MAF
Consultoria e Treinamento

Apresenta:

Guia Simples de Governança, Riscos e Compliance para Pequenas e Médias Empresas

1. Conceitos Introdutórios de GRC

GRC é a sigla para **Governança, Gestão de Riscos e Compliance** — três pilares fundamentais para garantir que uma organização seja bem dirigida, proteja seu valor e opere em conformidade com as normas.

Esse processo deve ser patrocinado pela alta administração (ou pelos sócios e seus comitês, no caso das PMEs) e exige o envolvimento de todos: desde os executivos até os colaboradores e terceirizados. Cada pessoa deve atuar dentro dos limites de risco estabelecidos para suas atividades, sempre buscando realimentar a cadeia de valor da empresa com informações relevantes para a gestão estratégica.

O conceito moderno de GRC surgiu em 2004, através da organização norte-americana **OCEG (Open Compliance Ethics Group)**. Foi formalizado no documento conhecido como **Livro Vermelho (REDBOOK)**, ajustando práticas de governança e gestão de riscos para empresas de todos os portes — inclusive pequenas e médias.

No Brasil, o **Instituto Brasileiro de Governança Corporativa (IBGC)** desempenhou um papel importante na adaptação desses conceitos para nossa realidade empresarial. Segundo o IBGC, GRC é composto por três elementos centrais:

1.1 Governança Corporativa

Governança corporativa é o **sistema pelo qual empresas e outras organizações são dirigidas, monitoradas e incentivadas**. Ela envolve a relação entre sócios, conselhos de administração, diretorias, órgãos de controle e todas as partes interessadas.

Seus princípios fundamentais são:

- **Transparência**: Comunicar com clareza as informações relevantes para todos os stakeholders.
- **Equidade**: Garantir tratamento justo e igualitário a todos os sócios e partes interessadas.
- **Prestação de Contas (Accountability)**: Ser claro e responsável na prestação de contas à sociedade e aos investidores.
- **Responsabilidade Corporativa**: Atuar de forma responsável diante dos impactos sociais e ambientais.

Nota prática para PMEs:

O IBGC recomenda que a estrutura de governança seja **proporcional** ao tamanho, complexidade e contexto da empresa — o que é especialmente importante para pequenas e médias empresas, que podem (e devem) adotar práticas ajustadas à sua realidade.

O que você precisa lembrar desta seção:

- GRC integra governança, gestão de riscos e compliance de forma estratégica.
- Foi desenvolvido para ser adaptável a empresas de todos os tamanhos, inclusive PMEs.
- Governança corporativa trata da direção, monitoramento e incentivo à boa gestão, com base nos princípios de transparência, equidade, prestação de contas e responsabilidade.
- Pequenas e médias empresas podem — e devem — adotar uma governança proporcional às suas necessidades e riscos.

2. A Importância da Integração de GRC para as PMEs

As **Pequenas e Médias Empresas (PMEs)** têm um papel vital na economia brasileira. Elas estão no centro da geração de empregos, da inovação e da dinâmica dos negócios regionais.

Segundo dados do SEBRAE e de outros órgãos, as PMEs representam:

- **27% a 30% do PIB nacional**
- **Mais de 50% dos empregos formais**
- **Cerca de 99% do total de empresas do Brasil**

Apesar dessa relevância, as PMEs enfrentam hoje um desafio crescente: **navegar num ambiente regulatório cada vez mais complexo**, sem ter a estrutura robusta de grandes corporações.

O desafio da proporcionalidade regulatória

Nos últimos anos, houve uma multiplicação de **leis, normas e obrigações** que também afetam as PMEs. Mesmo sem serem companhias listadas na bolsa, essas empresas estão sendo cobradas em áreas como:

- Proteção de dados (LGPD)
- Integridade e anticorrupção
- Sustentabilidade e ESG
- Cybersegurança
- Obrigações trabalhistas, tributárias e setoriais

O problema é que **a maioria das PMEs não tem equipes dedicadas de compliance, riscos ou auditoria interna**. E, mesmo assim, precisam lidar com pressões semelhantes às das grandes empresas — só que com muito menos recursos.

As dúvidas mais comuns entre os gestores de PMEs

Neste contexto, surgem perguntas práticas e legítimas:

- Quais normas realmente se aplicam à minha empresa — e quais são ruído?
- Como adotar uma metodologia de GRC simples, sem burocracia e com foco em riscos reais?
- Como tratar temas como LGPD, ESG e integridade de forma prática e inteligente?
- Por que existem tantos termos e órgãos diferentes falando de governança e compliance — e ninguém mostra um mapa simples?
- Vale mais a pena **centralizar ou descentralizar** a estratégia de mitigação de riscos?

Essas são **dúvidas recorrentes** entre líderes de PMEs — e precisam de respostas objetivas e adaptadas à realidade do negócio.

O que outros países já estão fazendo

Em vários países, como Estados Unidos, Reino Unido e Alemanha, **já existem frameworks e guias simplificados de GRC** voltados especificamente para pequenas e médias empresas.

No Brasil, embora existam boas iniciativas voltadas para empresas familiares (por exemplo, do IBGC), **ainda faltam modelos integrados de GRC adaptados à complexidade e ao porte das PMEs**.

A maioria dos materiais disponíveis é:

- Ou muito acadêmica e técnica
- Ou genérica e pouco aplicável
- Ou foca em apenas um dos pilares do GRC, sem integração entre governança, riscos e compliance

Por isso, há uma **lacuna prática de orientação** — que este guia se propõe a preencher.

O que propomos com o SIMPLES GRC

Este material tem como objetivo mostrar que é possível, sim, **implementar um GRC proporcional, inteligente e prático** em pequenas e médias empresas.

Isso inclui:

- Traduzir frameworks como **COSO ERM** e **ISO 31000** para a realidade da PME
- Integrar o que há de mais relevante em governança, integridade e conformidade
- Evitar duplicidades, burocracias ou abordagens teóricas demais
- E entregar **valor real e aplicável** — sem perder de vista os recursos limitados de tempo, pessoal e orçamento

O que você precisa lembrar desta seção

- As PMEs representam quase toda a base empresarial do Brasil — mas lidam com pressões desproporcionais.

- O aumento das exigências regulatórias afeta diretamente a operação, a competitividade e a continuidade das PMEs.
- Ainda há poucos guias no Brasil que traduzam GRC para a realidade prática das pequenas e médias empresas.
- Um modelo adaptado e simplificado de GRC é urgente e necessário — e possível de implementar com inteligência e foco.

3. Principais Leis Relevantes para PMEs

Implementar um modelo de GRC eficiente em pequenas e médias empresas exige, antes de tudo, **compreender o ambiente regulatório em que essas empresas estão inseridas**.

As PMEs estão sujeitas a um conjunto de leis que, se não forem corretamente observadas, podem gerar penalidades severas, riscos de imagem e entraves ao crescimento do negócio. Por isso, conhecer os marcos legais mais relevantes é o primeiro passo para construir um GRC proporcional, estratégico e funcional.

A seguir, destacamos os principais grupos de normas que impactam diretamente as PMEs no Brasil.

3.1 Leis Trabalhistas e Previdenciárias

Essas normas regulam todos os aspectos da relação entre empresa e colaborador, como:

- Contratos de trabalho
- Jornada, horas extras e descanso semanal

- Segurança e saúde no trabalho
- Contribuições ao INSS e depósitos de FGTS

Riscos do descumprimento:

Passivos trabalhistas, ações judiciais, autuações da fiscalização e impacto direto na imagem da empresa perante colaboradores e sindicatos.

3.2 Obrigações Fiscais e Tributárias

Incluem leis e normas que tratam de:

- Pagamento de tributos federais, estaduais e municipais
- Emissão de notas fiscais e escrituração contábil
- Regimes como Simples Nacional, Lucro Presumido ou Lucro Real

Riscos do descumprimento:

Sanções da Receita Federal e dos fiscos estaduais/municipais, perda de benefícios fiscais e complicações para participar de licitações e parcerias com grandes empresas.

3.3 Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018)

A LGPD regula o **tratamento de dados pessoais**, estabelecendo direitos para os titulares e obrigações para as empresas. Mesmo as PMEs devem estar atentas aos seus deveres em relação aos dados de clientes, funcionários, fornecedores e parceiros.

Pontos de atenção para PMEs:

- Coleta de consentimento
- Políticas de privacidade atualizadas
- Mapeamento e proteção do fluxo de dados
- Atendimento aos direitos dos titulares

Riscos do descumprimento:

Multas administrativas de até R$ 50 milhões, além de ações judiciais, perdas contratuais e danos reputacionais.

3.4 Código de Defesa do Consumidor (CDC – Lei nº 8.078/90)

Aplicável a empresas que vendem produtos ou prestam serviços ao consumidor final, o CDC garante:

- Direito à informação clara e objetiva
- Qualidade e segurança do produto ou serviço
- Garantias legais e contratuais
- Canais de atendimento e solução de conflitos

Riscos do descumprimento:

Ações civis públicas, danos à imagem da marca, perda de confiança e aumento de reclamações em órgãos como Procon e plataformas como Reclame Aqui.

3.5 Regulamentações Específicas por Setor

Cada atividade econômica possui **regras adicionais específicas**, como:

- Vigilância sanitária (alimentos e cosméticos)
- Normas técnicas da Anvisa ou Inmetro
- Autorizações setoriais (educação, saúde, finanças, transportes)

Recomendações para PMEs:

- Verifique junto ao contador e ao sindicato da categoria quais normas específicas se aplicam à sua empresa.
- Mantenha atualizado o cadastro junto aos órgãos reguladores do seu setor.

3.6 Normas de Segurança e Saúde no Trabalho (NRs)

As **Normas Regulamentadoras (NRs)** definem requisitos mínimos para segurança e saúde ocupacional, como:

- Equipamentos de proteção individual (EPI)
- Treinamentos obrigatórios
- Controle de agentes insalubres
- Ergonomia e ambiente físico adequado

Riscos do descumprimento:

Ações trabalhistas, interdições de operação, responsabilização civil e criminal dos gestores e aumento de custos com afastamentos.

3.7 Leis Ambientais (Federais, Estaduais e Municipais)

As empresas devem observar normas que regulam:

- Licenciamento ambiental
- Controle de emissão de resíduos, ruídos e poluentes
- Uso de recursos naturais
- Proteção de áreas de preservação

Mesmo empresas de pequeno porte podem estar sujeitas a essas leis, dependendo do tipo de atividade exercida.

3.8 ESG e Cybersegurança como extensões da conformidade

Embora não sejam leis isoladas, os temas de **sustentabilidade (ESG)** e **cybersegurança** estão diretamente relacionados ao GRC moderno. Reguladores e grandes empresas parceiras já esperam que PMEs tenham ações mínimas nessas frentes, como:

- Políticas de diversidade e inclusão
- Compromisso com práticas ambientais responsáveis
- Medidas de proteção contra vazamento de dados e ataques cibernéticos

Negligenciar esses pontos pode afetar a competitividade e a imagem institucional da empresa.

O que você precisa lembrar desta seção

- As PMEs precisam estar em conformidade com um conjunto amplo de normas, que vão além da área fiscal ou trabalhista.

- A LGPD e o Código de Defesa do Consumidor são dois marcos regulatórios que afetam diretamente a operação das PMEs.
- Regulamentos setoriais e normas ambientais e de segurança do trabalho também são críticos, mesmo em empresas de menor porte.
- Integrar esses aspectos ao modelo de GRC da empresa é essencial para evitar riscos legais e reputacionais.

4. Referências sugeridas para estrutura e finalidade do desenvolvimento de um Guia

A construção de um modelo de GRC adaptado à realidade das Pequenas e Médias Empresas requer mais do que boas intenções: exige **referenciais sólidos, testados e reconhecidos internacionalmente**.

Este capítulo apresenta as principais bases técnicas que fundamentam a proposta do Guia SIMPLES GRC. São normas, frameworks e publicações que — quando integradas — permitem estruturar um modelo enxuto, prático e proporcional às necessidades das PMEs.

Fontes e estruturas de referência

A seguir, estão os principais marcos normativos e guias utilizados na construção da metodologia sugerida neste material:

Gerenciamento de Riscos e Compliance

- **ISO 31000:2018** – Gestão de Riscos (ABNT NBR ISO 31000): fornece diretrizes universais para estabelecer e manter uma cultura e processo de gestão de riscos.

- **COSO ERM 2017** – Enterprise Risk Management: estrutura voltada para integrar riscos à estratégia e ao desempenho do negócio.
- **OCEG RED BOOK 3.5** – Guia internacional de GRC integrado, com foco em governança, riscos, compliance e cultura ética.

Governança Corporativa no contexto brasileiro

- **IBGC – Guia de Gerenciamento de Riscos Corporativos (2017)**
- **IBGC – Manual de Governança Corporativa (6ª edição – 2023)**
- **IBGC – Compliance à Luz da Governança Corporativa (2017)**
- **IBGC – Governança da Família Empresária (2016)**

Integridade e pequenas empresas

- **CGU – Programa de Integridade para Empresas Privadas (2024)**
- **CGU & SEBRAE – Integridade para Pequenos Negócios (2017)**

Proteção de dados, ESG e cibersegurança

- **NIST Cybersecurity Framework 2.0 – Small Business Guide (2024)**
- **SEBRAE – LGPD Connect (2020)**
- **SEBRAE – ESG para Micro e Pequenas Empresas (2023)**
- **SEBRAE – A importância do ESG para pequenos negócios (2024)**

Essas referências foram combinadas para **traduzir conceitos avançados em ações simples, práticas e alinhadas à realidade brasileira das PMEs**.

Por que é necessário um guia próprio para PMEs?

A maior parte dos materiais de GRC disponíveis hoje são voltados para grandes corporações, com estruturas formais de conselhos, comitês e times técnicos internos. As PMEs, por sua vez, **operam com recursos limitados, múltiplas funções concentradas nas mesmas pessoas e pouco tempo para estudar normas extensas**.

Por isso, é essencial:

- **Traduzir os conceitos técnicos em linguagem simples**
- **Adaptar os requisitos à estrutura real das PMEs**
- **Indicar caminhos viáveis para empresas com poucos recursos humanos e financeiros**
- **Criar uma lógica escalável, que possa crescer junto com a empresa**

O papel deste Guia para as PMEs

Este guia não pretende esgotar o tema, mas sim servir como uma **plataforma inicial de orientação e estruturação do GRC** em empresas de pequeno e médio porte.

Seus objetivos são:

- **Democratizar o conhecimento:** Tornar os princípios de GRC acessíveis a todos na organização, mesmo a quem não possui formação técnica na área.
- **Oferecer um roteiro claro:** Apresentar um passo a passo prático, da identificação de riscos à implementação de controles e rotinas de acompanhamento.
- **Adaptar a GRC à realidade da PME:** Ilustrar os conceitos com exemplos aplicáveis a estruturas mais enxutas e ágeis.
- **Facilitar a comunicação interna:** Criar uma linguagem comum sobre governança, riscos e compliance entre os gestores e colaboradores.

- **Reduzir a complexidade:** Evitar jargões desnecessários e transformar frameworks robustos em ferramentas simples e acionáveis.

O que você precisa lembrar desta seção

- As melhores práticas internacionais de GRC podem — e devem — ser adaptadas para a realidade das PMEs.
- Este guia é baseado em estruturas consagradas como ISO 31000, COSO ERM, IBGC, NIST, CGU e SEBRAE.
- A proposta não é implantar uma estrutura robusta e cara, mas sim **iniciar a jornada com passos viáveis e sustentáveis**.
- O foco está em orientar, simplificar e viabilizar, respeitando as limitações típicas das PMEs brasileiras.

5. Centralização e Descentralização de GRC em PMEs

A implementação de GRC em pequenas e médias empresas precisa considerar a estrutura organizacional real e os recursos disponíveis. Nesse contexto, uma das decisões mais importantes é **definir o equilíbrio entre centralização e descentralização das funções de Governança, Riscos, Compliance e Auditoria Interna**.

O modelo ideal dependerá do porte, da maturidade da empresa, da complexidade das operações e da qualificação dos gestores. A seguir, destacamos os pontos centrais a considerar.

5.1 Governança: centralizada, mas com estrutura

Nas PMEs, é comum que a governança seja mais concentrada nas mãos dos **sócios-fundadores ou da alta direção**. Isso, por si só, não é um problema — desde que haja clareza sobre:

- **Papéis e responsabilidades** de cada gestor
- **Processo decisório transparente e documentado**
- **Alinhamento estratégico entre os sócios**
- **Comunicação regular sobre objetivos e indicadores**

Mesmo sem um conselho formal, boas práticas de governança — como reuniões mensais, atas e registros de deliberações — ajudam a estruturar a empresa e facilitam a transição futura para um modelo mais distribuído.

5.2 Gestão de Riscos: foco e pragmatismo

A gestão de riscos em PMEs deve ser **centralizada nos gestores estratégicos**, com foco nos riscos mais críticos para a continuidade e o crescimento do negócio.

Esses riscos geralmente envolvem:

- **Financeiros:** inadimplência, fluxo de caixa, endividamento
- **Operacionais:** falhas de processos, retrabalho, gargalos produtivos
- **De mercado:** concorrência, mudanças regulatórias, sazonalidade
- **De crédito:** análise superficial de clientes ou fornecedores
- **De segurança e regulatórios:** LGPD, passivos trabalhistas, segurança do trabalho

Em empresas menores, o mapeamento e o tratamento desses riscos podem ser conduzidos por **reuniões de sócios com apoio de ferramentas simples**, como matriz de risco, planos de ação e indicadores de controle.

5.3 Compliance: legalidade como eixo central

A função de compliance em PMEs deve **garantir a conformidade legal e regulatória com base em um modelo simples, porém efetivo**. Isso inclui:

- Cumprimento de **leis trabalhistas, fiscais, ambientais, sanitárias e de proteção de dados (LGPD)**
- Definição clara de **obrigações periódicas** e **responsáveis por cada entrega**
- Monitoramento de **mudanças legais que impactam o setor de atuação**

Em áreas mais complexas, onde o conhecimento é técnico e específico (ex: contabilidade, jurídico, LGPD, segurança cibernética), o compliance pode ser delegado aos próprios gestores, com apoio de **uma estrutura mínima central de governança**, como uma planilha de controle ou um canal interno de reporte.

5.4 Auditoria Interna: proporcional ao porte

Auditoria interna em PMEs não precisa ser um departamento. Ela pode assumir diferentes formatos, sempre respeitando a maturidade e os recursos disponíveis:

Cenário 1: Microempresas ou pequenas com até 5 colaboradores

- Um dos sócios pode assumir a função de auditoria, com revisões periódicas dos principais processos e registros.
- Reuniões mensais com foco em **controle financeiro, contratos e indicadores** já são um bom começo.

Cenário 2: PMEs com estrutura administrativa básica

- Pode-se designar um colaborador de confiança com **visão global do negócio** para realizar revisões de processos e apontar melhorias, mesmo que essa não seja sua função principal.
- Essa função deve ter **autonomia relativa**, mas deve reportar diretamente aos sócios.

Cenário 3: Empresas em crescimento ou com mais exposição regulatória

- A contratação de **auditores externos por períodos (trimestral, semestral ou anual)** pode ser uma solução custo-efetiva para obter uma visão independente e garantir a integridade dos processos.
- Esses profissionais devem ter um **escopo definido e foco nos pontos críticos**, como controles financeiros, conformidade fiscal, segurança da informação e governança de dados.

O que você precisa lembrar desta seção

- Em PMEs, é natural que a governança seja mais centralizada, mas isso não significa ausência de estrutura.
- A gestão de riscos deve ser objetiva, com foco no que realmente ameaça a operação e o crescimento.
- A função de compliance pode ser compartilhada entre os próprios gestores, desde que exista uma estrutura mínima de coordenação e registro.
- Auditoria interna não precisa ser um departamento formal: pode começar como uma responsabilidade designada, com revisões simples e objetivas, evoluindo conforme o crescimento da empresa.

6. Desafios e Benefícios da Implementação de um Simples GRC em PMEs

Implementar práticas de Governança, Gestão de Riscos e Compliance em pequenas e médias empresas é um caminho necessário — mas nem sempre simples. Por isso, é importante reconhecer de forma objetiva **quais são os obstáculos mais comuns e quais os benefícios reais e mensuráveis** que esse tipo de iniciativa pode trazer para a empresa.

A seguir, apresentamos os principais **desafios enfrentados pelas PMEs** ao iniciar a estruturação de um GRC proporcional e inteligente.

6.1 Principais desafios na prática

1. Recursos limitados

A maioria das PMEs opera com **orçamento enxuto e equipes multifuncionais**. Isso dificulta:

- A criação de áreas exclusivas para GRC
- A alocação de tempo para desenvolver guias e políticas internas
- A contratação de consultorias especializadas ou auditores externos

2. Falta de conhecimento especializado

Muitas vezes, **os gestores desconhecem os conceitos, ferramentas ou benefícios** de um programa de GRC. Também pode faltar:

- Familiaridade com termos técnicos
- Capacidade de identificar riscos ocultos

- Tempo para estudar normas e frameworks

3. Priorização de áreas ligadas à receita

Em cenários de pressão por crescimento e estabilidade financeira, a gestão tende a **concentrar esforços em vendas, marketing, operações e produção**. Iniciativas de GRC acabam vistas como "custo" ou algo secundário — quando, na verdade, são **ferramentas para evitar perdas e fortalecer a sustentabilidade do negócio**.

4. Resistência à mudança

A cultura da empresa pode ser um freio natural ao avanço do GRC, especialmente quando os processos são historicamente informais. É comum ouvir frases como:

- "Sempre fizemos assim"
- "Isso é coisa para empresa grande"
- "Vai burocratizar demais"

Superar essa resistência exige comunicação clara sobre os benefícios e implementação gradual, com foco em resultados práticos.

6.2 Benefícios concretos da implementação

Apesar dos obstáculos iniciais, os ganhos são expressivos — especialmente a médio e longo prazo. Um modelo simples e bem aplicado de GRC pode trazer:

Redução de perdas

- Previne fraudes, erros operacionais e multas por descumprimento de normas
- Ajuda a evitar decisões mal fundamentadas ou riscos não identificados

Eficiência operacional

- Organiza processos, reduz retrabalho e facilita a delegação
- Promove a cultura de melhoria contínua com base em evidências

Confiança de stakeholders

- Melhora a imagem da empresa diante de clientes, fornecedores, bancos e investidores
- Facilita parcerias com grandes empresas que exigem critérios mínimos de integridade

Base para crescimento sustentável

- Ajuda na gestão profissionalizada do negócio
- Cria estrutura para expansão com menos riscos e mais controle

O que você precisa lembrar desta seção

- Implementar GRC em uma PME não é fácil, mas é viável — e estratégico.
- Os principais desafios são falta de recursos, conhecimento, tempo e adesão cultural.
- A abordagem precisa ser proporcional, objetiva e aplicada de forma progressiva.
- Os benefícios são reais: redução de perdas, ganho de eficiência, maior confiança no mercado e mais segurança para crescer com consistência.

7. Integrando conceitos e exemplos para um Guia de GRC e Auditoria em PMEs

A construção de um modelo de GRC eficaz em pequenas e médias empresas depende da capacidade de **traduzir os principais frameworks internacionais** em práticas aplicáveis à realidade brasileira, com foco na objetividade, simplicidade e custo-benefício.

Neste capítulo, apresentamos uma abordagem prática de como integrar as diretrizes do **COSO ERM (2017)**, da **ISO 31000:2018** e do **Guia IBGC (2020)** com ações adaptadas à estrutura de uma PME. A proposta é oferecer um roteiro que simplifique a aplicação dos 20 princípios do GRC, preservando sua essência.

7.1 Bases técnicas integradas

Os três marcos principais utilizados como base para este guia são:

- **COSO ERM (2017):** Estrutura voltada para alinhar riscos à estratégia e à criação de valor, com foco em cinco componentes e 20 princípios.
- **ISO 31000:2018:** Proposta baseada em princípios, estrutura e processo, com ênfase na personalização e integração com os processos de negócio.
- **IBGC – Guia de Gerenciamento de Riscos (2020):** Adapta o papel da governança e da alta administração à realidade brasileira, com orientações práticas.

Cada um desses modelos tem seu valor. A proposta aqui é **consolidar suas diretrizes em um único quadro adaptado à realidade das PMEs**, permitindo sua implementação gradual, com foco em resultados tangíveis.

7.2 Estrutura de integração para PMEs

A seguir, a tabela apresenta a relação entre os três marcos de referência e os exemplos de aplicação prática para pequenas e médias empresas.

- O conteúdo está organizado por **componente de GRC**, seguindo os cinco eixos do COSO ERM:
    - Governança e Cultura
    - Estratégia e Definição de Objetivos
    - Desempenho
    - Revisão e Monitoramento
    - Informação, Comunicação e Relatórios

- Em cada linha, mostramos:
    - O que o COSO e a ISO propõem
    - O que o IBGC recomenda
    - E como isso pode ser executado em uma PME, com poucos recursos e estrutura enxuta

COSO ERM (2017) Componentes e Princípios	ISO 31000:2018 – Diretrizes	IBGC (2020) – Guia de Gerenciamento de Riscos	Adaptação para PMEs (Brasil)

1. Governança e Cultura	- Liderança e comprometimento - Integração	- Papel do Conselho e da Alta Administração - Cultura organizacional	Envolver sócios/gestores; separar patrimônios e principal e agente; promover ética e cultura de riscos simples e com códigos de ética e sustentabilidade integrados
1. Exerce supervisão de risco			Responsável principal define tom e participa ativamente. Calibração da centralização com a descentralização. Eliminação de riscos por acordo de acionistas e separação de patrimônio.
2. Estabelece a estrutura operacional			Estrutura enxuta com papéis definidos (ex: sócio responsável, especialista em GRC e Auditoria e Gestores responsáveis por riscos muito especializados (TI-LGPD-Cyber, RH-Pessoas; ESG e continuidade operacional)
3. Define cultura desejada			Promover ética, confiança e comunicação clara e canais de comunicação para riscos, incidentes e irregularidades

4. Demonstra compromisso com valores essenciais			Reforça missão, visão, valores, estratégia, governança e Integridade como valor central do negócio
5. Atrai, desenvolve e retém indivíduos capacitados			Capacitação b/básica da equipe, contratando conforme necessário. Tem um plano de continuidade para recursos sensíveis
2. Estratégia e Definição de Objetivos	- Integração com governança, estratégia e planejamento - Apetite ao risco	- Alinhamento estratégico - Apetite ao risco	Definir objetivos claros e limites de risco aceitáveis
6. Analisa contexto de negócio			Entendimento básico do setor, concorrência, ambiente e modelos SWOT
7. Define apetite ao risco			Discussão qualitativa com sócios sobre riscos aceitáveis e com os quais não pode haver tolerância
8. Avalia alternativas de estratégias			Análise simplificada de cenários e de estratégias diante de movimentos da concorrência ou tecnologias
9. Fórmula objetivos de negócio			Objetivos mensuráveis e vinculados ao sucesso da empresa. Define indicadores de metas de cada objetivo

3. Desempenho	- Avaliação de riscos - Comunicação e consulta - Resposta e controles	- Identificação e avaliação - Resposta e controles	Riscos levantados com base na operação real
10. Identifica riscos			Brainstorming simples com equipe para listar riscos que impactam cada objetivo e meta de negócio
11. Avalia severidade do risco			Matriz impacto versus probabilidade com linguagem simples (ver gráfico exemplificativo no item x)
12. Prioriza riscos			Classificação por criticidade em relação ao tratamento (respostas a riscos)
13. Implementa respostas ao risco	- Tratamento de riscos	Estratégias de mitigação	Definir ações práticas (controles para evitar e reduzir, riscos aceitos, riscos transferidos) e análise custo do controle versus perda protegida ou valor adicionado)
14. Desenvolve portfólio de riscos			Visão consolidada dos principais riscos da empresa, com o apoio da unidade de GRC e Auditoria. Mapa de Calor faz parte das reuniões mensais gerenciais e com os sócios
4. Revisão e Monitoramento	- Monitoramento e revisão - Reavaliação de riscos	- Acompanhamento de indicadores - Reavaliação de riscos	Acompanhar evolução e eficácia das ações

15. Avalia mudanças significativas			Monitorar alterações legais, fiscais ou de mercado e da concorrência e alterações no mapa de riscos
16. Revisa desempenho de risco			Avaliar resultados periódicos e ajustar planos de remediação com base em relatórios e indicadores de incidentes e perdas
17. Melhora o ERM			Aprendizado contínuo com erros e acertos em brainstorming com a equipe
5. Informação, Comunicação e Relatórios	- Comunicação e consulta - Registro e relato	- Relatórios ao Conselho - Transparência	Comunicação interna clara e relatórios objetivos
18. Usa informação relevante			Dados simples, mas úteis para decisões (ex: fluxo de caixa, inadimplência)
19. Comunica risco de forma útil			Reuniões curtas para discutir riscos e ações em reuniões mensais ou por evento
20. Reporta sobre riscos, cultura e desempenho			Relatórios resumidos para sócios ou investidores ou à disposição dos órgãos reguladores para verificar efetividade do programa de compliance requerido pela legislação e licitações

7.3 Exemplos de adaptação prática

Governança e Cultura:

- Iniciar com o envolvimento direto dos sócios, definindo claramente papéis, ética e cultura de riscos.
- Separar decisões operacionais do patrimônio pessoal.
- Utilizar um código de conduta simples e reuniões periódicas para avaliar riscos.

Estratégia e Objetivos:

- Realizar análises SWOT e reuniões estratégicas semestrais para definição de metas e apetite ao risco.
- Trabalhar com indicadores simples e objetivos vinculados ao sucesso da empresa.

Desempenho e Risco:

- Aplicar brainstorming com a equipe para identificar riscos relevantes.
- Criar uma matriz de impacto x probabilidade com linguagem acessível.
- Definir respostas aos riscos com base em custo x benefício.

Monitoramento e Aprendizado:

- Acompanhar mudanças regulatórias, resultados e lições aprendidas com base em reuniões mensais.
- Utilizar relatórios simples para revisar desempenho e atualizar planos de mitigação.

Comunicação e Relatórios:

- Realizar reuniões objetivas com os sócios e lideranças para comunicar riscos.
- Manter relatórios internos sintéticos com indicadores de risco e plano de ação.

O que você precisa lembrar desta seção

- É possível aplicar as diretrizes do COSO, da ISO 31000 e do IBGC em PMEs com estruturas simplificadas.
- A integração entre os modelos permite evitar redundâncias e criar um sistema coerente e prático.
- O foco deve estar em **ações de alto impacto e fácil execução**, com instrumentos que possam evoluir com o tempo.
- O quadro apresentado resume as adaptações essenciais para uma PME implantar um GRC funcional

8. Estratégias de Mitigação de Riscos por Controles Internos

A identificação dos riscos é apenas o primeiro passo na estruturação do GRC em uma PME. O passo seguinte — e mais crítico — é definir **controles internos simples e eficientes para mitigá-los**.

Este capítulo apresenta sugestões práticas de controles divididos por **tipos de risco** mais comuns na realidade das pequenas e médias empresas, considerando seus recursos limitados e suas prioridades operacionais.

8.1 Riscos Estratégicos de Negócio

Desafio: Incapacidade de adaptação às mudanças de mercado, concorrência ou comportamento do consumidor.

Controles recomendados:

- Monitoramento contínuo da concorrência e tendências setoriais
- Análises SWOT semestrais com a equipe
- Planos de inovação e desenvolvimento de produtos/serviços
- Pesquisas de satisfação e canais de feedback
- Participação em redes e associações do setor

8.2 Riscos de Inovação Digital

Desafio: Adoção ineficaz de tecnologia, segurança cibernética frágil e uso irresponsável de dados.

Controles recomendados:

Governança da inovação:

- Comitê de Inovação Digital com foco em projetos estratégicos
- KPIs claros para inovação e transformação digital
- Gestão ágil de projetos tecnológicos

Segurança cibernética industrial:

- Plano de segurança digital
- Segmentação de redes industriais
- Monitoramento contínuo e treinamento para operadores

Gestão de dados e analytics:

- Políticas de coleta e armazenamento

- Ferramentas de análise e inteligência de dados
- Dashboards gerenciais

Checklist de uso de IA em PMEs:

Inclui tópicos como finalidade clara, transparência para o cliente, responsabilidade legal, segurança dos dados, avaliação de viés, explicabilidade e capacitação da equipe.

8.3 Riscos de Governança

Desafio: Falta de clareza em papéis, decisões e sucessão.

Controles recomendados:

- Organograma formalizado e descrição de cargos
- Acordo de sócios estruturado (especialmente em empresas familiares)
- Reuniões periódicas com stakeholders
- Políticas de alçadas e delegação de poderes
- Avaliação regular da performance da gestão

8.4 Riscos de Integridade

Desafio: Condutas antiéticas, corrupção, fraudes internas e danos à imagem institucional.

Controles recomendados:

- Código de ética e conduta divulgado e aplicado
- Canais de denúncia seguros e independentes

- Políticas anticorrupção formalizadas
- Treinamentos periódicos sobre ética e integridade
- Due diligence de terceiros
- Gestão de conflitos de interesse
- Cultura de conformidade como valor da empresa

8.5 Riscos Financeiros

Desafio: Falhas em controles, fraudes ou má gestão de fluxo de caixa.

Controles recomendados:

- Segregação de funções nas operações financeiras
- Controles no ciclo de compras, vendas e pagamentos
- Projeção e monitoramento do fluxo de caixa
- Reconciliação bancária periódica
- Política de investimentos
- Auditoria interna (mesmo simplificada)

8.6 Riscos Operacionais

Desafio: Interrupções, falhas técnicas ou processos não documentados.

Controles recomendados:

- Planos de continuidade de negócio
- Backups regulares e testados

- Manutenção preventiva de equipamentos
- Seguros contra perdas e interrupções
- Treinamentos para resposta a emergências
- Monitoramento de sistemas automatizados

8.7 Riscos ESG (Ambientais, Sociais e de Governança)

Desafio: Pressões de mercado, ativismo, exigências contratuais e responsabilidade social.

Controles recomendados:

- Práticas ambientais básicas (uso de recursos, descarte)
- Política de direitos humanos e boas condições de trabalho
- Programas de diversidade e inclusão
- Relatórios simplificados de sustentabilidade
- Engajamento com a comunidade local
- Indicadores ESG monitorados

8.8 Riscos de Conformidade (incluindo LGPD)

Desafio: Descumprimento de leis trabalhistas, fiscais, regulatórias ou de proteção de dados.

Controles recomendados:

- Política de privacidade e mapeamento de dados
- Consentimento formal e gestão dos dados pessoais

- Medidas de segurança da informação (firewall, criptografia etc.)
- Nomeação de encarregado de dados (DPO), se aplicável
- Treinamento em LGPD
- Procedimentos para atender aos titulares de dados

8.9 Riscos de Tecnologia e Cybersecurity

Desafio: Vazamento de dados, ataques digitais, falhas em sistemas.

Controles recomendados:

- Firewalls e antivírus atualizados
- Autenticação multifator (MFA)
- Backups seguros e criptografados
- Políticas de senha e trocas periódicas
- Treinamento de equipe sobre ciberameaças
- Atualizações constantes de softwares
- Monitoramento de rede e logs de acesso
- Plano de resposta a incidentes
- Testes de penetração periódicos (pentests)

8.10 Benefícios de um modelo SIMPLES GRC

- **Redução de perdas e penalidades**
- **Melhoria da eficiência operacional**
- **Aumento da confiança de stakeholders**

- **Menor exposição a ataques reputacionais**
- **Acesso facilitado a novos mercados e licitações**
- **Reputação positiva junto a clientes e fornecedores**
- **Base sólida para crescimento sustentável**

8.11 Funções práticas da área de GRC e Auditoria em PMEs

A atuação da função de GRC e Auditoria deve ser adaptada à realidade da empresa. Exemplos de atividades recomendadas:

- Compreender os riscos do negócio via workshops e conversas diretas
- Criar matriz de risco inerente e residual
- Associar riscos aos processos e à cadeia de valor
- Elaborar plano de auditoria baseado em riscos críticos
- Assessorar gestores em autoavaliação de risco
- Documentar testes e evidências de controle
- Definir prioridades com base em custo-benefício dos controles
- Monitorar alterações legais e eventos relevantes do setor
- Registrar incidentes e criar planos de remediação
- Promover treinamentos e garantir ciência dos códigos e políticas
- Atuar como ponto focal do GRC junto a sócios, contadores e auditores

O que você precisa lembrar desta seção

- Os riscos são diversos, mas podem ser controlados com ações simples e proporcionais.
- Controles internos não exigem alta complexidade — exigem constância e clareza de propósito.
- Um modelo SIMPLES de GRC bem implementado melhora processos, protege ativos e cria condições reais de crescimento sustentável.
- Mesmo empresas pequenas podem estruturar uma função de GRC com inteligência e foco em resultados.

Conclusão

Por que sua PME não pode mais ignorar o GRC

Ao longo deste guia, demonstramos que **Governança, Gestão de Riscos e Compliance não são temas exclusivos de grandes empresas**. Pelo contrário: em um ambiente regulatório cada vez mais exigente e competitivo, **as PMEs que estruturarem sua gestão com base nesses princípios terão uma vantagem clara e duradoura.**

A proposta aqui não é implantar estruturas complexas ou departamentos dedicados, mas sim **iniciar uma jornada prática, proporcional e estratégica**, com ações simples que geram valor imediato — como prevenir perdas, organizar decisões e fortalecer a reputação da empresa.

Implementar um GRC inteligente significa:

- **Entender os riscos que podem comprometer seu negócio**
- **Criar controles acessíveis e funcionais para reduzir essas exposições**

- **Tomar decisões com base em dados, ética e responsabilidade**
- **Construir uma cultura de integridade e profissionalismo desde já**

Com um modelo SIMPLES de GRC, sua PME pode:

- Reduzir riscos financeiros, jurídicos e operacionais
- Proteger a imagem e a continuidade do negócio
- Atender às expectativas de clientes, parceiros e reguladores
- Estar pronta para crescer com segurança e consistência

Um convite à ação

Se você chegou até aqui, já deu o primeiro passo. Agora, o próximo é aplicar — mesmo que aos poucos — os conceitos apresentados neste guia.

A recomendação é **começar com o básico**: identificar seus riscos mais críticos, definir responsabilidades, mapear os controles existentes e priorizar o que realmente importa. Com o tempo, a estrutura vai se fortalecendo e se adaptando à realidade e ao ritmo da sua empresa.

Lembre-se: **não existe GRC perfeito — existe GRC funcional e coerente com o seu negócio**.

E a MAF pode ajudar

Se você deseja apoio para estruturar ou evoluir o GRC da sua empresa, a MAF está pronta para ajudar.

Atuamos com:

- Diagnóstico de maturidade em GRC para PMEs
- Implantação de políticas e controles essenciais
- Treinamentos práticos e workshops com a equipe
- Apoio em auditoria interna, LGPD, ESG e risco reputacional
- Mentoria para sócios e lideranças na tomada de decisão baseada em riscos

Fale conosco e transforme governança e integridade em diferenciais reais para sua PME.