eBook

Centralize o Gerenciamento de Riscos e melhore a Resiliência da Organização

A gestão de riscos corporativos (GRC) vem ocorrendo, na maioria dos casos, na forma centralizada: a equipe de GRC comanda diretamente as ações referentes aos riscos, assumindo as funções de identificar, analisar, avaliar e mitigar riscos em toda a organização. Esse formato, que permite tomada rápida de decisão, coordenação mais simples e melhor alocação de recursos, tem as graves desvantagens de negligenciar nuances das operações diárias e burocratizar o processo de mitigação dos riscos. A equipe centralizadora tem carga de responsabilidade bem maior do que as de seus clientes – as pessoas dos demais departamentos. Dessa forma, eventuais novas ameaças ou vulnerabilidades podem não ser percebidas, ou receber avaliação equivocada. Esse tipo de negligência tem potencial para provocar grandes perdas à operação e causar desvios em relação aos objetivos da organização como um todo.

Outra opção seria a GRC descentralizada, que promove maior conhecimento dos riscos específicos de cada departamento, mais flexibilidade e agilidade na tomada de decisão.

A desvantagem ou, olhando de forma positiva, a grande vantagem, entretanto, é que demandaria uma cultura de risco disseminada por toda a empresa e forte o suficiente para garantir eficiência e eficácia de todas as gerências da corporação no que se refere aos riscos.

Nossa prática tem demonstrado que não é possível gerenciar de maneira totalmente centralizada, nem totalmente descentralizada. A sabedoria está em integrar e centralizar, ou seja, gerenciar de forma centralizada e ao mesmo tempo contemplar todas as diferentes atividades da organização. Tomemos o corpo humano como analogia: quando temos sede, o cérebro toma a decisão de beber água. O corpo usa os órgãos especializados – pés para caminhar, mãos para pegar e encher o copo, olhos, boca, e etc. A inteligência do corpo nos manda pensar de maneira centralizada e agir descentralizadamente. De modo semelhante, em uma GRC integrada, as áreas especialistas da empresa atuam para implantar e manter os controles dos riscos -- gerando soluções construídas diretamente nas áreas específicas, muitas vezes operacionais --, enquanto o comitê central cuida da manutenção do processo, da estrutura, das métricas e dos padrões, distribuindo o conhecimento. Assim, a resiliência organizacional fica assegurada por uma visão única, compartilhada pelas diversas equipes em modelo descentralizado.

Aí então a empresa pode examinar suas unidades de negócio e centralizar estratégias de risco e resiliência para garantir que não haja falhas nas defesas corporativas. Para orientação, conta com estândares como a norma da ISO 31000, sempre uma garantia de qualidade no gerenciamento, e o *modelo das três linhas*, recomentado pelo IIA – The Institute of Internal Auditors [1], já apresentado em artigo anterior.

O modelo prescreve uma estrutura clara de GRC como parte da governança corporativa, funcionando de modo contínuo no gerenciamento dos riscos em todos os níveis da empresa. As três linhas de defesa são: (1) controle gerencial e medidas de controle interno; (2) funções de supervisão ou especialização no gerenciamento de riscos; e (3) auditoria interna. Na distribuição de funções e responsabilidades, o modelo prima pela transparência na comunicação. Entre as funções centrais dessa estrutura estão diretores de conformidade, auditores internos, especialistas em controle interno e investigação de fraudes. O modelo não apresenta funções rígidas, deixa a cargo de cada organização avaliar seus recursos para compor suas defesas da melhor maneira.

Seis princípios regem o modelo: governança [2]; papéis do órgão de governança; gestão e papéis da primeira e segunda linhas; papéis da terceira linha; independência da terceira linha; criação e proteção de valor. Cada organização, com suas características próprias, saberá identificar em sua estrutura os papéis mais vocacionados para cada tarefa.

Nesse modelo, o órgão de governança determina a direção geral, definindo a visão, a missão, os valores e o apetite organizacional a riscos. A primeira linha, de gestão, identifica, analisa, avalia, trata e gerencia os riscos.

Ela projeta, opera e melhora os processos, procedimentos, políticas, garantias de conformidade, controles etc., além de coordenar estratégias para mitigação e estabelecer o nível aceitável de risco. Os papéis de segunda linha nunca são totalmente independentes da gestão, ao contrário dos papéis de terceira linha, que se caracterizam pela independência.

Encontra-se na norma da ISO 31000 a instrução para que a gestão de riscos cuide da integração de todos na abordagem dos riscos. E a recomendação do IIA destaca a necessidade de engajamento das três linhas nos objetivos da organização, o que tem consequência direta na interação do órgão de governança com as três linhas. A recomendação também assenta que “a base para uma coerência bem-sucedida é a coordenação, colaboração e comunicação regulares e eficazes” (pg. 8). Assim, consulta e feedback continuados sustentam uma GRC sem lacunas e sem redundâncias indesejadas. Seguindo esses dois estândares, a organização terá uma estrutura de gerenciamento de riscos robusta e flexível, ou seja, integrada em torno de um eixo sólido ao mesmo tempo descentralizada.

Apesar de não haver ainda adesão massiva à gestão descentralizada de riscos, ela está se tornando a realidade de algumas empresas e está mudando fundamentalmente a GRC. As crescentes ameaças de ataques ciberfísicos [3] inspiraram, ao redor do mundo, a criação de leis, regulamentos e portarias para garantir que empresas de diversos

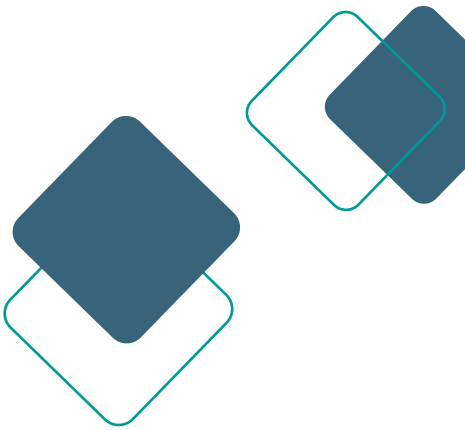
setores adiram a um conjunto comum de padrões sobre segurança, gerenciamento de riscos e resiliência operacional.

Para a equipe de risco, isso representa um grande progresso. Nos últimos 20 anos ou mais em que a resiliência operacional se tornou necessidade básica, os setores operacionais e até os estratégicos cuidaram de sua própria resiliência. Mais recentemente, veio a tendência à centralização nas mãos de um único líder, o CRO (Chief Risk Officer). Agora, entretanto, a resposta está sendo encontrada no meio termo – centralizar e integrar, seguindo a norma ISO 31000 e o modelo das três linhas.

A pandemia de Covid-19 e as mudanças climáticas representaram e representam riscos desconhecidos para os negócios em todo o mundo. Eventos como parada operacional, interrupção da cadeia de suprimentos, ataque cibernético e ameaças potenciais que ainda não estão identificadas apontam para a necessidade de as organizações terem meios para perceber e mitigar riscos em pouco tempo e manter nível ótimo de alerta para o que está por vir.

Se as empresas puderem implementar análises de cenários e quantificação de riscos aprimoradas, estarão em melhor posição para lidar com disrupções futuras. Da mesma forma, a quantificação do risco por meio de técnicas complementares de análise, como indicado na ISO 31010, pode apoiar a tomada de decisões com informações amplas e precisas.

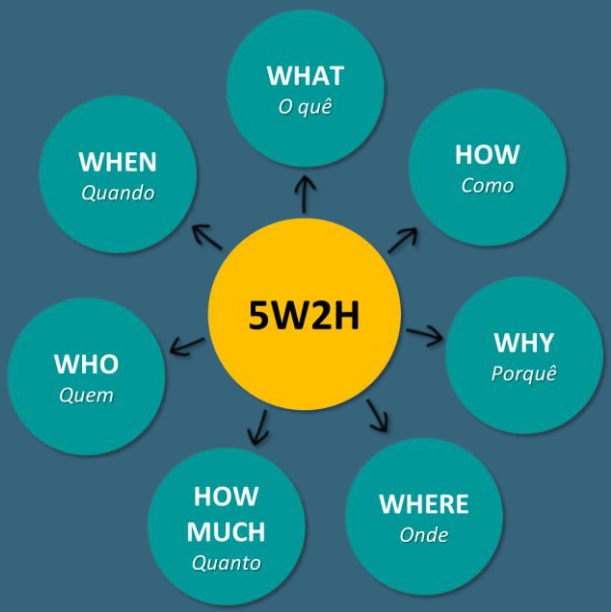
A capacidade do GRC de obter visibilidade em toda a organização não apenas leva a um negócio mais resiliente, mas também a uma reputação mais forte. Sem uma GRC apropriada para sustentar os negócios em longo prazo, haverá problemas de valor para o acionista e danos à reputação. Está a cargo das empresas criar estratégias para gerenciar os riscos de forma integrada e integral, ampliar a resiliência dos negócios e oferecer uma estrutura que favoreça a prosperidade da organização.

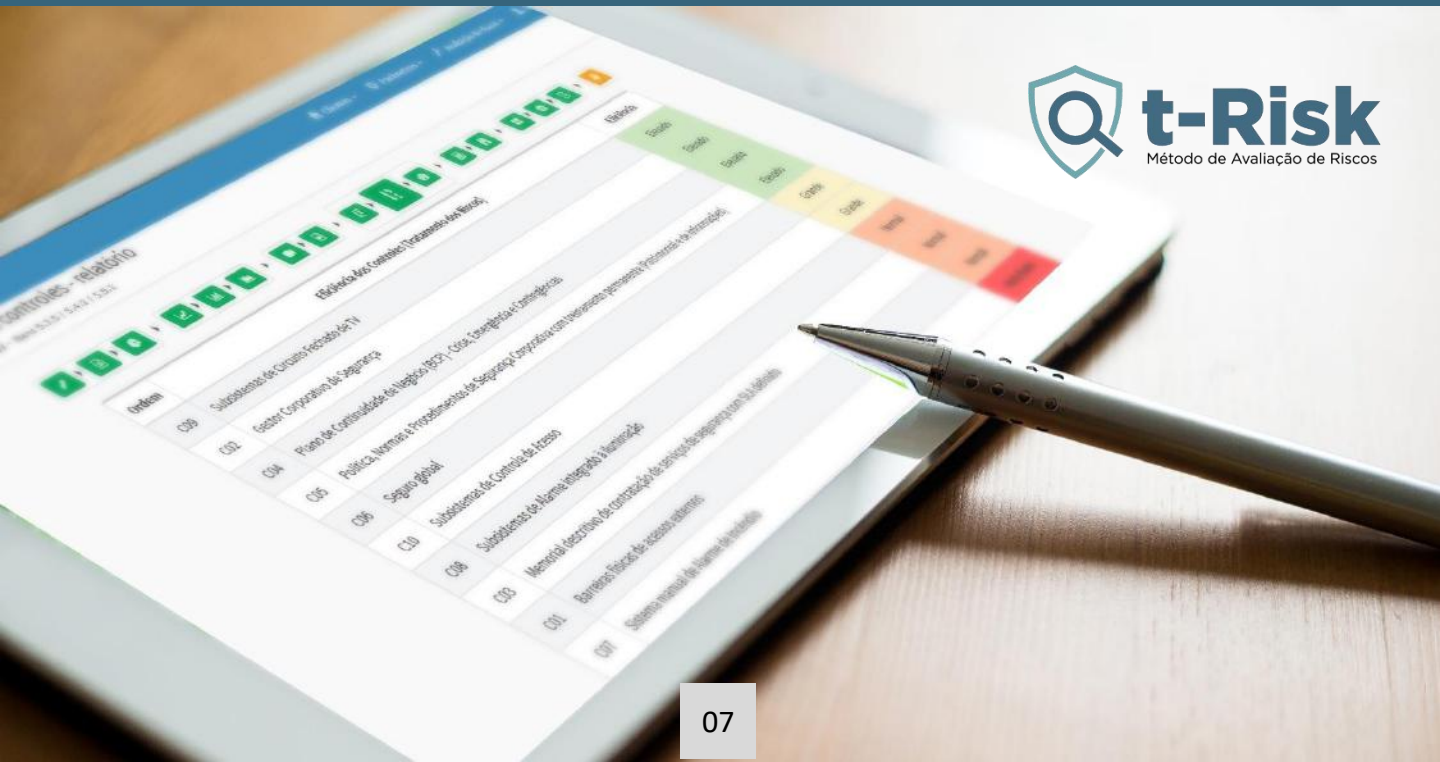


Sobre a Plataforma t-Risk

A **Plataforma t-Risk** (SaaS) está disponível **desde 2015** para apoiar as 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. Está em conformidade com o processo de gestão de riscos definido na ISO 31000. Disponível em **português, inglês e espanhol**, aumenta em até **80%** a produtividade.

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**.

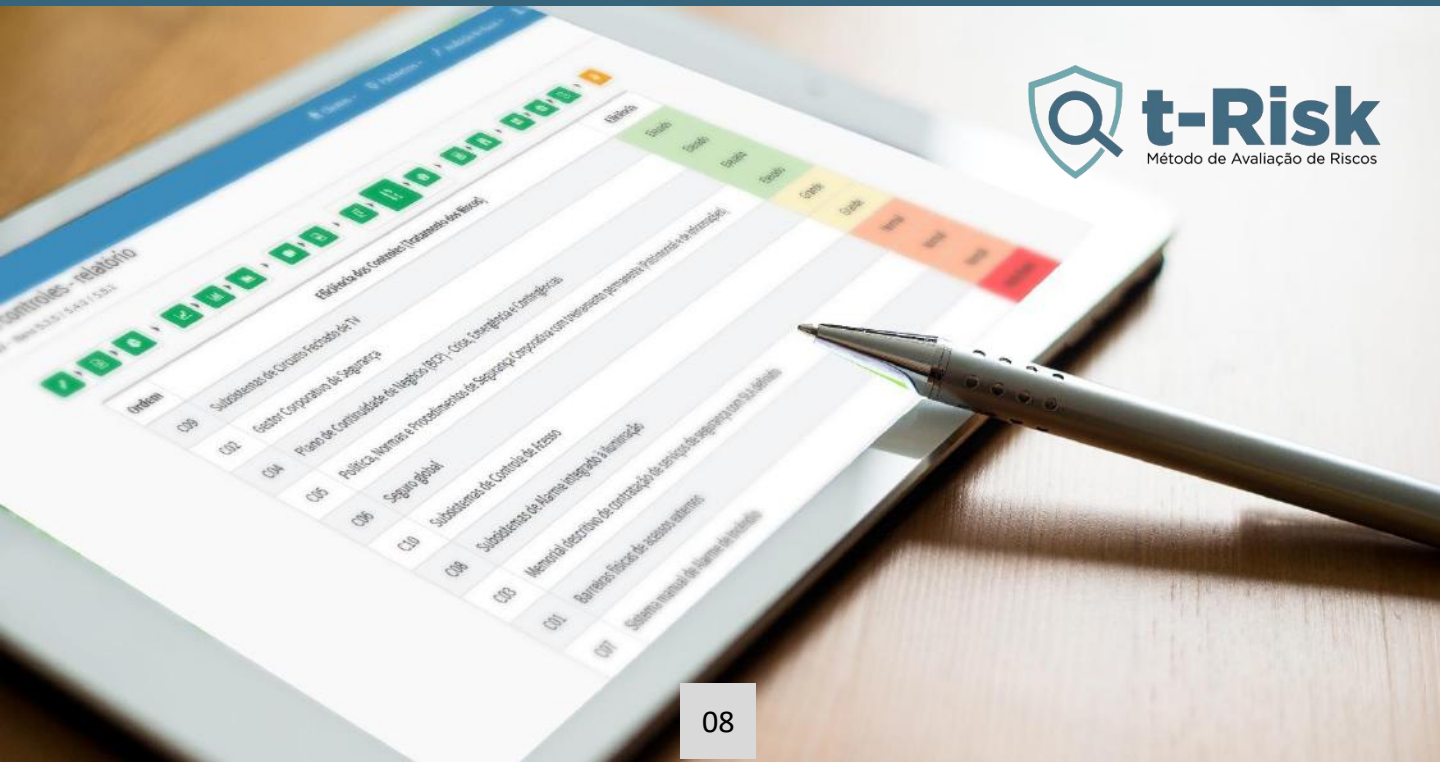




Sobre a Plataforma t-Risk

O Módulo de Gestão de Riscos de terceiros da Plataforma t-Risk, alinhando com a agenda ESG, colabora com a transformação digital das organizações, revolucionando o processo de gestão dos riscos de terceiros, proporcionando tomada de decisão ágil, eficaz, reduzindo custos em inúmeras atividades, como:

- Avaliação de **riscos de terceiros** (fornecedores e parceiros) **através de pesquisas automatizadas em bases de dados oficiais**;
- **Monitoramento permanente** dos riscos ESG (próprios e terceiros);
- Apoio em processos de **fusão e aquisição**;
- **Auditorias**, ***Due Diligence*** remotas e apoio nos processos de **investigação**;
- **Plano de ação** (5W2H) para mitigar riscos, monitoramento de pendências e prazos das tarefas com envio automático de e-mails;
- **Gráficos** e ***dashboards*** para acompanhamento em tempo real através de Power BI (Microsoft);
- Criação rápida e flexível de **relatórios para reuniões de conselho**;
- **Simplicidade** nos processos de coleta, cálculo e geração de relatórios.



Referências:

[1] www.globaliia.org; https://na.theiia.org/Pages/IIAês Home.aspx; https://iiabrasil.org.br/; https://guidehouse.com/insights/financial-services/2021/public-sector/garp-three-lines-of-defense.

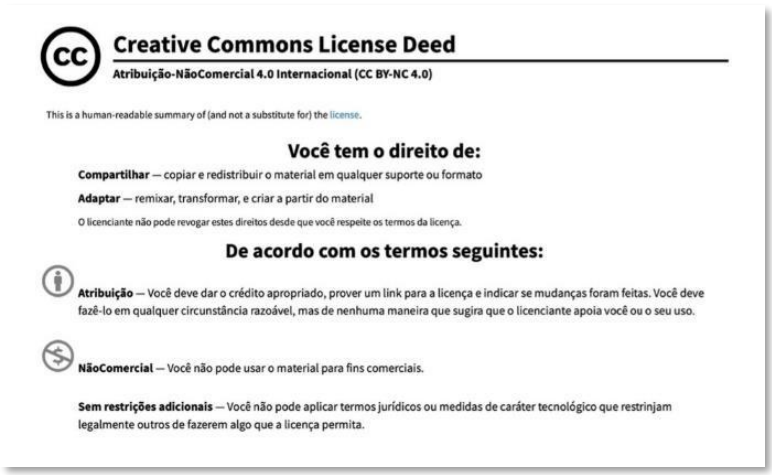
[2] *Ver o Código das Melhores Práticas de Governança Corporativa*: https://conhecimento.ibgc.org.br/Paginas/Publicacao.aspx?PubId=21138.

[3] *Ver o ebook Segurança ciberfísica nas empresas de energia: Desafios e oportunidades na proteção das infraestruturas críticas do setor elétrico brasileiro. Disponível em:* https://www.bibliotecadeseguranca.com.br/livros/seguranca-ciberfisica-nas-empresas-de-energia/.

Links úteis:

- www.totalrisk.com.br
- https://clearlinesaudit.com.au/centralised-decentralised/
- https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/enterprise-risk-management-practices-where-is-the-evidence
- https://www.niceactimize.com/blog/the-benefits-of-centralized-risk-management-systems-465/

Licença de distribuição, clique para acessar:



t-Risk

Método de Avaliação de Riscos