POLÍTICA DE GESTÃO DE RISCOS, CONTROLES INTERNOS E CONFORMIDADE

Quick Soft Tecnologia da Informação S.A.

---

1. APRESENTAÇÃO E OBJETIVOS

Esta política tem como objetivo estabelecer as diretrizes e responsabilidades para a gestão integrada de riscos, controles internos e conformidade (GRC). A política visa assegurar que a empresa esteja preparada para identificar, avaliar, mitigar e monitorar riscos de forma contínua, garantindo a continuidade dos negócios, a proteção de seus ativos, e a conformidade com as normas legais e regulatórias aplicáveis, alinhando-se ao limite de apetite e tolerância de risco definido pela organização.

1.1. Escopo

Esta política aplica-se a todos os colaboradores, administradores e terceiros envolvidos nas operações da empresa, abrangendo todos os processos de negócio, controle e administrativos. Seu escopo inclui riscos operacionais, estratégicos, financeiros, regulatórios, e de conformidade.

2. DIRETRIZES

2.1. Linhas de Defesa

A empresa adota um modelo de Três Linhas de Defesa para a gestão de riscos:

- **Primeira Linha:** Colaboradores e gestores operacionais são responsáveis pela gestão de riscos no nível dos processos diários, incluindo a identificação, avaliação e mitigação de riscos dentro de suas respectivas áreas de atuação. Eles devem garantir que os controles internos estejam implementados e operando de maneira eficaz.
- **Segunda Linha:** A função de GRC fornece suporte, estabelece políticas, monitora a conformidade e a eficácia dos controles, e oferece orientação às áreas de negócio. Essa linha de defesa é responsável por implementar frameworks de gestão de risco, como a **Matriz de Riscos**, e por garantir que o **limite de apetite e tolerância de Risco** da empresa seja claramente comunicado e seguido.
- **Terceira Linha:** A Auditoria Interna atua de maneira independente, avaliando a eficácia geral do gerenciamento de riscos e controles internos. Ela realiza auditorias periódicas para garantir que os processos estejam em conformidade com as políticas e regulamentos internos e externos.

2.2. Gestão de Riscos

O processo de gestão de riscos na empresa é composto pelas seguintes etapas:

- **Identificação de Riscos**: Utiliza-se uma combinação de métodos, como análise de cenários, mapeamento de processos e *workshops* de risco, para identificar os riscos.
- **Avaliação de Riscos**: Cada risco identificado é analisado em termos de probabilidade e impacto, usando a Matriz de Risco que ajuda a priorizar os riscos mais críticos. Riscos são avaliados tanto em termos de sua exposição inerente quanto residual.
- **Mitigação de Riscos**: Definição de estratégias de resposta a riscos que podem incluir **evitar, mitigar, transferir ou aceitar riscos**, conforme o apetite e tolerância de risco da empresa. As medidas mitigadoras incluem a implementação de controles internos robustos, a contratação de seguros, e o desenvolvimento de planos de contingência.
- **Monitoramento e Revisão de Riscos**: Os riscos e os controles associados são monitorados continuamente para avaliar a sua eficácia ao longo do tempo. Revisões periódicas e auditorias internas garantem que as estratégias de mitigação sejam adaptadas às mudanças no ambiente de negócios ou regulatório.
- **Comunicação e Relatórios**: Relatórios de risco são elaborados periodicamente e apresentados à alta administração, com destaque para quaisquer desvios em relação ao apetite ao risco definido.

2.3. Controles Internos

Os controles internos são fundamentais para assegurar a eficácia operacional, a confiabilidade das informações financeiras, e a conformidade com as normas. A abordagem para os controles internos inclui:

Para informações complementares, acesse o Manifesto da Administração e o Glossário de Termos.

- **Implementação e Manutenção**: Cada área funcional é responsável pela implementação dos controles internos, com suporte da área de GRC.
- **Avaliação e Monitoramento**: Avaliações periódicas da eficácia dos controles internos são realizadas por meio de auditorias e autoavaliações (*self-assessments*). Qualquer falha ou ineficiência identificada deve ser corrigida prontamente.
- **Melhoria Contínua**: A empresa está comprometida com a melhoria contínua dos controles internos, utilizando *feedback* das auditorias e avaliações para aprimorar processos e garantir que os controles estejam alinhados com as melhores práticas de mercado.

3. RESPONSABILIDADES

As responsabilidades na gestão de riscos, controles internos e conformidade são distribuídas entre diferentes níveis da organização. A tabela a seguir detalha essas responsabilidades:

Nível/Posição	Responsabilidades
Conselho de Administração ("CA")	- Define o limite de **Apetite e Tolerância a Risco** e aprova a política de gestão de riscos.
	- Aprova a aceitação de riscos "Extremos" ou fora dos parâmetros normais de apetite ao risco.
	- Supervisiona o sistema de governança e as práticas de GRC, sugerindo melhorias.
Diretoria Executiva	- Implementa as estratégias e diretrizes aprovadas pelo Conselho de Administração.
	- Monitora e gerencia os riscos operacionais, financeiros e regulatórios.
	- Realiza treinamento contínuo em GRC para todos e assegura o cumprimento das políticas.
Área de GRC	- Identifica, avalia e gerencia os riscos em todos os níveis da organização.
	- Mantém o *framework* de gestão de riscos, incluindo o gerenciamento e controle do **Apetite e Tolerância ao Risco** e a **Matriz de Riscos**.
	- Submente os relatórios de riscos e conformidade à Diretoria Executiva e ao CA.
	- Coordena as atividades de auditoria e responde a investigações sobre falhas de controle.
Gestores de Área	- Garantem que os riscos em suas áreas sejam identificados, avaliados e mitigados.
	- Asseguram que os controles internos necessários estejam implementados e operacionais.
	- Reportam riscos e problemas de conformidade à Diretoria de Riscos e Compliance.
Auditoria Interna	- Realiza avaliações independentes da eficácia do sistema de GRC.
	- Avalia a eficácia dos sistemas de controle de riscos e conformidade.
	- Reporta **diretamente ao CA** sobre as descobertas e recomendações.

4. TRATAMENTO E ACEITAÇÃO DE RISCOS

O processo de aceitação de riscos é determinado de acordo com a criticidade e o nível de apetite ao risco, seguindo a tabela abaixo:

Classificação	Proposta de Aceitação	Alçada de Aceitação	Informados
Extremo	Diretoria Executiva	Conselho de Administração	Diretoria Operacional + Área de GRC
Alto			
Moderado	Diretoria Operacional	Diretoria Executiva	Diretoria Executiva
Baixo	Gerentes	Diretoria Operacional	Diretoria Executiva

Para informações complementares, acesse o Manifesto da Administração e o Glossário de Termos.

5. CONTROLE DOCUMENTAL

Esta política entra em vigor imediatamente após a sua aprovação pelo Conselho de Administração e será revisada periodicamente para garantir sua adequação às mudanças no ambiente de negócios e regulatório. Revisões podem ser realizadas sempre que necessário para refletir mudanças nas práticas de GRC, no apetite ao risco ou em outras políticas corporativas relevantes.

Responsável	Controle de Revisões	
CEO	Versão Atual	1.0
	Data da Aprovação	16/10/2024
	Versão Anterior	-
	Ata de Aprovação	Conselho de Administração

Principais Modificações	Legislações e Documentos Relacionados
- Criação da política	- Resolução 304/2023 BCB

Para informações complementares, acesse o Manifesto da Administração e o Glossário de Termos.