POLÍTICA DE GESTÃO DE RISCOS CORPORATIVOS DA CAGECE

1. APRESENTAÇÃO

A Política de Gestão de Riscos Corporativos da Cagece tem por finalidade fornecer diretrizes para identificação e gerenciamento dos riscos de natureza estratégica, operacional, financeira e legal que possam vir a impactar em suas estratégias.

2. FUNDAMENTAÇÃO LEGAL

O processo de gestão de riscos corporativos da Cagece segue metodologia própria e tem como base o modelo internacional COSO ERM: *Committee of Sponsoring Organizations of the Treadway Commission – Enterprise Risk Management*, e as normas ABNT NBR ISO 31000:2018 e ABNT ISO GUIA 73:2009.

3. PRINCÍPIOS E DIRETRIZES

3.1. A estratégia empresarial e os processos de negócio devem considerar a gestão de seus riscos;

3.2 A prática de Gestão de Riscos deve estar alinhada com a Missão, Visão e Valores da Companhia;

3.3 A Gestão de Riscos deve ser realizada de forma sistemática nos processos organizacionais conforme padrão estabelecido pela Cagece, seguindo metodologia adotada e definida no Manual de Gestão de Riscos da Cagece.

3.4 Os riscos dos processos devem ser identificados, avaliados, tratados, comunicados e monitorados com o objetivo de mitigar o impacto às estratégias da Companhia e o cumprimento de seus objetivos.

3.5 Todos os envolvidos no processo de Gestão de Riscos Corporativos da Cagece devem estar capacitados na metodologia aplicada na Cagece;

3.6 Os riscos identificados devem ser classificados de acordo com as categorias e subcategorias apresentadas no Anexo I desta política.

3.7 O processo de gestão de riscos deve ser monitorado por indicadores de desempenho;

3.8 O nível de criticidade dos riscos deve ser avaliado e definido de acordo com o nível do risco residual;

3.9 A Gerência de Governança, Riscos e Conformidade deve promover a ampla discussão com as áreas para o desenvolvimento do processo de gestão de riscos;

3.10 A elaboração dos planos de resposta ao risco devem ser subsidiados pelos resultados das avaliações do nível do risco residual;

3.11 A gestão de riscos corporativos deve ocorrer por ciclos de avaliações e revisões frequentes ou em resposta a um fato específico, favorecendo a melhoria contínua e o fortalecimento das diretrizes estratégicas empresariais;

4. OBJETIVOS

4.1 Estabelecer princípios, diretrizes e competências a serem observadas no processo de gestão de riscos corporativos, de forma a assegurar a identificação, avaliação, priorização, tratamento, monitoramento e comunicação dos riscos do negócio com o propósito de contribuir para a sustentabilidade da Companhia e apoiar os processos decisórios;

4.2 Promover e disseminar uma cultura de conformidade e atuação proativa a fim de ampliar a capacidade da rede de governança;

4.3 Aperfeiçoar procedimentos e práticas de gestão de riscos corporativos em todos os níveis hierárquicos da organização com intuito de mitigar os riscos e apoiar o alcance dos objetivos estratégicos;

4.4 Promover uma linguagem comum e difundir o conhecimento de gestão de riscos corporativos.

5. CONCEITOS

O processo de gestão de riscos corporativos compreende as atividades de identificação, avaliação, resposta, comunicação e monitoramento dos eventos de riscos internos, capazes de afetar o alcance dos objetivos da Cagece. Abaixo relacionamos os conceitos e abreviações tratadas nesta política:

ABNT – Associação Brasileira de Normas Técnicas

AGR – Análise Geral de Risco

APETITE AO RISCO – A quantidade total de riscos que uma companhia ou outra organização está disposta a aceitar na busca de sua missão (ou visão) [COSO® ERM]. O apetite ao risco reflete a filosofia de gerenciamento de riscos da companhia. Quantidade e tipos de riscos que uma organização está preparada para buscar, reter, assumir ou afastar. [ABNT ISO GUIA 73:2009, definição 3.7.1.2]

AVALIAÇÃO DE RISCO – Processo de avaliação que permite que uma organização considere até que ponto os fatores de riscos em potencial podem impactar a realização dos objetivos. Os eventos são avaliados com base em duas perspectivas: probabilidade e impacto.

COSO® ERM – *Committee of Sponsoring Organizations of the Treadway Commission Enterprise Risk Management*

CONTROLE INTERNO – Processo efetuado pelo conselho, administração ou qualquer outro funcionário de uma empresa, desenhado para fornecer garantia razoável em relação à realização dos objetivos nas seguintes categorias: Eficácia e eficiência das operações, Confiabilidade dos relatórios financeiros, Conformidade com leis e regulamentos aplicáveis. [COSO® ERM].

DICIONÁRIO DE RISCOS CORPORATIVOS – Portfólio de riscos baseado em eventos que possam criar, aumentar, evitar, reduzir ou acelerar ou atrasar a realização dos objetivos (Anexo II).

GESTÃO DE RISCOS – Atividades coordenadas para dirigir e controlar uma organização no que se refere a riscos. [ABNT ISO GUIA 73:2009, definição 2.1]

GESTÃO DE RISCOS CORPORATIVOS – Processo de avaliação que permite que uma organização considere até que ponto os fatores de riscos em potencial podem impactar na realização dos objetivos.

GOVERNANÇA CORPORATIVA – Conforme definido pelo Instituto Brasileiro de Governança Corporativa (IBGC), governança corporativa é o sistema pelo qual as organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre proprietários, conselho de administração, diretoria e órgãos de controle.

GRAU DE EXPOSIÇÃO – Grau em que uma organização ou parte interessada está sujeita a um evento. [ABNT ISO GUIA 73:2009, DEFINIÇÃO 3.5.1.5]

GRC – Gestão de Governança, Riscos e Conformidade.

GRC-RCP – Coordenadoria de Gestão de Riscos, Controles Internos e Processos

IBGC – Instituto Brasileiro de Governança Corporativa

ISO – *International Organization for Standardization*

IDENTIFICAÇÃO DE RISCOS – Processo de busca, reconhecimento e descrição de riscos. [ABNT ISO GUIA 73:2009, definição 3.5.1] A identificação de riscos envolve a descrição de fatores e consequências. Pode envolver dados históricos, análises teóricas, opiniões de pessoas especialistas e as necessidades das partes interessadas.

IMPACTO - Resultado ou efeito de um evento de risco. Poderá haver uma série de impactos possíveis associados a um único evento. O impacto pode ser positivo ou negativo em relação ao alcance dos objetivos

KRI – *Key Risk Indicator*

MAPA DE RISCO – Representação gráfica referente ao processo de avaliação de riscos no ambiente corporativo apresentado no layout de Mapa 5 x 5, através de posicionamento do nível de risco em quadrante com cor correspondente representado no plano cartesiano por partes ordenadas (probabilidade e impacto)

PROBABILIDADE – Chance de um evento acontecer. Na terminologia de gestão de riscos, a palavra “probabilidade” é utilizada para referir-se à chance de algo acontecer, não importando se definida, medida ou determinada, ainda que objetiva ou subjetivamente, qualitativa ou quantitativamente, e se descrita utilizando-se termos gerais ou matemáticos (como probabilidade ou frequência durante um
determinado período de tempo).
Fonte: ISO 31000: 2018

PROPRIETÁRIO DO RISCO – Pessoa ou entidade com a responsabilidade e a autoridade para gerenciar um risco. [ABNT ISO GUIA 73:2009, definição 3.5.1.5]

RISCO – Conforme definido no COSO® ERM, risco é a possibilidade de ocorrência de um evento, oriunda de fontes internas ou externas, capaz de afetar adversamente o atendimento dos objetivos da companhia. É o efeito da incerteza nos objetivos. [ABNT ISO GUIA 73:2009, definição 1.1]

RISCO DE NEGÓCIO – Exposição aos impactos, resultantes de decisões ou eventos, internos ou externos, de natureza estratégica, operacional, financeira, legal e outras decorrentes da maneira pela qual a organização busca atingir os seus objetivos.

TOLERÂNCIA AO RISCO – A variação aceitável relativa à realização de um objetivo [COSO® ERM]. Disposição da organização ou parte interessada em suportar o risco após o tratamento do risco, a fim de atingir os seus objetivos. [ABNT ISO GUIA 73:2009, definição 3.7.1.3]

6. CARACTERÍSTICAS

6.1. A gestão de riscos corporativos deve ocorrer nos processos e subprocessos da Companhia, com o uso de linguagem comum e padrões estabelecidos na política e manual de Gestão de Riscos da Cagece;

6.2. As competências do Conselho de Administração, Diretoria Executiva, Comitê de Gestão de Riscos Corporativos, gestores de negócio e Coordenadoria de Gestão de Riscos, Controles Internos e Processos, estão definidas no Anexo I desta política;

6.3. Os limites de tolerância são definidos com base na variação aceitável do apetite ao risco, definidos com base na filosofia de riscos adotada pela Diretoria Executiva e Conselho de Administração. Tais limites são definidos pela Diretoria Executiva e Conselho de Administração e balizam a classificação da avaliação dos riscos e processos nas dimensões “impacto” e “probabilidade”.

Tabela 1 - Critérios para avaliação da probabilidade

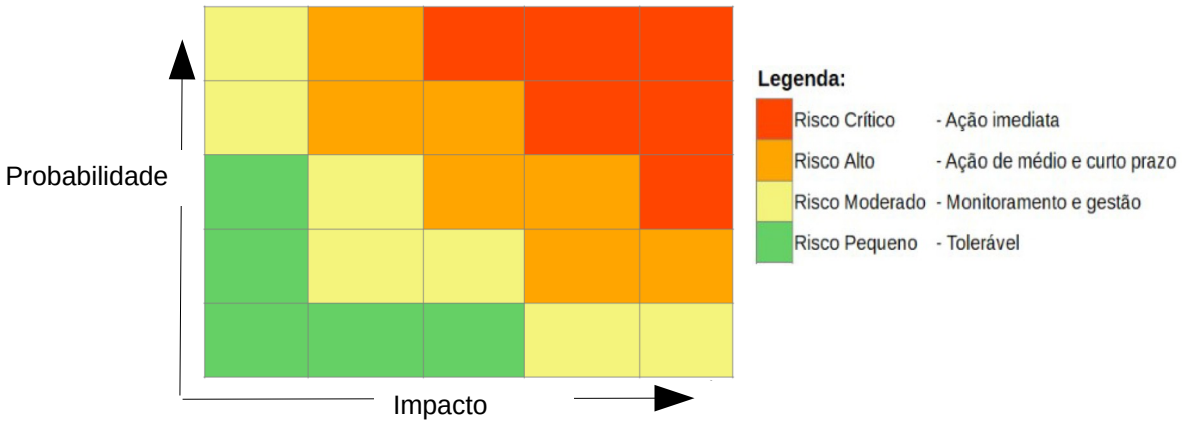
Probabilidade						
Fator de análise					Grau de exposição	Pontuação
Pessoas	Tecnologia da Informação	Infraestrutura	Processo	Ambiente externo		
Nível muito alto de influência para a materialização do risco					Diário/ Semanal	5 Elevado
Nível alto de influência para a materialização do risco					Quinzenal	4 Muito alto
Nível moderado de influência para a materialização do risco					Mensal	3 Alto
Nível leve de influência para a materialização do risco					Anual	2 Médio
Nível muito leve de influência para a materialização do risco					Eventual	1 Baixo

Tabela 2 - Critérios para avaliação do impacto

Impacto					
Fator de análise	Imagem	Financeiro	Legal	Operacional	Pontuação
Peso	2	4	4	5	
Orientações para análise	De caráter nacional - Brasil	Acima de 2% da receita líquida	Perturbações muito graves	Impacta outros processos muito fortemente	5 Catastrófico
	Regional - Estado	Entre 1% e 2% da receita líquida	Perturbações graves	Impacta outros processos de forma direta	4 Severo
	Local – Região metropolitana	Entre 0,5% e 1% da receita líquida	Perturbações limitadas	Impacta somente o próprio processo consideravelmente	3 Moderado
	De caráter interno – Dentro da organização	Entre 0,1% e 0,5% da receita líquida	Perturbações leves	Impacta somente o próprio processo levemente	2 Leve
	De caráter interno – Dentro da área	Até 0,1% da receita líquida	Perturbações muito leves	Não há impacto	1 Insignificante

6.4 O Mapa de Riscos é graduado em quatro níveis, definidos na matriz, considerando impacto e probabilidade, conforme apresentado na Figura 1:

Figura 1 - Mapa de riscos



7. RESPONSABILIDADES

7.1 A Gestão de Riscos Corporativos na Cagece é realizada pela Gerência de Governança, Riscos e Conformidade – GRC, tendo as ações coordenadas pelo Comitê de Gestão de Riscos Corporativos

7.2 Na Cagece, o Modelo de 3 linhas tem como objetivo indicar como as estruturas e processos se relacionam, auxiliam no atingimento dos objetivos e facilitam o gerenciamento de riscos. As linhas estão assim definidas:

7.2.1 Administração: Conselho de Administração, Diretoria Executiva e Comitê de Auditoria Estatutário.

- Cultiva cultura que promove comportamento ético e de responsabilidade;
- Estabelece estruturas e processos para governança;
- Envolve as partes interessadas para monitorar seus interesses e se comunica de forma transparente sore o atingimento dos objetivos;
- Delega responsabilidades e oferece recursos à gestão para atingir os objetivos da organização;

- Determina o apetite organizacional a riscos e exerce supervisão do gerenciamento de riscos
- Estabelece e supervisiona função de auditoria interna independente, objetiva e competente.

7.2.2 Gestão – Primeira linha: Gerente do processo.

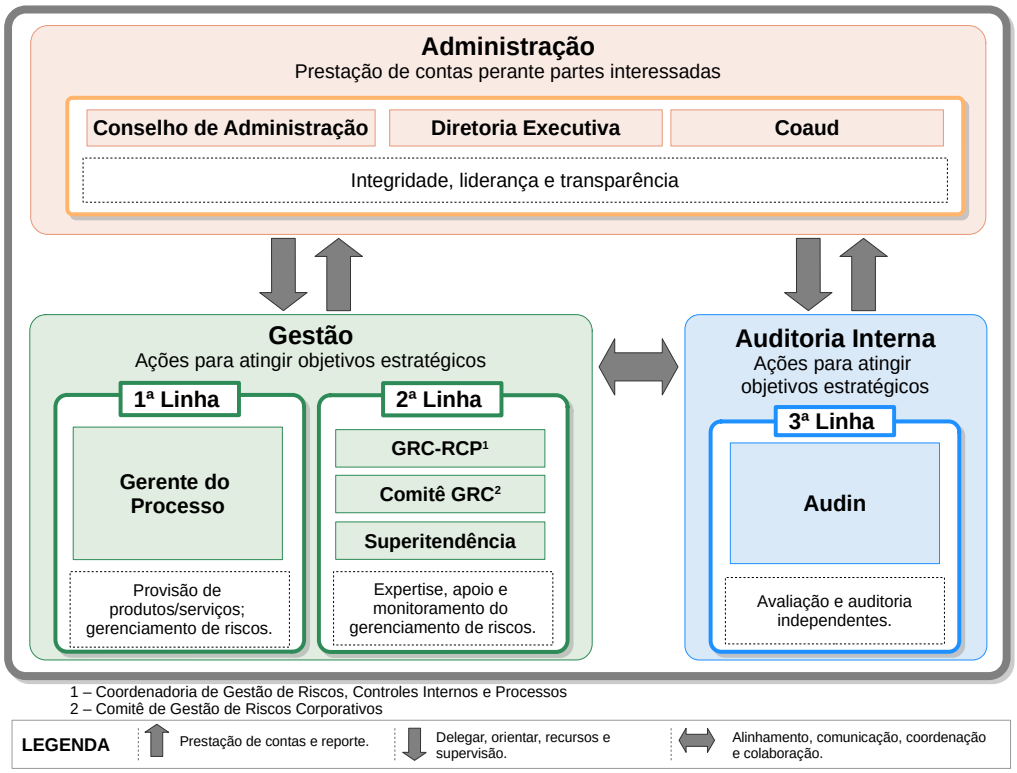
- Lidera, dirige ações e aplica recursos para atingir os objetivos da organização;
- Mantém diálogo contínuo com a Administração para reportar resultados quanto aos objetivos da organização e a riscos;
- Estabelece e mantém estruturas e processos apropriados para o gerenciamento de operações e riscos (incluindo controle interno);
- Garante a conformidade com as expectativas legais, regulatórias e éticas.

7.2.3 Gestão – Segunda linha: Coordenadoria de Riscos, Controles Internos e processos, Comitê de Gestão de Riscos Corporativos e Superintendência.

- Fornece expertise complementar, apoio e monitoramento quanto ao gerenciamento de riscos, incluindo:
  - Desenvolvimento, implantação e melhoria contínua das práticas de gerenciamento de riscos (incluindo controle interno);
  - Atingimento dos objetivos de gerenciamento de riscos.
- Fornece análises e reportes sobre a adequação e eficácia do gerenciamento de riscos.

7.2.4 Auditoria Interna – Terceira linha: Auditoria interna (Audin)

- Mantém prestação de contas primária perante a Administração e a independência das responsabilidades da gestão;
- Comunica avaliação e assessoria independentes e objetivas à Gestão e à Administração sobre a adequação e eficácia do gerenciamento de riscos (incluindo controle interno), para apoiar o atingimento dos objetivos organizacionais e promover e facilitar a melhoria contínua;



7.3 Os riscos corporativos devem ser supervisionados pelo Comitê de Auditoria Estatutário, Conselho Fiscal e de Administração, por meio de Relatórios produzidos pela GRC, de periodicidade anual.

7.4 Aos profissionais da GRC é permitido o acesso a dados, documentos e informações necessários à execução de suas atividades, responsabilizando-se pela confidencialidade das informações.

7.5 As exceções, eventuais disposições e casos omissos a esta política devem ser submetidas à apreciação do Comitê de Gestão de Riscos Corporativos e encaminhados para posterior aprovação do Conselho de Administração.

8. VIGÊNCIA

A presente Política de Gestão de Riscos Corporativos entra em vigor a partir de 27 de julho de 2020, aprovada na 528ª Reunião do Conselho de Administração da Cagece.

9. HISTÓRICO DE ALTERAÇÕES

Versão	Elaborador/Unidade	Revisor/Unidade	Aprovador/ Unidade	Alteração	Data da publicação
01	Gislene Ellery/GRC-RCP	Simone Arrais/GRC		---	
02	Gislene Ellery/GRC-RCP	Michele Aguiar/GRC		Itens: 1, 3, 5, 6.2, 6.7, 6.8, 6.9, 6.12, 6.14, Figura 1, Figura 2, 6.15, Figura	

				3, 6.16, 7, Anexo I, Anexo II.	

10.REFERÊNCIAS

Código de Conduta e Integridade
Lei nº. 13.303/16
ABNT ISO GUIA 31000:2018
ABNT ISO GUIA 73:2009
COSO® ERM

ANEXOS

ANEXO I – MATRIZ DE RESPONSABILIDADES

A matriz a seguir especifica os papéis e responsabilidades no processo de Gestão de Riscos Corporativos na Cagece através da distribuição das seguintes funções:

R – Responsável (Executa a atividade)
A – Aprovador (Aprova a atividade. Responsável primário pelos resultados)
C – Consultado (Consultado sobre a atividade)
I – Informado (Informado sobre a atividade)

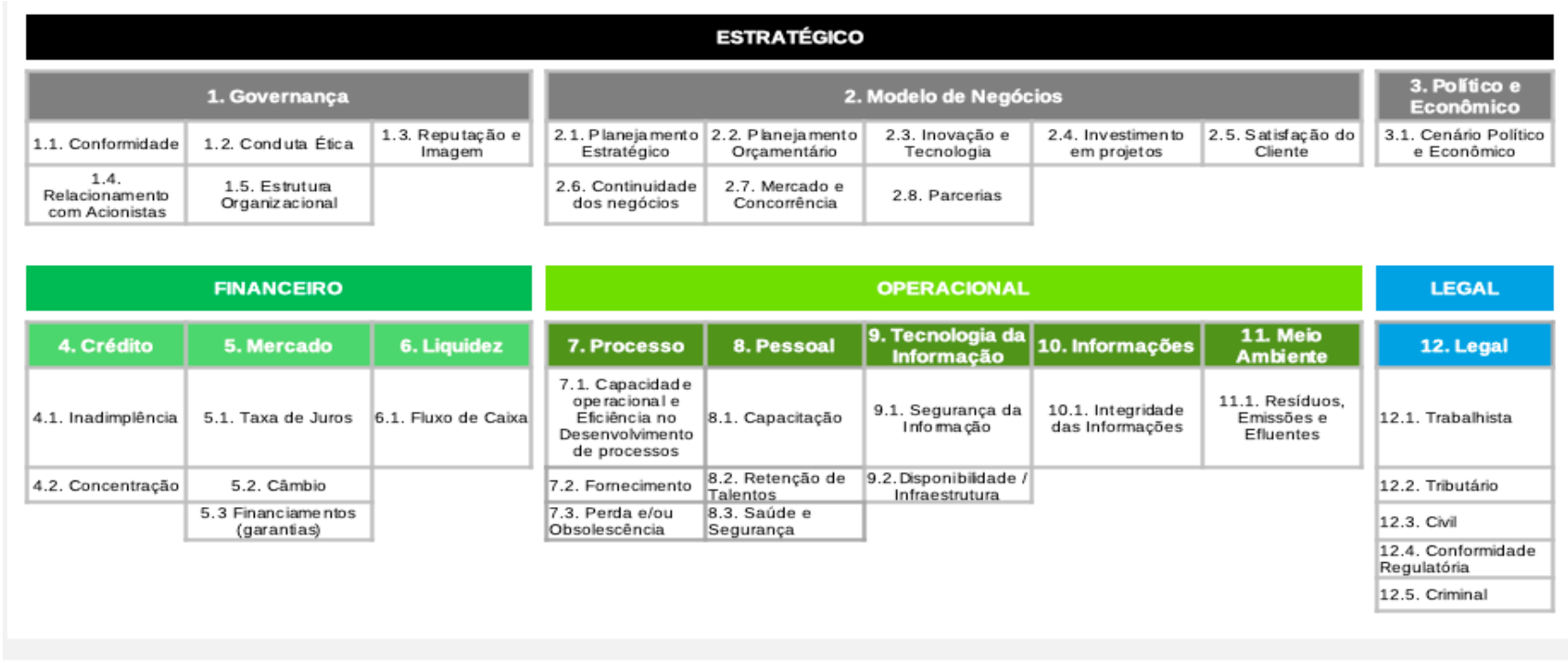
As responsabilidades foram divididas entre os seguintes agentes:

- Coordenadoria de Gestão de Riscos, Controles Internos e Processos
- Gestores das áreas de negócios
- Comitê de Gestão de Riscos Corporativos
- Diretoria Executiva
- Conselho de Administração

Grupo de Atividades	Atividade	Responsável					Observação
		Coord de Riscos e Controles Internos	Gestores de Negócio	Comitê de Gestão de Riscos Corporativos	Diretoria Executiva	Conselho de Adm.	
PLANEJAMENTO	Análise Geral de Riscos	R	C	A	A	A	Os ciclos de Análise Geral de Riscos devem ocorrer, no mínimo, a cada 2 anos, ou a partir de decisão da Diretoria Executiva ou Conselho de Administração.
	Apetite ao risco	R	I	R	A	A	Aprovar o grau de apetite a riscos da Companhia e possíveis alterações.
	Avaliação e priorização dos processos e programação de realização de Gestão de Riscos	C	R	A	A	A	Considerar processos listado no documento de Atribuições da área
	Definição dos indicadores para monitoramento dos riscos prioritários	R	C	A	I	I	Os riscos selecionados como prioritários terão indicadores a serem monitorados periodicamente.
MAPEAMENTO DE RISCOS E PLANO DE RESPOSTAS	Identificação e análise dos riscos.	C	R	A	I		Eventualmente, os diretores podem ser consultados durante a atividade de identificação dos riscos nos processos.
	Monitoramento dos riscos de nível moderado e pequeno	C	R	I	I		
	Definição dos planos de resposta aos riscos com nível alto e crítico.	C	R	A	I		Os planos de resposta aos riscos devem contemplar as ações para redução da probabilidade e/ou mitigação do impacto.
	Implantação dos planos de resposta aos riscos	I	R	I	I		Os Planos de Resposta ao Risco devem ser acompanhados sistematicamente e informado o andamento dos mesmos.
REPORTES PERIÓDICOS	Reporte dos trabalhos e status dos riscos com nível alto ou crítico	R	I	I	I	I	Mensal

Grupo de Atividades	Atividade	Responsável					Observação
		GRC-RCP	Gestores de Negócio	Comitê de Gestão de Riscos Corporativos	Diretoria Executiva	Conselho de Administração	
MONITORAMENTO CONTÍNUO DOS RISCOS	Monitoramento dos planos de resposta aos riscos	C	R	I	I	I	Monitoramento dos planos de resposta ao risco podem ser levados periodicamente à GRC-RCP.
	Monitoramento dos riscos de nível pequeno e moderado	I	R	I	I		O monitoramento dos riscos de nível pequeno e moderado deve ocorrer de forma pontual, através do acompanhamento de eventos de perda ou contingências associadas ao risco.
	Monitoramento dos indicadores riscos de nível alto e crítico	R	R	I	I	I	O monitoramento dos riscos de nível alto e crítico deve ocorrer através de: - Indicadores de risco (KRI) para os riscos prioritários; - Acompanhamento dos planos de resposta aos riscos.
DISCORDÂNCIAS DE OPINIÃO	Deliberação sobre discordâncias na avaliação e/ou sobre o plano de resposta para riscos de nível alto ou crítico	R	C	A	I		A diretoria da área será acionada para eventuais pontos de discordância entre a GRC-RCP e o Comitê de Gestão de Riscos Corporativos sobre a avaliação e/ou sobre o plano de resposta para riscos altos. O Conselho só será acionado para eventuais pontos de discordância entre o Comitê Gestão de Riscos Corporativos e a Diretoria Executiva, sobre a avaliação e/ou sobre o plano de resposta para riscos críticos.
	Aprovação de alterações na política de gestão de riscos	R	I	R	A	A	

ANEXO II – DICIONÁRIO DE RISCOS CORPORATIVOS



ESTRATÉGICO									
1. Governança			2. Modelo de Negócios					3. Político e Econômico
1.1. Conformidade	1.2. Conduta Ética	1.3. Reputação e Imagem	2.1. Planejamento Estratégico	2.2. Planejamento Orçamentário	2.3. Inovação e Tecnologia	2.4. Investimento em projetos	2.5. Satisfação do Cliente	3.1. Cenário Político e Econômico
1.4. Relacionamento com Acionistas	1.5. Estrutura Organizacional		2.6. Continuidade dos negócios	2.7. Mercado e Concorrência	2.8. Parcerias			

FINANCEIRO			OPERACIONAL					LEGAL
4. Crédito	5. Mercado	6. Liquidez	7. Processo	8. Pessoal	9. Tecnologia da Informação	10. Informações	11. Meio Ambiente	12. Legal
4.1. Inadimplência	5.1. Taxa de Juros	6.1. Fluxo de Caixa	7.1. Capacidade operacional e Eficiência no Desenvolvimento de processos	8.1. Capacitação	9.1. Segurança da Informação	10.1. Integridade das Informações	11.1. Resíduos, Emissões e Efluentes	12.1. Trabalhista
4.2. Concentração	5.2. Câmbio		7.2. Fornecimento	8.2. Retenção de Talentos	9.2. Disponibilidade / Infraestrutura			12.2. Tributário
	5.3 Financiamentos (garantias)		7.3. Perda e/ou Obsolescência	8.3. Saúde e Segurança				12.3. Civil
								12.4. Conformidade Regulatória
								12.5. Criminal