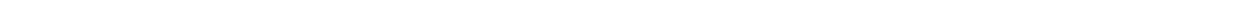




POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS



1. OBJETIVO

A presente Política de Gestão de Riscos é parte integrante do Sistema de Gestão de Riscos e Controles Internos da Concórdia, o qual consiste em um conjunto de instrumentos de governança e de gestão que suportam a concepção, implantação, monitoramento e melhoria contínua da gestão de riscos e dos controles internos, sendo um pilar do Programa de Compliance da Concórdia.

2. PRINCÍPIOS

- a) Integrada:** A gestão de riscos é parte integrante de todas as atividades organizacionais.
- b) Estruturada e abrangente:** Uma abordagem estruturada e abrangente para a gestão de riscos contribui para resultados consistentes e comparáveis.
- c) Personalizada:** A estrutura e o processo de gestão de riscos são personalizados e proporcionais aos contextos externos e internos da organização relacionados aos seus objetivos.
- d) Inclusiva:** O envolvimento apropriado e oportuno das partes interessadas possibilita que seus conhecimentos, pontos de vista e percepções sejam considerados. Isto resulta em melhor conscientização e gestão de riscos fundamentada.
- e) Dinâmica:** Riscos podem emergir, mudar ou desaparecer à medida que os contextos externos e internos de uma organização mudem. A gestão de riscos antecipa, detecta, reconhece e responde a estas mudanças e eventos de uma maneira apropriada e oportuna.
- f) Melhor informação disponível:** As entradas para a gestão de riscos são baseadas em informações históricas e atuais, bem como em expectativas futuras. A gestão de riscos explicitamente leva em consideração quaisquer limitações e incertezas associadas a estas informações e expectativas. Convém que a informação seja oportuna, clara e disponível para as partes interessadas pertinentes.
- g) Fatores humanos e culturais:** O comportamento humano e a cultura influenciam significativamente todos os aspectos da gestão de riscos em cada nível e estágio.
- h) Melhoria contínua:** A gestão de riscos é melhorada continuamente por meio do aprendizado e experiências.

3. RESPONSABILIDADES

Agentes de Riscos: auxilia o Responsável pela Gestão de Riscos no processo de identificação e avaliação dos riscos relacionados à sua área de atuação, terão o papel de facilitadores desse processo, promovendo e acompanhando de todas as fases definidas nesta Política.

Comitê de Compliance e Gestão de Riscos: órgão de assessoramento vinculado diretamente ao CEO, tendo como algumas de suas atribuições o acompanhamento, análise, avaliação dos riscos, monitoramento, assessoria, orientação e reporte ao Comitê Consultivo sobre assuntos relacionados ao gerenciamento de riscos; avaliação do nível de exposição a risco aceitável pela EMPRESA, os quais ela está preparada e disposta a assumir em busca dos objetivos estratégicos.

Facilitadores: colaborador operacional designado pelo Agente de Risco para apoiá-lo do mapeamento e gerenciamento dos riscos da área.

Gestor de Riscos: responsável por conduzir as etapas de identificação, avaliação, priorização e ações futuras. Também realizará o monitoramento e reportará periodicamente às instâncias superiores, a

fim de promover o conhecimento sobre o andamento dos trabalhos por ele conduzidos, assim como o acompanhamento da evolução atrelada aos riscos identificados. Todas as etapas mencionadas serão realizadas em conjunto com os Agentes de Riscos e em conformidade com os requisitos das legislações e resoluções normativas vigentes.

Gestores: responsáveis por dar suporte ao Responsável pela Gestão de Riscos no que tange ao acompanhamento junto as áreas, acompanhar os trabalhos desenvolvidos pelos Agentes de Risco.

4. CONCEITOS, TRATAMENTO E ETAPAS DE GESTÃO DE RISCOS

4.1. Conceito de Risco: Segundo o IBGC-Instituto Brasileiro de Governança Corporativa, o termo risco é proveniente da palavra *risicu* ou *riscu*, em latim, que significa ousar. Costuma-se entender “risco” como probabilidade de “algo não dar certo”, mas seu conceito atual envolve a quantificação e qualificação da incerteza, tanto no que diz respeito às “perdas” como aos “ganhos”, com relação ao rumo dos acontecimentos planejados, seja por indivíduos, seja por organizações.

4.2. Conceito de Gestão de Riscos: Gestão de Riscos é a disciplina destinada a identificar e mensurar os riscos a que estamos expostos e definir qual a estratégia para lidar com os mesmos. Fazemos isso o tempo todo em nossas vidas profissional e pessoal.

4.3. Níveis de Riscos: A combinação entre impacto e probabilidade de um determinado evento permite a identificação do nível natural do risco analisado:

4.3.1. Risco Inerente: É o nível de risco ao qual se estaria exposto caso não houvesse nenhum controle implantado.

4.3.2. Risco Residual: O nível de risco existente considerando os controles aplicados.

4.3.3. Risco Alvo ou Desejável: O nível de risco resultado futuro das ações implementadas.

4.4. Etapas do Processos de Gestão de Riscos: São fases do gerenciamento de riscos:

4.4.1. Estabelecimento do Contexto: Envolve o entendimento da organização, dos objetivos e do ambiente, inclusive do controle interno.

4.4.2. Identificação do Risco: Etapa de busca, reconhecimento e descrição dos riscos, tendo por base o contexto estabelecido.

4.4.3. Análise dos Riscos: Processo de compreender a natureza e determinar o nível do risco, de modo a subsidiar a avaliação e o tratamento de riscos.

4.4.4. Avaliação dos Riscos: Auxilia na tomada de decisões, determinando se o risco é aceitável ou tolerável ou se algum tratamento é exigido.

4.4.5. Tratamento dos Riscos: Envolve a seleção de uma ou mais opções para modificar o nível de cada risco e a elaboração de planos de tratamento e a definição de novos controles ou seu aperfeiçoamento.

5. PRINCIPAIS TIPOS DE RISCOS

Risco de Crédito: Medida de incerteza relacionada à probabilidade da contraparte de uma operação, ou de um emissor de dívida, não honrar, total ou parcialmente, seus compromissos financeiros.

Risco de Imagem e Reputação: Está ligado a problemas e danos relacionados à imagem e a marca de uma empresa, a probabilidade da Concórdia sofrer perdas financeiras, em consequência de algumas práticas internas, eventos de risco, e fatores externos que impactam negativamente a sua imagem perante o mercado.

Risco de Integridade: Que configurem ações ou omissões que possam favorecer a ocorrência de fraudes ou atos de corrupção.

Risco de Mercado: Medida de incerteza relacionada aos retornos esperados de seus ativos e passivos, em decorrência de variações em fatores como taxas de juros, taxas de câmbio, índices de inflação, preços de imóveis e cotações de ações, ou seja, o comportamento verificado no preço de um bem dia a dia.

Risco de Segurança da Informação: São riscos de falhas e vulnerabilidades que podem expor dados e informações da empresa e seus clientes.

Risco Estratégico: Definido como a estimativa das perdas diretas ou indiretas resultantes de falha, deficiência ou inadequação de processos relacionados aos objetivos de alto nível, assim entendidos, os que dão suporte e estejam alinhados à missão institucional. São riscos abrangentes que afetam os objetivos estratégicos de forma sistêmica e podem eventualmente ameaçar a perenidade da companhia.

Risco Legal: Medida de incerteza relacionada aos retornos da Concórdia por falta de um completo embasamento legal de suas operações. Envolve o não cumprimento de leis, regras, regulamentações, acordos, práticas vigentes ou padrões éticos aplicáveis, considerando, inclusive, o risco de que a natureza do produto/serviço prestado possa tornar a instituição particularmente vulnerável a litígios.

Risco Operacional: Compreendem os demais riscos enfrentados pela Concórdia, relacionados aos procedimentos internos, tais como risco de perda resultante de inadequações ou falhas em processos internos, pessoas e sistemas, ou seja, é qualquer possibilidade de perda originada por falhas na estrutura organizacional, seja ela oriunda de sistemas, procedimentos, recursos humanos ou tecnológicos ou pela perda dos valores éticos e corporativos que unem os diferentes elementos.

Risco Socioambiental: Risco relacionado com a possibilidade de ocorrência de perdas resultantes de ações desenvolvidas pela companhia, ou por seus fornecedores e prestadores de serviços, que possam gerar impactos para sociedade e/ou meio ambiente.

Riscos de Compliance: Caracterizado pela probabilidade de ocorrência e pelas consequências do não cumprimento com as obrigações de compliance da Concórdia, é a exposição a penalidades legais, perdas financeiras e de reputação que a empresa pode enfrentar, caso não atue dentro da lei, das regras que delimitam a atuação do seu setor, bem como regras e norma internas.

Sugestão: Riscos de Saúde e Segurança: Situação que apresente risco de dano à saúde do trabalhador caracteriza um risco ocupacional, estão associados iluminação inadequada, ergonomia no ambiente de trabalho, dentre outras possibilidades.

6. PRINCIPAIS PROCESSOS

- ✓ **Desenvolvimento de Produtos:** Envolve em pesquisa, projeto e desenvolvimento de novos produtos;
- ✓ **Gestão de Fornecedores e Matérias-Primas:** Importante gerenciar fornecedores de matérias-primas, componentes eletrônicos para a produção dos produtos;
- ✓ **Compra de Estoque:** O processo de compra de estoque é o primeiro passo, onde adquire os produtos que serão produzidos;
- ✓ **Produção e Fabricação:** Com base nos projetos desenvolvidos, inicia o processo de produção e fabricação dos produtos;
- ✓ **Controle de Qualidade:** Antes de disponibilizar a venda é essencial realizar controles de qualidade;
- ✓ **Gestão de Estoque:** Após a produção/recebimento de novos produtos é realizado a gestão de estoque, que desenvolve categorização, registros de entradas e saídas, monitoramento e identificação de produtos;

- ✓ **Marketing:** Enquanto os produtos estão disponíveis para a venda inclui também campanhas publicitárias e ações do setor do marketing;
- ✓ **Gestão de Vendas e Atendimento ao Cliente:** Quando os produtos estão disponíveis para a venda, é realizado o gerenciamento de vendas, incluindo processo de venda, atendimento ao cliente, processamento de pedidos, emissão de notas fiscais e entrega do produto;
- ✓ **Suporte Técnico, Pós-Venda e SAC:** É oferecido suporte técnico, auxiliando-os na configuração dos produtos, fornecendo assistência técnica, solucionando problemas e oferecendo garantia pós-venda;
- ✓ **Gestão de Finanças e Contabilidade:** Durante todo o processo é feita uma gestão financeira e contábil;
- ✓ **Logística e Distribuição:** Gerenciamento de logística e distribuição é importante no processo, garantindo que sejam armazenados adequadamente, embalados com segurança e entregues ao cliente dentro do prazo;
- ✓ **Gestão de Recursos Humanos:** É importante gerenciar a equipe, incluindo recrutamento, seleção, treinamentos, avaliação e desempenho da equipe;
- ✓ **Setor Jurídico:** Além disso, o setor jurídico é responsável por questões legais, contratos, conformidade, resolução de disputas legais e assessoria jurídica em questão relacionadas ao negócio;

7. PROBABILIDADE DO RISCO

É a chance que a falha tem de acontecer ou que aconteceu no período analisado, definida de acordo com monitoramento do risco.

A probabilidade é definida conforme tabela abaixo:

ESCALA DE PROBABILIDADES		
Magnitude	Descrição	
Muito baixa	Evento Improvável de ocorrer: Excepcionalmente poderá até ocorrer, porém não há elementos ou informações que indiquem essa possibilidade.	1
Baixa	Evento raro de ocorrer: O evento poderá ocorrer de forma inesperada, havendo poucos elementos ou informações que indicam essa possibilidade.	2
Média	Evento possível de ocorrer: Há elementos e/ou informações que indicam moderadamente essa possibilidade.	3
Alta	Evento possível de ocorrer: É esperado que o evento ocorra, pois os elementos e as informações disponíveis indicam de forma consistente essa possibilidade.	4
Muito alta	Evento praticamente certo de ocorrer: Inequivocamente e o evento ocorrerá, pois os elementos e informações disponíveis indicam claramente essa possibilidade.	5

8. IMPACTO DO RISCO

É o impacto no negócio caso houver a ocorrência do risco no período analisado, definido de acordo com monitoramento do risco.

O impacto é definido conforme tabela abaixo:

ESCALA DE IMPACTOS		
Magnitude	Descrição	
Muito baixa	Degradação de operações ou atividades de processos, projetos ou programas da organização, porém causam impactos mínimos nos objetivos de prazo, custo, qualidade, escopo, imagem ou relacionados ao atendimento de metas, padrões ou à capacidade de entrega de produtos/serviços às partes interessadas (clientes internos/externos, beneficiários)	1

Baixa	Degradação de operações ou atividades de processos, projetos ou programas da organização, causando impactos pequenos nos objetivos	2
Média	Interrupção de operações ou atividades de processos, projetos ou programas, causando impactos significativos nos objetivos, porém recuperáveis.	3
Alta	Interrupção de operações ou atividades de processos, projetos ou programas, causando impactos de reversão muito difícil nos objetivos.	4
Muito alta	Paralisação de operações ou atividades de processos, projetos ou programas, causando impactos irreversíveis/catastróficos nos objetivos.	5

9. NÍVEIS DE RISCO E TRATAMENTO AO RISCO

NÍVEIS DE RISCO TRATAMENTO AO RISCO		
Nível do Risco	Descrição	Resposta ao Risco
Baixo (1 a 8)	Risco Aceitável: pode expor a empresa a danos de menor relevância, no entanto, não deve dificultar o alcance dos objetivos do processo.	Aceitar: Nenhuma medida é adotada para afetar a probabilidade.
Médio (9 a 16)	Risco Tolerável: pode expor a empresa a danos graves, o que dificultaria o alcance dos objetivos do processo.	Mitigar: Medidas para reduzir a probabilidade dos riscos.
Extremo (17 a 25)	Risco Inaceitável: expõe a empresa a danos severos com impactos de difícil correção, impossibilitando o alcance dos objetivos estratégicos.	Evitar: Descontinuação das atividades que geram os riscos.

10. ALÇADAS PARA DELIBERAÇÃO

RISCO RESIDUAL			
	Baixo	Médio	Extremo
Alçadas	Gestores	Comitê	Comitê e CEO

11. ETAPAS DO PROCESSO DE GESTÃO DE RISCOS

A identificação de riscos visa determinar os riscos que podem afetar a EMPRESA, bem como, documentar suas características. Isto significa que, a partir da identificação, cada risco deve ser descrito formalmente.

Os participantes das atividades de identificação de riscos podem incluir: gestores, membros de equipe, equipe de gerenciamento de riscos, especialistas no assunto, clientes, usuários finais, partes interessadas e especialistas no assunto.

1. O processo de gerenciamento de riscos e controles internos, segue a lógica dos padrões internacionais, possuindo as seguintes etapas:

1.1. Comunicação e consulta:

Nesta fase, é crucial estabelecer canais de comunicação eficazes entre todas as partes interessada. Isso garante que todos tenham acesso às informações necessárias e possam contribuir com suas perspectivas e experiências na identificação e avaliação dos riscos.

1.2. Estabelecimento do contexto:

O contexto organizacional abrange todos os fatores internos e externos que podem influenciar a capacidade da organização de alcançar seus objetivos. Compreender esse contexto é fundamental para identificar e priorizar os riscos mais relevantes e alinhá-los com a estratégia da empresa.

1.3. Identificação dos riscos inerentes:

Durante essa etapa, é necessário identificar e catalogar todos os possíveis riscos que podem afetar, desde riscos operacionais até riscos estratégicos e de conformidade, dando ênfase nas conformidades legais. Isso envolve uma análise minuciosa.

1.4. Análise dos Riscos:

Após a identificação dos riscos, é crucial realizar uma análise detalhada para compreender a probabilidade de ocorrência e o impacto potencial de cada risco. Foram feitas através de técnicas qualitativas e quantitativas, permitindo uma priorização adequadas dos riscos com base em sua gravidade.

1.5. Avaliação dos riscos:

Nesta fase, os riscos são avaliados de acordo com critérios predefinidos, levando em consideração sua probabilidade e impacto, bem como a capacidade da empresa de lidar com eles. Isso resulta na classificação dos riscos em categorias como **baixo, médio e extremo**, ajudando na priorização das ações de tratamento.

1.6. Tratamento dos riscos:

Uma vez avaliados, os riscos são tratados através da implementação de medidas de mitigação, aceitação ou prevenção. O objetivo é reduzir a probabilidade de ocorrências ou minimizar seu impacto.

1.7. Monitoramento e análise crítica:

Após o tratamento dos riscos, é essencial monitorar continuamente sua eficácia e a evolução do ambiente de riscos ao longo do tempo. Algumas ferramentas devem ser utilizadas para o monitoramento de riscos:

- a) **Análise de documentos:** consiste na revisão e análise de documentos. Isso ajuda a identificar informações cruciais relacionadas aos riscos organizacionais.
- b) **Entrevistas estruturadas:** são entrevistas planejadas e conduzidas de forma sistemáticas com partes interessadas para obter informações sobre os riscos.
- c) **Matriz de riscos inerentes e residuais:** a matriz de risco inerentes avalia probabilidade e impactos dos riscos antes da implementação de medida de tratamento. Já a matriz residual avalia os riscos remanescentes após a implementação.
- d) **Brainstorming:** é uma técnica de geração de ideias em grupos, essa abordagem colaborativa ajuda a explorar diferentes perspectivas e a enriquecer o processo de gestão de riscos.

1.8. Reporte dos riscos aos órgãos de governança, com periodicidade mínima anual, destacando, no mínimo:

- 1.8.1.** Informações atualizadas sobre os riscos classificados como Médio e Extremo;
- 1.8.2.** Novos riscos avaliados ou riscos reavaliados no período;
- 1.8.3.** Status dos trabalhos planejados;
- 1.8.4.** Planos de ação para tratamento dos riscos.