Modelo das três linhas integrado à ISO 31000

Uma abordagem em governança e gestão dos riscos corporativos

SUMÁRIO

01 Modelo das três linhas

Não é mágica, nem moda. Trata-se apenas de fazer bem-feito. Empresas de qualquer porte precisam de uma gestão dos riscos corporativos (GRC) adequada às suas características. Uma estrutura de GRC plenamente entrosada com a governança corporativa dá à empresa uma proteção orgânica que perpassa todos os níveis da atividade, de maneira robusta, flexível e eficiente.

Dois guias para levar e manter a organização em nível ótimo de gestão de riscos são a norma da ABNT ISO 31000 e o modelo das três linhas. Cada um desses guias se encaixa nas lacunas do outro como peças de Lego. Enquanto a ISO 31000 detalha o processo de gerenciamento de riscos, o modelo das três linhas se detém na estrutura, esmiuçando como as pessoas devem se organizar e interagir para que a GRC flua com mais eficiência.

O MODELO DAS TRÊS LINHAS

Antes chamado de modelo das três linhas de defesa, o modelo das três linhas é parte do sistema de governança corporativa, de acordo com o IIA - The Institute of Internal Auditors. O modelo oferece um processo contínuo de gerenciamento da exposição ao risco, levando em conta o nível de risco aceito para o negócio. Nessa estrutura em que todos têm alguma responsabilidade, atuam como elementos centrais: gestores de riscos operacionais, diretores de conformidade, especialistas em controle interno, auditores internos e externos, especialistas na investigação de fraudes, além de outros. O modelo das três linhas envolve pessoas e setores diversos, formando uma estrutura clara, com transparência na comunicação e na distribuição de funções e responsabilidades.

Entre as partes envolvidas na estrutura global de gestão de risco, a governança corporativa é a instância que converte os princípios básicos da organização em recomendações objetivas, visando preservar e otimizar o valor econômico da organização em longo prazo. O Código das Melhores Práticas de Governança Corporativa define governança corporativa como um sistema “pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas”. A responsabilidade final pela GRC cabe ao conselho de administração, que reporta aos acionistas e reguladores.

Subordinadas ao órgão de governança, estão as três linhas, que são: (1) controle gerencial e medidas de controle interno; (2) funções de supervisão ou especialização no gerenciamento de riscos; e (3) auditoria interna.

Com esses grupos genéricos, cada empresa se organiza de acordo com suas circunstâncias, podendo alterar a estrutura sempre que necessário. Funções, equipes e até mesmo indivíduos podem ter responsabilidades que incluam papéis de primeira e de segunda linha. Pode ser criada uma direção ou supervisão específica para a segunda linha a fim de garantir certo grau de independência em relação à primeira linha — e até mesmo aos níveis mais altos da gestão. O modelo permite quantas linhas de reporte forem necessárias. Nas instituições financeiras, a independência entre as linhas costuma ser garantida por requisitos estatutários. Mesmo nessas situações, entretanto, os gerentes com papéis de primeira linha permanecem respondendo pelo gerenciamento dos riscos.

Uma referência forte nesse modelo é o livro de Karl Weick e Kathleen Sutcliffe Managing the Unexpected (Gerenciando o inesperado), publicado em 2001. Observando instituições de alta confiabilidade, como operações de transporte aéreo, equipes de emergência em hospitais e corpo de bombeiros, os autores constataram que, por absoluta necessidade, eles desenvolveram meios de agir e formas de aprender que lhes permitem administrar o inesperado melhor do que outras organizações. Por isso, representam um bom modelo a ser seguido pelas empresas em geral para gerenciar seus riscos.

Figura 1 – Modelo das três linhas do IIA integrado à ISO 31000

O modelo é regido por seis princípios: governança; papéis do órgão de governança; gestão e os papéis da primeira e segunda linhas; papéis da terceira linha; independência da terceira linha; criação e proteção de valor. Mesmo com as particularidades de cada organização, alguns papéis de alto nível são mais vocacionados para amplificar os princípios do modelo das três linhas.

São estes os principais papéis atribuídos a cada instância:

O órgão de governança - atuação acima das três linhas

- Aceitar, perante os stakeholders, a prestação de contas feita pela diretoria executiva.
- Estimular nos stakeholders a comunicação transparente e o monitoramento dos interesses do grupo.
- Sustentar a cultura de responsabilidade e o comportamento ético.
- Estabelecer estruturas e processos de governança, incluindo comitês, se necessário.
- Delegar responsabilidades e apoiar a gestão para atingir os objetivos da organização.
- Determinar o apetite ao risco e supervisionar a gestão de riscos (incluindo o controle interno).
- Supervisionar a conformidade com as expectativas legais, regulatórias e éticas.
- Estabelecer e supervisionar auditoria interna independente, objetiva e competente.

Gestão - papéis da primeira linha (proprietários dos processos)

- Liderar ações e aplicar recursos para atingir os objetivos da organização.
- No diálogo contínuo com o órgão de govervança, reportar os resultados planejados e os alcançados, além dos riscos associados à operação.
- Estabelecer e manter estruturas e processos para gerenciar operações e riscos (incluindo controle interno).
- Garantir a conformidade com as expectativas legais, regulatórias e éticas.

Gestão - papéis da segunda linha (comitê integrado de gestão de riscos)

- Fornecer expertise complementar, apoio, monitoramento e questionamento quanto à gestão de riscos, incluindo desenvolvimento, implantação e melhoria contínua das práticas de gerenciamento de riscos (incluindo controle interno) nos níveis de processo, sistemas e estrutura.
- Definir os objetivos de gerenciamento de riscos -- conformidade com leis, regulamentos e comportamento ético; controle interno; segurança da informação e tecnologia; sustentabilidade; e avaliação da qualidade.
- Fornecer análises e reportar sobre a adequação e eficácia do gerenciamento de riscos (incluindo controle interno).

Auditoria interna – papéis da terceira linha

- Manter prestação de contas primária perante o órgão de governança e ter independência em relação à gestão.
- Comunicar avaliação e prestar assessoria, de modo independente e objetivo, à gestão e ao órgão de governança sobre a adequação e eficácia da governança e da GRC (incluindo controle interno), para apoiar a realização dos objetivos organizacionais e promover melhoria contínua.
- Reportar ao órgão de governança prejuízos à independência e à objetividade e implantar salvaguardas conforme a necessidade.

Resumindo, o órgão de governança determina a direção da organização, definindo a visão, a missão, os valores e o apetite organizacional a riscos. A primeira linha, de gestão, é responsável por identificar, analisar, avaliar, tratar e gerenciar os riscos. Ela projeta, opera e melhora os processos, procedimentos, políticas, garantias de conformidade etc. E também coordena estratégias de mitigação dos riscos. A segunda linha é o comitê dedicado a estabelecer as métricas, modelos, processos, níveis aceitáveis de riscos etc. Os papéis de segunda linha nunca são totalmente independentes da gestão, ao contrário dos papéis de terceira linha, que se caracterizam pela independência.

02 A norma ISO 31000

Os princípios e a estrutura descritos pela norma ISO 31000, que o modelo das três linhas complementa de maneira notável, prescrevem o gerenciamento de riscos como parte integrante "do propósito organizacional, governança, liderança e comprometimento, estratégia, objetivos e operações" (p.6).

Os princípios oferecem excelente base para o estabelecimento tanto da estrutura quanto do processo para a organização gerenciar a incerteza, elemento presente em toda ação humana. O propósito da gestão de riscos, segundo a ISO 31000, é criar e proteger valor, uma vez que "melhora o desempenho, encoraja a inovação e apoia o alcance dos objetivos" (p.2).

A norma reitera que, para ser eficaz, a gestão de riscos precisa apresentar estes oito requisitos (Figura 2): ser integrada, ou seja, participar de todas as atividades da organização; ser estruturada e abrangente, para ajudar a organização a obter resultados consistentes e passíveis de comparação; ser personalizada na estrutura e no processo, atendendo assim aos contextos externo e interno da organização; ser inclusiva, ou seja, envolver as partes interessadas para que seus conhecimentos, pontos de vista e percepções sejam levados em conta; ser dinâmica, pois, como os riscos sempre emergem, mudam ou desaparecem, é preciso antecipar, detectar, reconhecer e responder tempestivamente às mudanças; usar como base a melhor informação disponível e, para tanto, utilizar informações históricas e atuais, bem como expectativas futuras, e entregar informação "oportuna, clara e disponível para as partes interessadas pertinentes"; zelar pelos fatores humanos e culturais, os quais "influenciam significativamente todos os aspectos da gestão de riscos em cada nível e estágio"; promover melhoria contínua, por meio das experiências e do aprendizado.

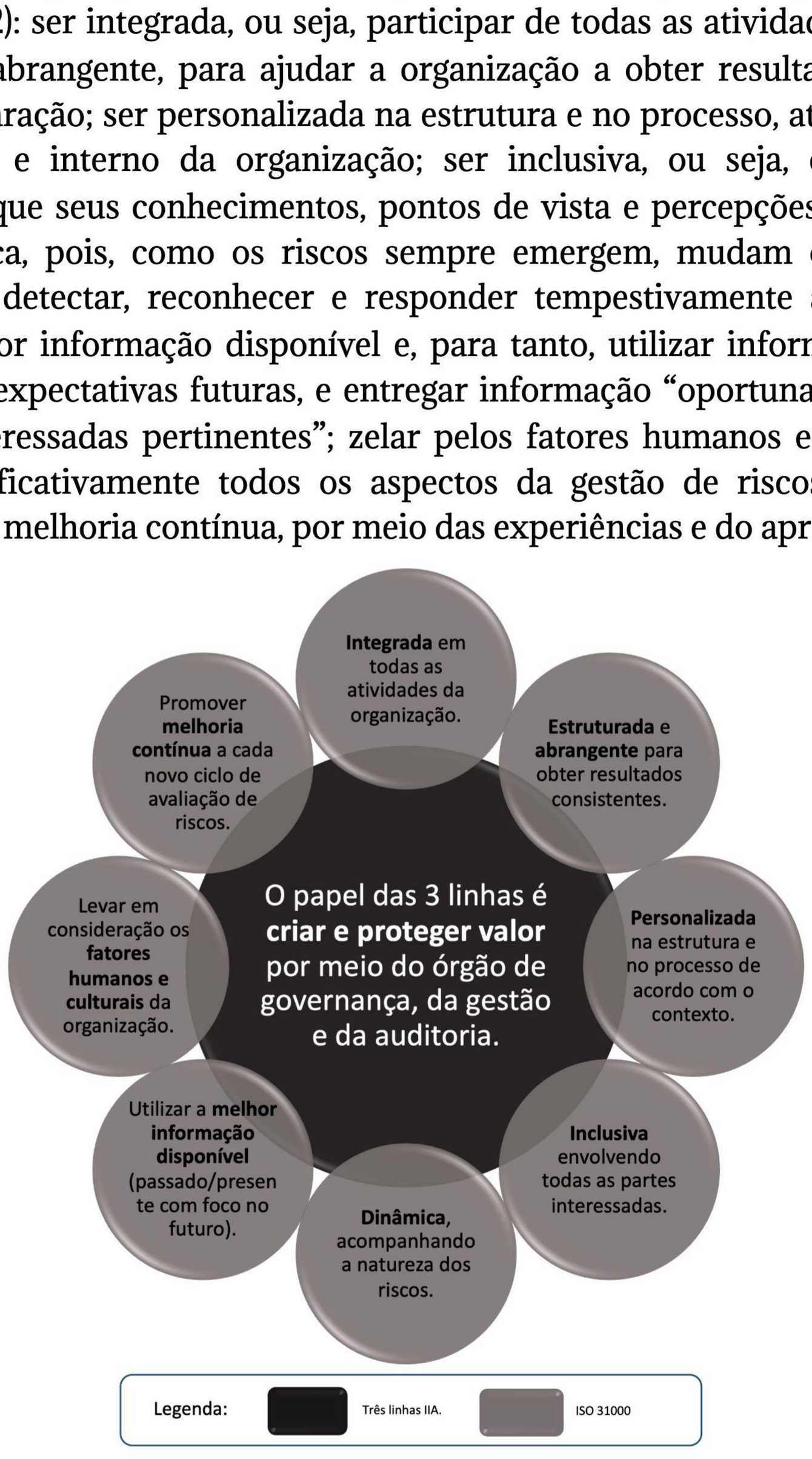


Figura 2: Princípios da ISO 31000 integrados às 3 linhas

Quanto à estrutura, seu propósito “é apoiar a organização na integração da gestão de riscos em atividades significativas e funções” (p.4). A gestão de riscos será mais eficaz ou menos eficaz conforme o grau de integração com a governança e todas as demais atividades, incluindo a tomada de decisões. O bom gerenciamento de riscos depende do comprometimento e da liderança da alta direção e dos órgãos de supervisão, uma vez que estão sob sua responsabilidade: personalizar os componentes da estrutura; estabelecer a abordagem, curso ou plano de ação; assegurar os recursos necessários; atribuir autoridades, responsabilidades e responsabilização.

Do órgão de supervisão espera-se: assegurar que os riscos sejam considerados de maneira adequada aos objetivos da organização, compreender a exposição da organização a riscos, sustentar a implementação e a eficácia de sistemas de gerenciamento de riscos e garantir comunicação apropriada das informações.

A concepção da estrutura para o gerenciamento dos riscos deve levar em conta o contexto externo à organização (fatores socioculturais, jurídicos, políticos, regulatórios, ambientais, tendências etc.) e o contexto interno (visão, missão valores, estrutura, responsabilidades, estratégia, objetivos, políticas, cultura, recursos, conhecimentos etc.).

A tarefa constante de articular o comprometimento de todos com a gestão de riscos exige enfatizar o propósito da organização e suas políticas, enfrentar eventuais objetivos conflitantes, além de fazer medições e relatá-las nos indicadores de desempenho, buscando sempre análise crítica e melhoria.

A ISO 31000 propõe ainda a adequada alocação dos recursos humanos, processos, métodos e ferramentas, em constante compartilhamento das informações e sondagem quanto à adequação da estrutura e dos papéis atribuídos.

Na implementação de estruturas, a norma recomenda construir planos que incluam prazos e recursos, determinar as alçadas para tomada de decisão e assegurar compreensão e aplicação adequada do que foi disposto para o gerenciamento de riscos.

03 O modelo das três linhas e a norma ISO 31000 - benefícios para o negócio

O primeiro parágrafo da norma indica que ela “é para ser usada por pessoas que criam e protegem valor nas organizações, gerenciando riscos, tomando decisões, estabelecendo e alcançando objetivos e melhorando o desempenho”. Ou seja, os profissionais envolvidos nas três linhas estão dentro desse contexto.

A ISO 31000 recomenda que a estrutura da gestão de riscos sustente a integração da gestão de riscos na governança e nas diversas atividades da organização, esclarecendo que a responsabilidade por gerenciar riscos é de todos. Por sua vez, o IIA afirma, a respeito do relacionamento entre o órgão de governança e as três linhas, que são distintas as responsabilidades de cada uma das quatro instâncias, mas mesmo assim suas atividades precisam estar engajadas nos objetivos da organização. Diz também, na sua página 8, que “a base para uma coerência bem-sucedida é a coordenação, colaboração e comunicação regulares e eficazes”.

A auditoria externa é mais um fator a garantir compreensão sobre a efetividade do processo de gestão dos riscos, podendo até ser considerada como uma quarta linha de defesa. Esse tipo de auditoria pode ser realizado por consultorias independentes.

Coordenação e coerência são essenciais para a primeira linha não sofrer fadiga causada por ações duplicadas da segunda e da terceira linhas, resultando em menos tempo para a primeira linha se concentrar no negócio em questão. É importante que a terceira linha concentre seus esforços em transferir a propriedade de certos elementos da gestão de risco para a primeira e segunda linhas, por meio de educação e da conscientização. Um exemplo: ao fomentar a digitalização dos processos anteriormente realizados manualmente ou a utilização de métodos inovadores, a terceira linha é a que tem mais recursos e acesso a evidências, enquanto a primeira linha, por sua vez, pode dedicar menos tempo ao gerenciamento de riscos e focar nos controles, o que representa ganho de qualidade e eficiência no processo de gestão de riscos.

O modelo não é tudo na GRC e tampouco é um plano ou projeto organizacional. Seu grande mérito é favorecer a criação e a manutenção de uma estrutura ao mesmo tempo flexível e robusta. Assim, ele torna fluente um processo de gestão de riscos aderente à norma 31000. Os dois guias se complementam na disseminação de uma cultura de proteção em todas as atividades da empresa para que ela evolua e amadureça cada vez mais. Juntos, dão as bases para se enfrentar o grande desafio de construir uma cultura de risco eficiente e ensinar a todos -- absolutamente todos na empresa -- habilidades de gerenciamento de risco para que, caso ele se concretize (e é provável que ocorra um dia), todos saibam o que fazer!

04 Fontes de referência

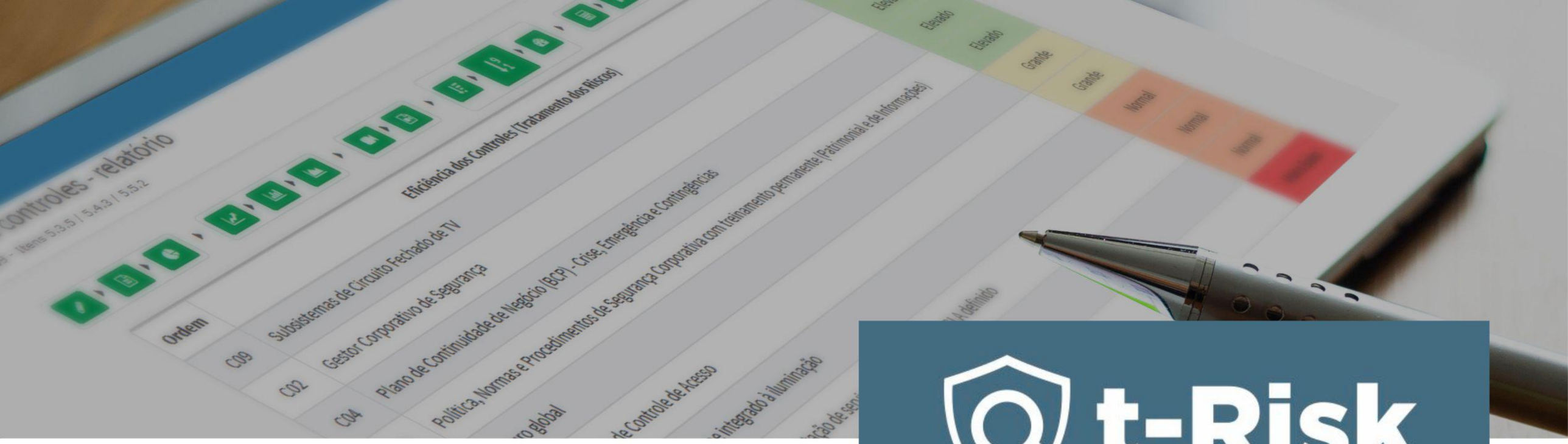
ABNT NBR ISO 31000. Gestão e Riscos – Diretrizes. Segunda Ed., 28.03.2018 <www.abnt.org.br>.

HOLLAND, T.; FLOAM, S. Three Lines of Defense: A New Principles-Based Approach. Guide House. Disponível em <https://guidehouse.com/insights/financial-services/2021/public-sector/garp-three-lines-of-defense>

IBGC (Instituto Brasileiro de Governança Corporativa). Código das Melhores Práticas de Governança Corporativa. 5. ed., São Paulo, IBGC, 2015. Disponível em: <https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=21138>. Acesso em: dez. 2021.

IIA – The Institute of Internal Auditors (global). Modelo das Três Linhas do IIA 2020 – Uma atualização das Três Linhas de Defesa. Tradução do IIA Brasil. Disponível em <https://iiabrasil.org.br/noticia/novo-modelo-das-tres-linhas-do-iia-2020>.

WEICK, K. E.; SUTCLIFFE, K. M. Managing the unexpected. San Francisco: Jossey-Bass, 2001.



t-Risk
Método de Avaliação de Riscos

Sobre a Plataforma t-Risk

O Software t-Risk (SaaS) está disponível desde 2015 para apoiar organizações no gerenciamento de seus riscos. Ferramenta analítica que auxilia na identificação, análise e avaliação de riscos, além de apoiar nos processos de priorização e tratamento dos riscos.

A base de dados é criptografada e confidencial, somente o usuário tem acesso às informações de seu projeto. Além disso, ela é mantida em servidor de alta performance com backup permanente dos dados.

Está em conformidade com o processo de gestão de riscos definido na ISO 31.000 e 31.010. Disponível em português, inglês e espanhol, aumenta em até 80% a produtividade, o que representa mais rapidez e menor custo para entregar um quadro claro das condições de riscos em que a organização opera.

Após definição dos controles que serão implantados, melhorados ou mantidos, para manter os riscos dentro do apetite ao risco da organização, ainda será possível monitorar todos os projetos, tarefas e controles através do módulo 5W2H para gestão de projetos com envio de e-mails automáticos aos envolvidos no projeto.

Saiba mais, conheça todos os detalhes em nosso site.

t-Risk

Método de Avaliação de Riscos

www.totalrisk.com.br