Política de Gestão de Riscos

29.04.2022

Revisão: 4
Aprovação: 29/04/2022 - Próxima Revisão: 29/04/2024
POL 10.3.4

POLÍTICA DE GESTÃO DE RISCOS

Sumário

POLÍTICA DE GESTÃO DE RISCOS

1. Objetivo

Estabelecer diretrizes para o desenvolvimento, disseminação e implementação de metodologias de gerenciamento de riscos institucionais, visando apoiar a melhoria contínua de processos de trabalho, projetos e a alocação e utilização eficaz dos recursos disponíveis, além de conduzir e alinhar o apetite à tomada de risco no processo decisório para o cumprimento dos objetivos da Companhia.

Esta Política deve sempre ser interpretada e cumprida em conjunto com o Código de Ética da ATMA Participações S.A.

2. Abrangência

É destinado a todos os colaboradores ATMA Participações S.A e suas Controladas, Fornecedores e Clientes.

3. Regras

I. DONOS DE RISCO

São considerados Donos de Risco, assim entendidos, aqueles que são os titulares responsáveis pelo gerenciamento dos riscos em seus respectivos âmbitos e escopos de atuação, responsáveis por processos de trabalho, projetos e iniciativas estratégicas, táticas e operacionais da Companhia.

O Dono de Risco deve ser colaborador da Companhia que possui cargo de liderança e toda a estrutura hierárquica acima dele é corresponsável por monitorar o risco e assegurar que o plano de ação para tratamento do risco seja implantado ou que o controle opere satisfatoriamente.

Competências do Dono de Risco

- Decidir sobre a escolha dos processos de trabalho que devem ter os riscos gerenciados e tratados com prioridade, à vista da dimensão dos prejuízos e dos impactos que possam causar, sob os aspectos estratégico, orçamentário e de imagem;
- Estabelecer as ações de tratamento ou monitoramento a serem implementados, fixar prazo de implementação e avaliar os resultados obtidos;
- Definir quais riscos deverão ser priorizados para tratamento, por meio de ações de caráter imediato, curto, médio ou longo prazo ou de ações de aperfeiçoamento contínuo, bem como fixar prazo para implementação e avaliação dos resultados obtidos por meio de indicadores.

II. MODELO DAS 3 LINHAS DE DEFESA

1° Linha de Defesa: São os Donos de Riscos e as áreas responsáveis pelos processos de negócio, que devem definir e gerenciar controles que minimizem os riscos da Companhia, bem como realizar o devido monitoramento dos mesmos.

2° Linha de Defesa: São as áreas e profissionais da Companhia que têm como objetivo apoiar a gestão para que cumpram com suas responsabilidades da primeira linha de defesa, fornecendo ferramentas e conhecimentos adequados a cada processo.

3° Linha de Defesa: Avaliação e assessoria independentes e objetivas sobre questões relativas ao atingimento dos objetivos estratégicos da organização, realizando prestação de contas perante o Comitê de Auditoria.

III. APETITE A RISCO

Riscos classificados como “Alto” e “Muito Alto” devem possuir um plano de ação para tratamento.

Os riscos cujo investimento para o seu respectivo tratamento sejam maiores do que o impacto da sua materialização podem ser assumidos pela gerência responsável, desde que não ocasionem prejuízos de imagem ou descumprimento normativo.

IV. CATEGORIAS DE RISCO

Riscos Externos

São os riscos decorrentes de perdas e mudanças verificadas nas condições políticas, culturais, sociais, econômicas ou financeiras do Brasil, ou riscos de mercado, como pressão por alteração nos preços e custos de insumos.

Riscos de *Compliance* (Legal ou Regulatório)

Eventos derivados de falhas no cumprimento de aplicação de leis, acordos, regulamentos e das políticas da Companhia. Ou ainda alterações legislativas ou normativas não previstas e que podem comprometer as atividades da Companhia.

Riscos Operacionais

São os riscos geralmente isolados em um departamento ou processo, mas que podem impactar a operação da empresa, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas.

Riscos de Imagem

Eventos que podem comprometer a confiança das partes interessadas em relação à capacidade da Companhia em cumprir com seus compromissos, princípios, conceitos e valores, e de atuar com ética, integridade e transparência.

Riscos Financeiros

Eventos que podem comprometer a capacidade da Companhia de contar com os recursos financeiros necessários à realização de suas atividades e gestão do fluxo de caixa, além de riscos relacionados à concessão de garantias aos seus negócios, tornando-se solidária a pagamentos que não estão previstos no seu fluxo de caixa. Adicionalmente, riscos associados à não contabilização ou registro de forma íntegra, transparente e eficiente das transações da Companhia.

Riscos Estratégicos

Eventos decorrentes da tomada de decisão da alta administração e que podem gerar perda substancial no valor econômico da empresa. Normalmente, são associados à continuidade do negócio, mercado, competidores, investimentos, sucessão e inovação tecnológica.

Riscos de Tecnologia

São riscos ocasionados pela deficiência de controles tecnológicos, descontinuação ou obsolescência de tecnologias, *Cyber Security,* dentre outros.

V. GERENCIAMENTO DE RISCOS

O gerenciamento de risco possibilita a identificação dos riscos do negócio previamente, possibilitando que a Companhia consiga planejar ações, prevenir, transferir, reduzir, aceitar ou mitigar problemas que possam afetar diretamente a organização.

O ciclo de análise e gerenciamento de riscos deve ser contínuo e realizado conforme mudanças nos cenários internos e externos, ou renovado em até **1 ano** caso não possua alterações de contexto durante esse período.

O limite temporal a ser considerado para o ciclo de gerenciamento de riscos de cada processo de trabalho será decidido pelo respectivo Dono de Risco de acordo com a criticidade do mesmo, levando em conta o limite máximo estipulado anteriormente.

É responsabilidade do departamento de ***Compliance*** avaliar o contexto do negócio e alinhar sua análise de acordo com as diretrizes estratégicas da organização, bem como do escopo e propósito da avaliação de riscos. Assim como é responsabilidade do Dono de Risco avaliar a necessidade dos processos de trabalho que devem ter os riscos gerenciados e tratados com prioridade em seu departamento, de acordo com os impactos que possam causar, sob os aspectos estratégico, orçamentário, imagem, etc. E principalmente alinhado ao apetite à risco da organização.

Durante uma análise de riscos, os envolvidos devem dispor dos insumos requisitados e apoiar com informações pertinentes a cada tipo de projeto, tais como ativos, processos, projetos, entrevistas, etc.

Adicionalmente, o departamento de **Auditoria Interna** deve manter comunicação dos Riscos Relevantes para a Alta Administração da Companhia de forma a garantir participação estratégica no processo de gestão de riscos.

VI. ANÁLISE E IDENTIFICAÇÃO DE RISCOS

Os riscos da Companhia são identificados e avaliados de acordo com as diretrizes estratégicas da organização, sendo a identificação da necessidade da análise de riscos de responsabilidade de todo integrante responsável por um processo, seja por mudanças normativas, sistêmicas, de projeto, etc. Ou, até mesmo, por meios distintos, tais como:

- - Resultados de auditorias internas e/ou externas;
- Pesquisas de satisfação;
- Solicitações da alta direção;

- Denúncias;
- Identificação de ameaças ou vulnerabilidades;
- Entrevistas com os responsáveis pelos processos de negócios;
- Outras fontes de análise dos profissionais da empresa.

As análises serão amparadas nos processos contínuos que a Companhia conduz para fornecer, compartilhar ou obter informações e envolvimento com as partes interessadas e outros, com relação ao gerenciamento dos riscos. O entendimento e consulta às partes interessadas são relevantes na medida em que elas fazem críticas sobre riscos com base em suas percepções. Entretanto, as percepções variam devido às diferenças de conceitos, valores, preocupações, necessidades, suposições e ideias das partes interessadas. Como os seus pontos de vista geralmente possuem impactos significativos nas decisões tomadas, convém que as percepções das partes interessadas sejam identificadas, registradas e levadas em consideração no processo de tomada de decisão.

VII. CLASSIFICAÇÃO DE RISCOS

Os riscos mapeados serão registrados e gerenciados pela área de gestão de riscos.

Esse registro deve conter a informação da probabilidade de ocorrência e impacto que podem ser causados para a Companhia, por meio da geração de uma nota obtida pela fórmula:

R = P x I	**R** = Risco **P** = Probabilidade **I** = Impacto

Probabilidade

A probabilidade do risco é a frequência que ele pode ocorrer em determinado período de tempo, utilizando como parâmetro a facilidade de explorar o risco.

1. Muito Baixo
Rara, ocorre em situações excepcionais.

2. Baixo
Improvável, pode ocorrer em algumas circunstâncias.

3. Médio
Possível, provavelmente ocorrerá em determinadas circunstâncias.

4. Alto
Provável, ocorrerá na maioria das circunstâncias.

5. Muito Alto
Quase certa, ocorrerá em quase todas as circunstâncias.

Impacto

O impacto do risco será a consequência que esse risco causará para a Companhia caso seja explorado. A sua definição ocorrerá de acordo com a tabela abaixo e/ou entrevistas realizadas:

1. **Muito Baixo**
   Eventos que não causam impacto na produção/operação, danos à reputação, violação de requisitos legais, aos atributos de segurança e/ou faturamento da Companhia.

2. **Baixo**
   Eventos de baixo impacto na produção, podendo gerar queda de performance de um ou mais sistemas, violação de requisitos legais e aos atributos de segurança da Companhia

3. **Médio**
   Incidentes que causam impacto parcial na produção/operação, danos à reputação, violação de requisitos legais, aos atributos de segurança e/ou faturamento da Companhia.

4. **Alto**
   Incidentes de grande impacto na produção/operação, gerando indisponibilidade de um ou mais sistemas e/ou a impossibilidade de faturamento da Companhia.

5. **Muito Alto**
   Incidentes que causam impacto na produção/operação, danos à reputação, violação de requisitos legais, aos atributos de segurança e/ou faturamento da Companhia.

MAPA DE CALOR

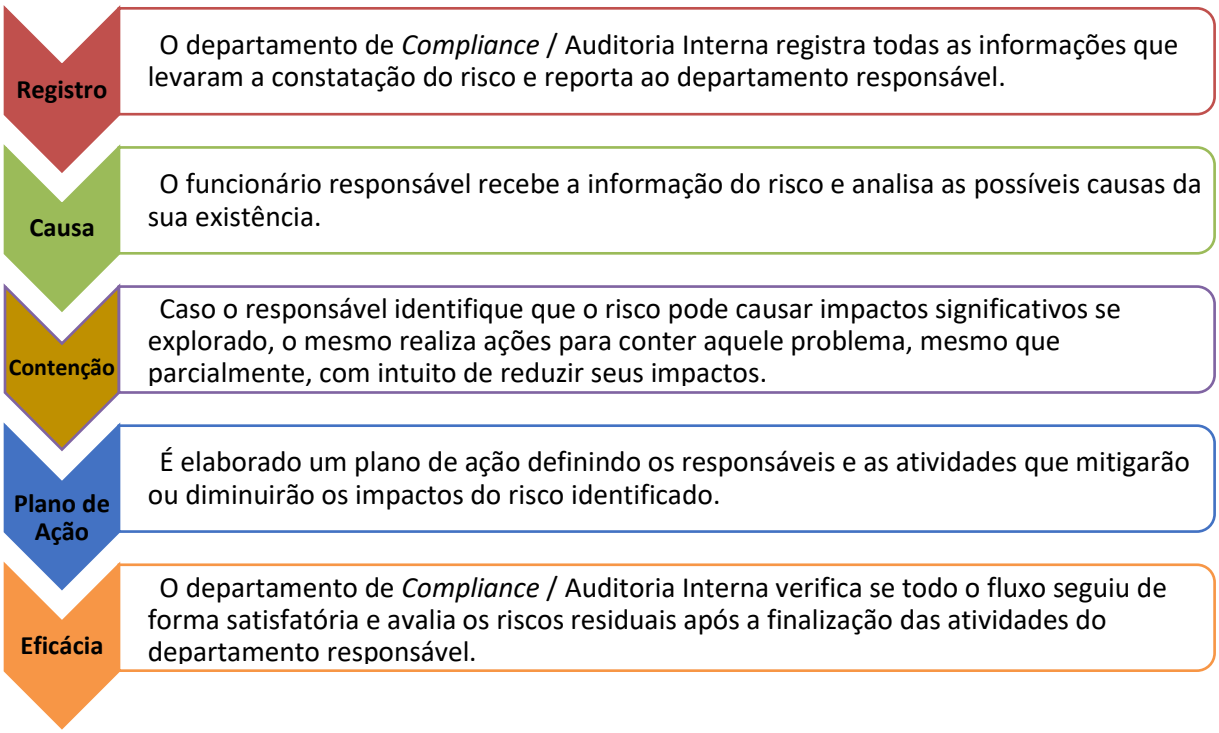
Probabilidade						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Impacto				

Legenda	
	Muito Alto
4	Alto
3	Médio
2	Baixo
	Muito Baixo

O processo de gestão de riscos deve, no mínimo:

- Compartilhar os resultados do processo de Gestão de Riscos;
- Apresentar um Plano de Tratamento dos Riscos;
- Prover responsabilidades sobre os Riscos;
- Aprimorar a conscientização.

Após o mapeamento de riscos identificados, o departamento de gestão de riscos reportará os resultados identificados para o gestor responsável, sendo que os riscos não aceitáveis devem possuir as seguintes etapas:



VIII. TRATAMENTO DE RISCOS

Considerando todas as disposições desta Política, posteriormente à avaliação dos riscos haverá a definição do tratamento que deverá ser realizado aos riscos relevantes e como estes deverão ser monitorados e comunicados a todas as partes envolvidas.
O Programa de *Compliance* da ATMA Participações S.A. possui como foco a gestão dos riscos sobre os quais se encontra exposta. A Companhia não medirá esforços para disseminar a cultura de *Compliance* entre todos seus colaboradores e parceiros.

As atividades de controle para a mitigação dos riscos são compreendidas por políticas e procedimentos elaborados para assegurar que as diretrizes e os objetivos definidos para minimizar seus riscos estão sendo observados nas atividades executadas.

Cabe à Auditoria Interna elaborar e atualizar o seu plano anual com foco nos riscos de maior relevância e exposição. Além da responsabilidade com tal plano, a Auditoria Interna atua em atividades de auditoria contínua, que promove a melhoria contínua do ambiente de controles e gestão de riscos via análise de dados visando a redução de fraudes e correção de erros. Esta também está incumbida de realizar auditorias de *Compliance* externas e internas, auditorias de processos de negócio e demandas especiais.

Evitar ou Eliminar o Risco

Se possível e não estiver em desacordo com o negócio, missão e objetivos da Companhia, a primeira opção para o tratamento de riscos deve ser “evitar o risco”. “Evitar o risco” implica em deixar de utilizar a tecnologia, controle ou processo à qual o risco é inerente, tal ação deve ser comprovada

Mitigar o Risco

Caso não seja possível evitar o risco, devem ser implementados “controles preventivos” para minimizar os riscos. “Controles preventivos” são aqueles que têm a finalidade de impedir que um evento seja explorado.

Todos os riscos identificados e que não puderam ser evitados, devem possuir controles implementados.Exceções em que não será possível implementar controles preventivos, seja pela relação custo benefício, por contrariedade aos objetivos e missão da Companhia ou por algum outro fator impeditivo, opta-se por “controles detectivos”.

“Controles detectivos” têm a finalidade de identificar as atividades que possuem riscos após a sua ocorrência, o que permite apenas que ações corretivas sejam tomadas no caso da identificação de uma exploração de vulnerabilidade.

Transferir o Risco

Caso não seja possível, viável ou estrategicamente interessante implementar controles internamente, a Companhia pode optar por transferir riscos considerando:

Terceirização de atividades relacionadas ao risco, desde que permitido no contexto legal e regulatório.

Contratação de seguros (a contratação de seguros pode ser utilizada em situações em que as vulnerabilidades envolvidas apresentem riscos financeiros significativos para a Companhia.)

Aceitar o Risco

Os riscos classificados como “Muito Baixo/Baixo”, ou cujo investimento para o seu respectivo tratamento seja maior que o impacto da materialização do risco e não ocasionam prejuízos de imagem para da Companhia, podem ser assumidos pela gerência responsável.

Assumir o risco significa entender a vulnerabilidade, os impactos da sua exploração e formalmente assumir a responsabilidade pelas consequências.

IX. AVALIAÇÃO DE RISCO RESIDUAL

Uma vez aplicado um controle, o valor de risco será recalculado considerando a forma como o controle atua sobre o evento. O risco resultante é chamado de Risco Residual.

Dessa forma, os riscos identificados devem ser reduzidos, apresentando valores do nível de classificação “muito baixo/baixo”, o que significa que uma vez aplicada à medida selecionada, o risco está sob controle. Quando todos os riscos não toleráveis de determinado ativo estiverem sendo tratados, ou por controles ou por outra opção de tratamento, o ativo passa a ser indicado como controlado.

X. FORNECEDORES

A área de Suprimentos é responsável por avaliar os riscos relacionados a fornecedores, que serão avaliados previamente à celebração de contrato e renovados periodicamente.

Caso, após a realização da análise, a área de gestão de riscos dê um parecer desfavorável e a viabilidade estratégica do negócio for de grande relevância para a Companhia, a contratação dos serviços somente será realizada com a aprovação da alta direção da Companhia. Sendo "reprovados" pela diretoria, tais fornecedores serão bloqueados pela Companhia. Para negociações futuras de fornecedores bloqueados, será necessária uma nova análise.

XI. RESPONSABILIDADE DAS PARTES

Conselho de Administração:

(i) Aprovar o apetite de risco para a Companhia em função da relação "risco x retorno" apresentado pela Alta Direção; e
(ii) Deliberar sobre os limites aceitáveis de exposição dos riscos da Companhia.

Comitê de Auditoria:

(i) Assessorar o Conselho de Administração nas questões relacionadas à auditoria interna e externa, aos mecanismos e controles de gestão de riscos;
(ii) Definir estratégias e políticas voltadas a controles internos e conformidade com as normas aplicáveis em assuntos relacionados aos temas de sua competência; e
(iii) Sempre que julgar necessário, propor alterações na Política de Gestão de Riscos e submetê-las ao Conselho de Administração.

Alta Direção:

(i) Gerir os riscos da Companhia e de suas controladas;
(ii) Implementar as estratégias e diretrizes da Companhia aprovadas pelo Conselho de Administração;
(iii) Sempre que julgar necessário, propor revisões na Política de Gestão de Riscos e submetê-las ao Conselho de Administração;
(iv) Conscientizar os colaboradores sobre a importância da gestão de riscos; e
(v) Aprovar normas específicas com base na presente Política, nas deliberações e orientações do Conselho de Administração e do Comitê de Auditoria.

Gestão de Risco:

(i) Realizar o *Risk Assessment* para identificar os riscos a que a Companhia e suas controladas estão expostas;

(ii) Discutir e acompanhar as recomendações propostas pelos Donos dos Riscos para minimizar os riscos da Companhia de acordo com a estratégia e objetivos definidos; e
(iii) Monitorar a implementação dos planos de ação para tratar os riscos não mitigados e testá-los quando implementados.

Auditoria Interna:

(i) Executar o plano de auditoria com base nos riscos relevantes mapeados no *Risk Assessment*;
(ii) Reportar os pontos de ações e falhas de controles e processos para o Comitê de Auditoria; e
(iii) Monitorar a implementação dos planos de ação dos riscos relevantes para tratar os riscos não mitigados e testá-los quando implementados.

Donos dos Riscos:

(i) Gerenciar os riscos inerentes às suas atividades, identificando-os, avaliando-os e tratando-os, com o intuito de assegurar a geração de valor para os acionistas e demais partes interessadas;

(ii) Avaliar anualmente o desempenho e resultados dos riscos e controles sob sua gestão; e

(iii) Comunicar à Auditoria Interna novos riscos identificados e qualquer alteração em seu processo de negócio.

Compliance:

(i) Realizar o *Risk Assessment* anualmente ou quando julgar necessário conforme identificação de necessidade de averiguação de novos riscos os quais a ATMA e suas controladas estejam expostas; e

(ii) Responsável por aprovar o Código de Ética e Conduta, providenciar sua divulgação, esclarecer dúvidas sobre seu conteúdo e analisar as infrações cometidas por colaboradores, que constituem violação do *Compliance* ao Código de Ética e Conduta.

Segurança da Informação:

(i) Identificar, analisar e tratar os riscos de Segurança da Informação e;

(ii) Implementar e manter o sistema gestor de segurança da informação de acordo com as necessidades da empresa, leis, regulamentos, contratos locais e internacionais.

4. Anexos

Não aplicável.

5. Glossário

Não aplicável.

POLÍTICA DE GESTÃO DE RISCOS

6. Ficha Técnica

Nome da Política: Política de Gestão de Riscos
Código da Política: POL 10.3.4
Número e data da versão: 4
Área Responsável pelo Documento: Diretoria de *Compliance*
Referências:
Nome e cargo do colaborador que elaborou a Política: Vitor Hugo Ataide Almeida
Nome e cargo do colaborador do Jurídico Corporativo que revisou a Política: Patrícia Montoro
Nome e cargo do colaborador do *Compliance* que revisou a Política: Letícia Malheiros
Nome do(a) Diretor(a) que aprovou a Política: Letícia Malheiros
Data de aprovação da versão atual da Política: 29/04/2022
Data de publicação da versão atual da Política: 29/04/2022
Prazo para a revisão da Política: 29/04/2024
Classificação da Informação: Pública
Áreas relacionadas com o processo disciplinado: Todas
Processo: Gestão de Riscos

Histórico de Versões

Versão	Data	Alterações
1	02/02/2016	Elaboração da Política
2	22/03/2017	- Inclusão da categoria de riscos de Segurança da Informação; - Inclusão da atuação de Segurança da Informação; - Inclusão da atuação de Compliance; - Atualização da descrição dos riscos financeiros.
3	19/07/2018	Adequação da marca LIQ
4	29/04/2022	Revisão geral; mudança de numeração; adequação da marca ATMA