas durante crises climáticas.

7) **Criação de cenários prospectivos**: A criação de cenários prospectivos permite que a organização visualize possíveis futuros e se prepare para eles. Esses cenários devem considerar uma variedade de fatores, como impactos regulatórios, mudanças climáticas e possíveis ataques cibernéticos. No ESRM, isso pode ser adaptado para analisar como diferentes tipos de ameaças e vulnerabilidades, combinadas, podem afetar a segurança dos ativos críticos e qual seria a resposta mais apropriada.

8) **Desenvolvimento de planos de contingência e estratégias adaptativas:** Com base nos cenários prospectivos e nos sinais fracos identificados, a organização deve desenvolver planos de contingência sólidos. Esses planos devem prever ações a serem tomadas em caso de crises emergentes, como ataques cibernéticos durante desastres naturais, conforme discutido em exemplos anteriores. A ISO 31050 orienta a adaptação contínua, assegurando que os planos sejam flexíveis e possam ser ajustados conforme o cenário evolua.

9) **Comunicação e colaboração transversal:** A comunicação eficaz entre as áreas da organização é essencial para garantir que a gestão de riscos seja um esforço coletivo. Tanto o ESRM quanto a ISO 31050 enfatizam a importância de envolver diferentes *stakeholders*, e isso deve se refletir na prática. As equipes de segurança física, TI, *compliance*, operações e gestão de riscos devem trabalhar juntas para identificar, avaliar e responder aos riscos de maneira coordenada.

10) **Monitoramento e melhoria contínua**: Finalmente, a implementação da ISO 31050 deve incluir o monitoramento contínuo dos riscos emergentes e uma avaliação regular dos processos adotados. Aprender com eventos passados e ajustar as estratégias é fundamental para garantir a eficácia da gestão de riscos. Esta etapa deve ser um ciclo constante de melhoria, no qual se incorporem as lições aprendidas e se aprimorem continuamente as práticas de gestão de riscos para se adaptar às mudanças do ambiente empresarial.


10 passos para realizar a implementação da ISO 31050 de maneira eficaz.
01. Comprometimento da liderança e definição de objetivos estratégicos.
02. Análise do sistema atual de gestão de riscos.
03. Desenvolvimento de competências e capacitação.
04. Criação de um ciclo de inteligência de risco.
05. Integração com o ESRM: alinhamento com a gestão de ativos.
06. Identificação e análise de sinais fracos.
07. Criação de cenários prospectivos.
08. Desenvolvimento de planos de contingência e estratégias adaptativas.
09. Comunicação e colaboração transversal.
10. Monitoramento contínuo e melhoria contínua.

ANEXO I – Análise comparativa entre ESRM-ASIS e ISO 31000

Resultado da análise comparativa entre as duas normas (ISO 31000 e ESRM da ASIS), encontramos os seguintes resultados:

Semelhanças:

1. **Gestão de Riscos como Processo Sistemático:** Ambas as normas consideram a gestão de riscos como um processo sistemático, estruturado e iterativo, que envolve a identificação, análise, avaliação e tratamento de riscos.
2. **Integração e Alinhamento com os Objetivos Organizacionais**: As duas normas enfatizam a importância de integrar a gestão de riscos nos processos estratégicos da organização, alinhando os esforços de mitigação de riscos com os objetivos e metas organizacionais.
3. **Participação das Partes Interessadas**: As normas destacam a importância da comunicação e consulta com as partes interessadas no processo de avaliação e mitigação de riscos, garantindo que a informação seja considerada na tomada de decisão.

Diferenças:

1. **Abordagem Específica vs. Abordagem Geral**:
    - **ISO 31000**: Apresenta uma abordagem ampla para a gestão de qualquer tipo de risco, sendo aplicável a todo tipo de organização, independentemente do setor.
    - **ESRM ASIS**: Foca especificamente nos riscos relacionados à segurança, incluindo riscos físicos, lógicos e não físicos, e está orientada a ativos específicos que podem ser impactados por ameaças e vulnerabilidades.
2. **Orientação para a Segurança**:
    - A norma **ESRM ASIS** enfatiza a segurança dos ativos tangíveis e intangíveis, além de oferecer diretrizes detalhadas sobre a identificação de ameaças e a análise de vulnerabilidades que afetam a segurança.
    - A **ISO 31000** adota uma visão mais ampla do risco, abrangendo todo tipo de incertezas, sem focar exclusivamente na segurança.

Complementariedade:

- A **ISO 31000** fornece uma base geral e sólida para a gestão de riscos, enquanto a ESRM ASIS detalha como aplicar esses conceitos especificamente no contexto da segurança. Uma pode complementar a outra da seguinte maneira:

    - A **ISO 31000** estabelece o processo fundamental para a gestão de riscos corporativos.
    - A **ESRM ASIS** complementa este processo fornecendo diretrizes específicas para os riscos de segurança, ajudando a identificar e mitigar ameaças específicas que possam comprometer os ativos críticos da organização.
- Juntas, essas normas ajudam a empresa a gerenciar não apenas os riscos gerais que afetam suas operações, mas também os riscos específicos relacionados à segurança de seus ativos.

Pontos Antagônicos:

- Não existe um ponto explicitamente antagônico entre as normas, mas o foco difere substancialmente. A **ISO 31000** é mais ampla e aplica-se a uma variedade de riscos, enquanto a **ESRM ASIS** concentra-se estritamente na segurança. Essa diferença de foco pode levar a diferentes abordagens na priorização de riscos, já que a **ESRM** prioriza a segurança física e operacional, o que pode não ser o foco principal em todos os contextos de gestão de riscos definidos pela **ISO 31000**.

Em resumo, ambas as normas têm abordagens que se alinham em muitos aspectos, sendo a **ISO 31000** adequada para estabelecer uma visão ampla da gestão de riscos, enquanto a **ESRM ASIS** oferece uma abordagem mais prática e detalhada sobre a gestão de riscos de segurança. São complementares e podem ser utilizadas conjuntamente para uma gestão de riscos mais holística e integrada.

ANEXO II – Referências bibliográficas

- ISO 31000:2018. Gestão de riscos – Diretrizes. Organização Internacional de Normalização (ISO), 2018.
  Disponível em https://www.iso.org/standard/65694.html;

- ISO/TS 31050:2023 (en) Risk management – Guidelines for managing an emerging risk to enhance resilience.
  Disponível em https://www.iso.org/standard/54224.html;

- ASIS STANDARD – Security Risk Assessment – ASIS SRA, 2024.
  Disponível em https://store.asisonline.org/security-risk-assessment-standard-asis-sra-2024-softcover.html.

Sobre a Plataforma t-Risk

A **Plataforma t-Risk** é uma solução SaaS disponível desde 2015, projetada para transformar a **gestão de riscos nas organizações**. Ela combina inovação tecnológica com as melhores práticas normativas globais, especialmente as diretrizes das **normas ISO 31000, ISO 31050 e 31010**. Totalmente alinhada aos padrões internacionais, a t-Risk oferece uma **abordagem analítica e prática**, auxiliando as empresas em todas as etapas da gestão de riscos corporativos: **identificação, análise, avaliação, priorização e tratamento**. Disponível em português, espanhol e inglês, a plataforma **aumenta em até 80% a produtividade do processo de gestão de riscos**, entregando eficiência e precisão.

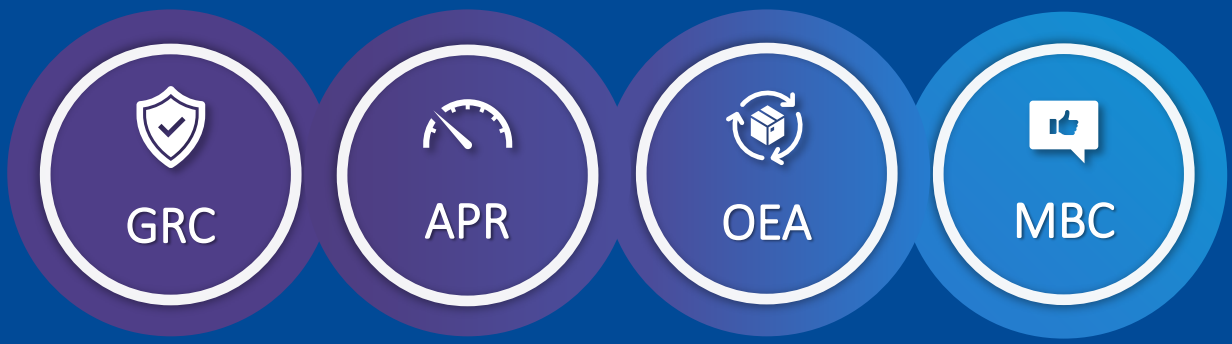
Com funcionalidades avançadas, a t-Risk integra **inteligência artificial** e oferece módulos robustos, como **GRC** (Gestão de Riscos Corporativo), **APR** (Análise Preliminar de Riscos), **MBC** (Módulo de *Background Check*), **MAM** (Módulo de Avaliação de Maturidade em Gestão de Riscos) e **OEA** (Operador Econômico Autorizado), AVSEC (Gestão de Riscos na Aviação Civil), além de um **Painel de Indicadores** (BI) e um **APP Mobile**. O **módulo 5W2H** permite um acompanhamento detalhado de projetos, tarefas e controles, com e-mails automáticos, garantindo que os riscos permaneçam dentro do apetite de risco da organização.

Além de **fortalecer o *compliance* e otimizar processos**, a t-Risk capacita seus clientes a transformarem desafios em oportunidades, oferecendo **insights valiosos para decisões estratégicas**. Seja para fortalecer a resiliência organizacional ou impulsionar o crescimento sustentável, a t-Risk é **uma aliada indispensável para enfrentar um cenário de riscos** cada vez mais dinâmico e complexo.

Descubra como a t-Risk pode revolucionar a gestão de riscos na sua organização. Explore o poder de nossas soluções e **fortaleça sua estratégia de gestão de riscos com uma ferramenta que vai além da tecnologia**: uma verdadeira parceira na sua jornada de transformação.

Softwares t-Risk

Conheça todos os módulos e ferramentas da Plataforma Total Risk.



Módulo Gestão de Riscos Corporativos

Gestão de riscos integrados e estratégicos.

Módulo Análise Preliminar de Riscos

Análise prévia e operacional dos riscos.

Módulo Operador Econômico Autorizado

Gerenciamento dos riscos logísticos - OEA.

Módulo Background Check

Due Diligence Digital para gestão de riscos de terceiros.

Módulo Avaliação de Maturidade

Análise do nível de maturidade organizacional em gestão de riscos.

Módulo AVSEC Aeroportos

Gestão de riscos de segurança da aviação civil (Security).

Aplicativo de Avaliação de Riscos

APP mobile completo para identificação de riscos.

IA Vision Pro

Inteligência Artificial criada pela t-Risk para potencializar a gestão de riscos corporativos.


TURBINE SUAS ANÁLISES DE RISCOS
COM A INTELIGÊNCIA ARTIFICIAL DA
T-RISK!
Acesse agora mesmo e
confira mais essa novidade.
CLIQUE AQUI

t-Risk

Método de Avaliação de Riscos

WSC