

POLÍTICA DE GESTÃO DE RISCOS

GRUPO EQUATORIAL

GRUPO

equatorial



SUMÁRIO

1. FINALIDADE	5
2. CAMPO DE APLICAÇÃO	5
3. RESPONSABILIDADES	5
1. Conselho de Administração	5
2. Comitê de Auditoria Estatutária	6
3. Área de Gestão de Riscos e Controles Internos	6
4. Presidentes e Superintendentes	7
5. Gestores das Áreas de Negócios (Donos dos Riscos - Risk Owners)	7
6. Auditoria interna	8
4. DEFINIÇÕES	8
1. Auditoria	8
2. Appetite a Risco	8
3. Avaliação de Risco	9
4. CA	9
5. CAE	9
6. Controle Interno	9
7. Criticidade	9
8. Dano	9
9. Evento	9
10. Gestão de Riscos	9
11. Impacto	10



SUMÁRIO

12. Matriz de Riscos Corporativos	10
13. Processo	10
14. Probabilidade	10
15. Resposta ao Risco	10
16. Risco	10
17. Risco Corporativo	11
18. Risco Inerente	11
19. Risco Residual	11
20. Risco prioritário do negócio	11
21. Risco prioritário transversal	11
22. Stakeholder	11
23. Vulnerabilidade	11
24. Indicadores de Risco (KRI's)	12
5. DIRETRIZES DA GESTÃO DE RISCOS	12
1. Estabelecer, disseminar e cultivar uma cultura voltada à Gestão de Riscos	12
6. OBJETIVOS DA GESTÃO DE RISCOS	12
7. CATEGORIA DOS RISCOS	13
1. Estratégicos	13
2. Financeiros	13
3. Regulatórios	13
4. Cibernéticos e de Tecnologia	14
5. Operacionais	14



SUMÁRIO

8. ESTRUTURA DE GESTÃO DE RISCOS	14
1. Modelos das Três Linhas	16
9. ETAPAS DA GESTÃO DE RISCOS	16
1. Identificação e Análise de Riscos	16
2. Avaliação de Riscos	17
3. Resposta aos Riscos	19
4. Monitorar os Riscos	20
10. REFERÊNCIAS	21



1.0 - FINALIDADE

Estabelecer diretrizes para assegurar as melhores práticas da Gestão de Riscos Corporativos, relacionadas à identificação, avaliação, monitoramento e reporte dos riscos, que possam afetar os objetivos estratégicos do Grupo Equatorial.



2.0 - CAMPO DE APLICAÇÃO

Aplica-se ao Grupo Equatorial e suas controladas.

No caso de sociedades nas quais o Grupo Equatorial exerça influência significativa, tais como joint ventures e sociedades que a Companhia detenha participação minoritária, o conteúdo desta Política deverá ser levado ao conhecimento dos stakeholders, permitindo a incorporação, sempre que possível e alinhada com a Superintendência de Auditoria, Riscos e Controles Internos do Grupo Equatorial, das diretrizes por ela preconizadas.



3.0 - RESPONSABILIDADES

3.1 Conselho de Administração

- a) Definir as estratégias para alcance dos objetivos e perenidade dos negócios do Grupo Equatorial;
- b) Aprovar a Política de Gestão de Riscos e suas revisões quando necessário;
- c) Avaliar e aprovar a matriz de riscos corporativos, validando os limites aceitáveis ao apetite a riscos do Grupo Equatorial;

d) Decidir sobre a periodicidade da avaliação dos riscos contidos na Matriz, considerando seu impacto e a vulnerabilidade no Grupo Equatorial.

3.2 Comitê de Auditoria Estatutária

a) Garantir que o Grupo Equatorial mantenha uma cultura voltada à Gestão de Riscos, incentivando o cumprimento da Política e da Norma de Procedimento de Gestão de Riscos;

b) Analisar a Política de Gestão de Riscos, metodologia e os documentos que suportam o processo de gestão de riscos do Grupo, submetendo-os à ciência e aprovação do Conselho de Administração;

c) Avaliar, periodicamente, a estrutura de controles internos do Grupo Equatorial, verificando sua eficiência e influências decorrentes de potenciais mudanças no ambiente interno e/ou externo do Grupo Equatorial, por meio da Superintendência de Auditoria, Riscos e Controles Internos;

d) Supervisionar as atividades de responsabilidade a Superintendência de Auditoria, Riscos e Controles Internos;

e) Reportar periodicamente o nível de exposição dos riscos prioritários ao Conselho de Administração;

f) Supervisionar a adequação dos processos relativos ao gerenciamento de riscos e ao sistema de controles internos, em linha com as diretrizes estabelecidas pelo Conselho de Administração.

3.3 Área de Gestão de Riscos e Controles Internos

a) Definir a estrutura e metodologia, bem como executar a estratégia de Gestão de Riscos Corporativos do Grupo Equatorial;

b) Avaliar e monitorar as exposições a riscos, acompanhando a implantação das ações de mitigação das áreas de negócio e reportando o cenário, periodicamente, à Alta Administração e ao Comitê de Auditoria Estatutária;

- c) Assessorar a Alta Administração na proposição do Apetite a Risco, bem como auxiliar as áreas de negócio na identificação de
- d) Reportar ao Comitê de Auditoria Estatutária o resultado da avaliação contínua da estrutura de controles internos, mantendo a base atualizada com os registros de perdas que se materializarem na Companhia;
- e) Desenvolver em conjunto com as áreas de negócio os indicadores para monitoramento dos riscos, bem como proposta dos limites de tolerância;
- f) Apoiar as áreas de negócio no desenho e na melhoria de Controles Internos para tratamento das não-conformidades identificadas nos trabalhos de Auditoria Interna e mapeamento de riscos;
- g) Conscientizar os gestores sobre a importância da gestão de Riscos e a responsabilidade inerente a cada colaborador.

3.4 Presidentes e Superintendentes

- a) Fomentar a cultura da Gestão de Riscos junto as áreas de negócio;
- b) Monitorar os Indicadores de Risco (KRI's) sob suas responsabilidades, garantindo a execução de planos de resposta e/ou ações mitigadoras para manutenção dos limites de tolerância estabelecidos;
- c) Informar, tempestivamente, à Superintendência de Auditoria, Riscos e Controles Internos riscos não mapeados, sejam eles novos ou não identificados anteriormente.

3.5 Gestores das Áreas de Negócios (Donos dos Riscos - Risk Owners)

- a) Fomentar a cultura da Gestão de Riscos junto as áreas de negócio, incorporando-a no planejamento e gestão de processos críticos;
- b) Monitorar os riscos, direta ou indiretamente, envolvidos nas operações sob sua gestão, a partir da identificação das causas e consequências associadas à materialização;

c) Garantir que os riscos estejam dentro dos limites de tolerância definidos pelo Conselho de Administração;

d) Informar, tempestivamente, à Superintendência de Auditoria, Riscos e Controles Internos eventos relevantes que afetem o grau de exposição do Grupo Equatorial a riscos, incluindo os resultados dos indicadores de riscos prioritários;

e) Garantir a operacionalização da gestão de riscos, sendo parte integrante do processo de identificação, avaliação e mensuração, bem como, a implementação de ações e planos de resposta, relativos aos riscos envolvidos nas operações sob sua gestão, de acordo com as deliberações tomadas em conjunto com a Área de GRC e Comitê de Auditoria e Riscos.

3.6 Auditoria interna

a) Avaliar a adequação e eficácia dos controles internos das unidades que compõem o Grupo Equatorial;

b) Apresentar recomendações para minimizar riscos através do aprimoramento das estruturas de controle existentes;

c) Apontar ao Comitê de Auditoria Estatutária a ocorrência de não conformidades, oportunidades de melhorias nos processos e nos controles, falhas, desvios, irregularidades e/ou ilegalidades observadas.

4.0 - DEFINIÇÕES

4.1 Auditoria

Processo de exame, análise e validação de um sistema, atividade ou informação.

4.2 Apetite a Risco

Nível de risco que uma organização está disposta a aceitar para atingir seus objetivos.



4.3 Avaliação de Risco

Significância do risco identificado, relacionado ao impacto e à vulnerabilidade dos controles internos.

4.4 CA

Conselho de Administração.

4.5 CAE

Comitê de Auditoria Estatutária.

4.6 Controle Interno

Conjunto de atividades, métodos ou rotinas destinadas a assegurar confiabilidade aos processos do negócio, atender às leis e regulamentos aplicáveis, proteger os ativos e ajudar a administração no alcance dos objetivos da Companhia.

4.7 Criticidade

Nível de risco implícito em um processo ou atividade. Quanto maior o risco intrínseco, mais crítico se torna o processo ou atividade.

4.8 Dano

Perda ou prejuízo sofrido em razão de ação, omissão ou influência de alguém.

4.9 Evento

Ocorrência ou mudança em um conjunto específico de circunstâncias, que materializadas possam representar risco aos objetivos do processo ou da política da Companhia.

4.10 Gestão de Riscos

Atividade coordenada que visa identificar, avaliar, priorizar e monitorar a organização no que se refere a riscos.

4.11 Impacto

Nível de severidade dos efeitos causados por certa ação ou acontecimento. É a magnitude do dano levando-se em consideração a gravidade das consequências aos negócios da Companhia.

4.12 Matriz de Riscos Corporativos

Ferramenta que permite à Alta Administração mensurar, avaliar e ordenar os eventos de riscos estratégicos que podem afetar o alcance dos objetivos de suporte do Grupo, tipificando os riscos em baixo, médio, alto ou muito alto.

4.13 Processo

Conjunto de macroatividades interdependentes e interligadas, objetivando desempenhar uma função corporativa.

4.14 Probabilidade

Possibilidade de materialização de um determinado Risco.

4.15 Resposta ao Risco

Decisões tomadas pela Companhia que visam reduzir as ameaças que possam comprometer, e até prejudicar, o alcance dos objetivos e perenidade dos negócios do Grupo.

4.16 Risco

Incertezas inerentes a um conjunto de possíveis consequências (ganhos ou perdas) que resultam de decisões tomadas diariamente pela organização, com possibilidade de causar problemas de continuidade do negócio, responsabilização criminal dos administradores, fragilidades e deficiências importantes.

4.17 Risco Corporativo

Riscos que podem afetar a Companhia como um todo, impactando diretamente os objetivos estratégicos da organização.

4.18 Risco Inerente

Riscos sempre presentes no ramo do negócio, nos processos ou na atividade, independente dos controles internos administrativos adotados.

4.19 Risco Residual

Risco remanescente após a mitigação por controles internos.

4.20 Risco prioritário do negócio

Riscos priorizados pela Alta Administração e exclusivos de cada negócio (Distribuição, Transmissão, Renováveis e Saneamento).

4.21 Risco prioritário transversal

Riscos priorizados pela Alta Administração e presentes em todos os negócios do grupo.

4.22 Stakeholder

Público estratégico e descreve uma pessoa ou grupo que tem interesse em uma empresa, negócio ou indústria, podendo ou não ter feito um investimento neles.

4.23 Vulnerabilidade

Refere-se ao quão preparada as empresas estão com controles internos para mitigar os riscos identificados. O que se exemplifica em instrumentos normativos, sistemas e projetos em desenvolvimento.

4.24 Indicadores de Risco (KRI's)

Componentes do processo de monitoramento de riscos utilizados para verificar a evolução de um risco ou condições de risco em potencial, informando o perfil do risco em relação ao apetite ao risco (nível de risco tolerável), sinalizando aos gestores a necessidade de ações a serem tomadas em relação ao apetite ao risco (nível de risco tolerável), sinalizando aos gestores a necessidade de ações a serem tomadas.

5.0 - DIRETRIZES DA GESTÃO DE RISCOS

5.1 Estabelecer, disseminar e cultivar uma cultura voltada à Gestão de Riscos



- a) Identificar os riscos inerentes ao negócio, priorizá-los, avaliar e responder de acordo com o apetite a riscos do Grupo Equatorial;
- b) Garantir que todos os colaboradores compreendam os objetivos, papéis, funções e as responsabilidades atribuídas para cada agente envolvido no processo de gestão de riscos;
- c) Estabelecer, de forma tempestiva e em conjunto com as áreas de negócio, planos de resposta aos riscos tempestivamente monitorados pelas instâncias responsáveis no Grupo.
- d) Reportar os KRI's de acordo com os limites de tolerância a riscos, previamente aprovados pelo Conselho de Administração e as estratégias de mitigação dos riscos.

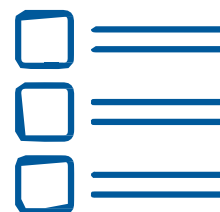


6.0 - OBJETIVOS DA GESTÃO DE RISCO

- a) Atuar em sintonia com as melhores práticas de mercado quanto à gestão de riscos;
- b) Proteger o Grupo Equatorial contra potencial perda de valor, a partir de indicadores de riscos definidos com as áreas de negócio;
- c) Identificação e tratamento de riscos que possam ameaçar a execução dos objetivos estratégicos do Grupo;
- d) Melhorar a confiança das partes interessadas;

- e) Buscar reduzir a probabilidade de ocorrência de fraudes e erros em processos operacionais;
- f) Identificação de oportunidades de melhorias, objetivando a redução de atividades manuais, morosidades e gargalos em processos;
- g) Aumentar o alinhamento e sinergia entre gerências e processos dentro da empresa;
- h) Garantir o alinhamento das diretrizes da Alta Administração com os processos operacionais.

7.0 CATEGORIA DOS RISCOS



O Dicionário de Riscos Corporativos do Grupo Equatorial considera as características e o ambiente de negócio da empresa, classificando os riscos mapeados em cinco categorias de riscos:

7.1 Estratégicos

Possível impacto decorrente de práticas frágeis governança, decisões não baseadas em um planejamento estratégico, investimentos indevidos e falta de capacidade de resposta às mudanças no ambiente, ou de publicidade negativa sobre práticas e/ou negócios da organização.

7.2 Financeiros

Possível impacto derivado de operações financeiras incoerentes com boas práticas de mercado, ou em desacordo com os valores da Companhia.

7.3 Regulatórios

Possível impacto originário do descumprimento de leis/regulamentos ou processos movidos por clientes, contrapartes e denúncias.

7.4 Cibernéticos e de Tecnologia

Possível impacto decorrente do desalinhamento estratégico da tecnologia da informação com os objetivos do negócio, ataques cibernéticos e comprometimento da segurança das informações, indisponibilidade de sistemas e perda de integridade

7.5 Operacionais

Possível impacto decorrente de problemas operacionais, como falhas nos controles internos.



8.0 - ESTRUTURA DE GESTÃO DE RISCOS

A definição da estrutura de Gestão de Riscos do Grupo Equatorial considera o contexto atual da companhia, boas práticas de mercado e a integração dos riscos aos processos do Grupo, reforçando a responsabilidade de todos os colaboradores para gestão dos riscos corporativos, permitindo que os objetivos estratégicos do Grupo sejam alcançados, conforme adotado no modelo das Três Linhas de Defesa proposto pelo IIA (Institute of Internal Auditors):



LEGENDA

↑ Prestação de contas, reparte

↓ Delegar, orientar, recursos, supervisão

↔ Alinhamento comunicação coordenação, colaboração

8.1 Modelos das Três Linhas

1. Como 1ª linha, as Áreas e Unidades de negócio da Companhia são responsáveis pela gestão contínua dos riscos e exploração de oportunidades, propagando uma cultura de desenvolvimento dos processos, sistemas e controles internos, para atingimento das metas e objetivos estratégicos do Grupo Equatorial.
2. Como 2ª linha, tem o intuito de fornecer conhecimento complementar, de apoio a implantação e manutenção dos planos de resposta associados aos riscos e controles internos, assim como o desenvolvimento da melhoria contínua das práticas do gerenciamento de riscos.
3. Como 3ª linha, a Auditoria Interna deve atuar no assessoramento da administração, relacionado ao exame e avaliação da adequação, eficiência e eficácia dos sistemas de controles internos, conforme conceitos de gerenciamento de riscos do negócio.

9.0 - ETAPAS DA GESTÃO DE RISCOS



O processo de gestão de riscos do Grupo Equatorial considera as seguintes etapas:

9.1 Identificação e Análise de Riscos

1. Identificação de Risco e Fatores de Risco
A partir dos riscos identificados, devem ser mapeados os fatores de riscos relacionados a fim de permitir um melhor entendimento das principais causas que, potencialmente, levam à materialização dos mesmos, assim como, principais agravantes e atenuantes que servirão de insumo para avaliação de riscos.

Essa atividade deve ser coordenada e consolidada pela Superintendência de Auditoria, Riscos e Controles Internos, em conjunto com as áreas de negócio, responsáveis pela gestão contínua dos riscos.

9.1.2 Análise Geral de Riscos (AGR)

A AGR reflete, de maneira estruturada, as percepções da Alta Administração, bem como os executivos (áreas e unidades de negócio) em relação aos principais aspectos de gestão e riscos envolvidos nas operações, áreas/processos de negócio e características da Companhia;

A Área de GRC auxiliará as Áreas e unidades de negócio da Companhia na identificação dos riscos, sendo necessário ter em vista os possíveis cenários de perda para o Grupo Equatorial, ligando a estes suas respectivas causas e consequências relacionadas à materialização do risco.

9.2 Avaliação de Riscos

A avaliação de riscos tem como objetivo atribuir um nível de exposição aos riscos com base em vetores e critérios definidos. Os vetores principais utilizados pelo Grupo Equatorial são: Impacto e Vulnerabilidade.

9.2.1 Impacto

Refere-se à extensão que um evento de risco pode afetar à Companhia. A classificação de impacto do Grupo Equatorial considera um vetor principal financeiro e vetores auxiliares qualitativos.

A avaliação do impacto poderá ser realizada exclusivamente de forma qualitativa ou quantitativa, dependendo do risco que está sendo avaliado. É preferível a aplicação de método qualitativo caso a Companhia não possua dados confiáveis, íntegros ou não exista modelo reconhecido capaz de quantificar o risco ou cujo, modelo seja demasiado complexo e que o retorno da quantificação não supere o esforço do cálculo.

9.2.2 Vulnerabilidade

A Vulnerabilidade refere-se à quão preparada estão as defesas da organização frente aos eventos de riscos. A classificação da vulnerabilidade no Grupo Equatorial considera três vetores auxiliares: Controles Internos, Planos de Ação e/ou Resposta e Eventos Externos, logo será obtido o valor residual do risco.

9.2.3 Exposição ao Risco e Priorização

O resultado dos vetores principais (de impacto e vulnerabilidade) será a exposição ao risco, conforme demonstração gráfica abaixo:

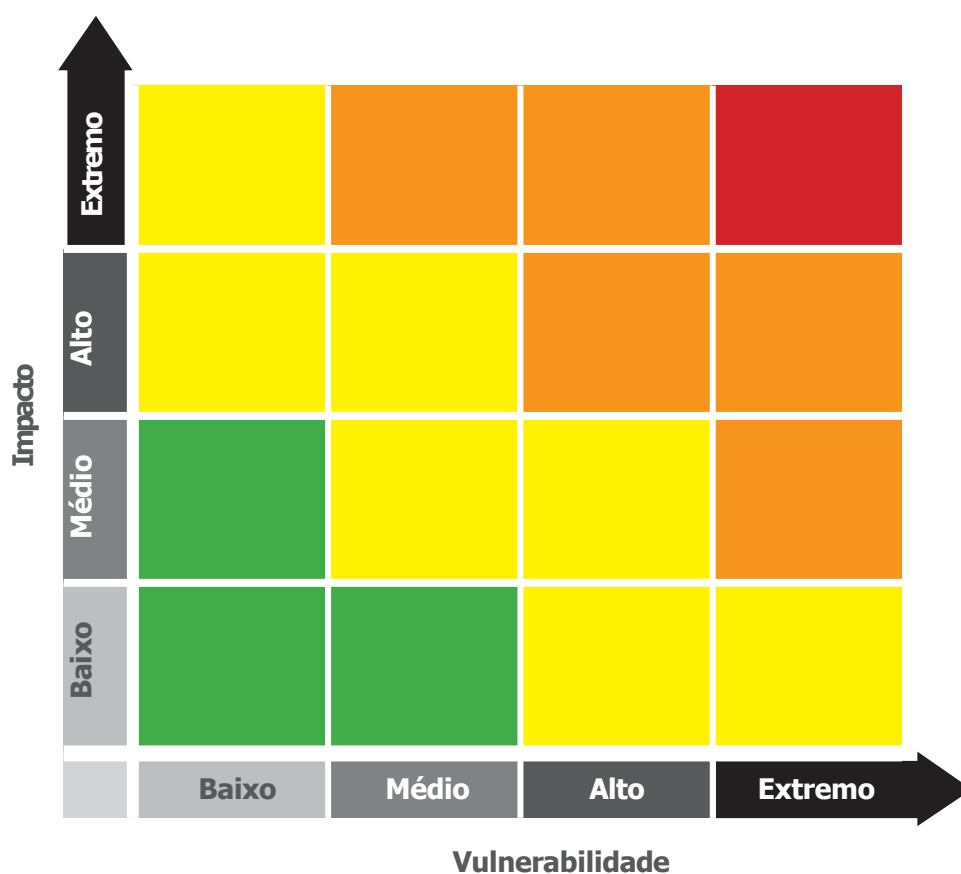


Figura 2: Mapa de Risco

A partir do resultado obtido na avaliação dos vetores de Impacto e Vulnerabilidade, os riscos devem ser classificados, conforme o grau abaixo:

a) EXTREMO: Representa extrema ameaça em potencial, é um evento intolerável, essa atividade não deve ser iniciada ou prossegui-la até que o risco seja reduzido. Em caso de não ser possível a redução do risco, mesmo utilizando recursos elevados, a atividade deve ser proibida.

b) ALTO: Representa grande ameaça em potencial, portanto, a atividade não deve ser iniciada até que o risco seja reduzido. Esforços e recursos devem ser alocados para mitigá-lo. Para atividade em andamento, ação urgente deve ser tomada.

c) MÉDIO: Realizar esforços para reduzir o risco, mas o custo de prevenção deve ser avaliado e limitado, possui menor o nível de criticidade quanto ao impacto nos negócios do Grupo. As medidas de redução de riscos devem ser implementadas em período de tempo definido.

d) BAIXO: Não requer controles adicionais aos que já existem. É necessário monitoramento e informação existentes. Há necessidade de instrução e monitoramento pelos responsáveis das atividades.

Os riscos prioritários, tanto transversais quanto os do negócio, seguem um fluxo diferenciado de tratamento, considerando: maior criticidade na implantação dos planos de resposta e ações de remediação de gaps de controle; definição de Indicadores de Risco para monitoramento e; maior frequência de reporte do status do risco e dos planos de resposta ao CAE e CA.

9.3 Resposta aos Riscos

Após a classificação dos riscos apresentadas no item anterior, é definido pela Companhia as estratégias para a tomada de decisão quando de possível materialização destes, a partir de uma série de medidas/respostas formais para mitigar as ameaças aos objetivos do Grupo Equatorial, a fim de estarem alinhadas aos respectivos apetites de risco definidos. As possibilidades de resposta ao risco são aceitar, compartilhar, evitar e reduzir:

a) Aceitar: a Alta Administração concorda em enfrentar o risco, se e quando ele se materializar. Um plano de solução, ou contingência pode ser desenvolvido para essa eventualidade. Estratégia utilizada quando não é possível ou prático responder ao risco, ou uma resposta não se justifica pela importância do risco;

b) Compartilhar: transferência ou compartilhamento de uma porção do risco, visando a redução da probabilidade ou do impacto (Exemplo: No risco de incêndio, onde o custo do sinistro poderia ser transferido para Seguradoras);

c) Evitar: está relacionada a uma ação que elimina totalmente a fonte de um risco específico (Exemplo: Venda de determinada operação);

d) Reduzir: são adotadas medidas para reduzir o nível de exposição de um evento de risco adverso para um limite aceitável pelo Grupo Equatorial;

Os Planos de Resposta devem definir também ações corretivas ou planos de emergência no caso de materialização de riscos, mesmo que a resposta tenha sido aceitar.

9.4 Monitorar os Riscos

O monitoramento dos riscos é um processo contínuo da Gestão de Riscos que consiste em definir, acompanhar e atualizar, periodicamente, os Indicadores e Fatores de Riscos, assim como o acompanhamento e atualização do status de implementação dos planos de resposta e/ou de ação em conjunto com as partes interessadas no gerenciamento de riscos.

Periodicamente, os resultados dos Indicadores devem ser reportados para: i) as áreas responsáveis pela gestão contínua dos riscos (1º linha), conforme frequência estabelecida para cada risco; ii) ao Comitê de Auditoria Estatutária e; iii) Conselho de Administração, de acordo com os respectivos calendários de reuniões e regimentos.

10- REFERÊNCIAS



1. Gerenciamento de Riscos Corporativos - Enterprise Risk Management - Aligning Risk with Strategy and Performance - COSO 2017;
2. Risk Assessment in Practice by Deloitte Touche Tohmatsu Services, Inc. - COSO 2012;
3. Developing Key Risk Indicators to Strengthen Enterprise Risk Management - COSO 2010;
4. Implementing Enterprise Risk Management - John R.S. Fraser - 2015;
5. Gerenciamento de Riscos Corporativos - Risk Assessment in Practice - COSO 2013;
6. Regulamento do Novo Mercado da B3;
7. ABNT NBR 31.000 ISO - Technical Management Board Working Group on Risk Management.

