FIAP ON

GESTÃO DE VULNERABILIDADES

GESTÃO DE RISCOS

MARCELO LAU

3

LISTA DE FIGURAS

Figura 3.1 – Operação Lava Jato 4
Figura 3.2 – Relação entre os princípios da gestão de riscos, estrutura e processo 7
Figura 3.3 – Relacionamento entre os componentes da estrutura para gerenciar riscos 9
Figura 3.4 – Processo de gestão de riscos 12

SUMÁRIO

3 GESTÃO DE RISCOS 4
3.1 Processo de gestão de riscos 5
3.2 Princípios da gestão de riscos 7
3.3 Estrutura da gestão de riscos 8
3.4 Processo da gestão de riscos 11
REFERÊNCIAS 15

3 GESTÃO DE RISCOS

A gestão de riscos começou a ser percebida como aliada da segurança da informação quando empresas, organizações e seus respectivos negócios passaram a ser impactados significativamente com as consequências da concretização de tais riscos, incluindo desastres humanos ou naturais, espionagem, terrorismo e outros fatores que resultaram em perdas financeiras a acionistas, empregados, fornecedores e demais componentes da cadeia produtiva.

Considerando fatos recentes, atrelados à investigação e seus respectivos desdobramentos da Operação Lava Jato, é importante que negócios considerem a adoção de medidas de conformidade e um melhor controle dos processos de governança corporativa, que permitem mensurar, de forma próxima aos gestores, os riscos que uma empresa pode vir a sofrer em função do desconhecimento dos mesmos.

Figura 3.1 – Operação Lava Jato
Fonte: Folha on-line (2018)

A gestão de riscos em âmbito corporativo conta com informações relacionadas a ameaças, fragilidades, controles, impacto e frequência, disponíveis em atividades realizadas pelo meio ambiente dos negócios, incluindo dados fornecidos pelos responsáveis pela segurança física e segurança lógica. Essa

gestão de riscos, quando realizada de maneira adequada, permite a harmoniosa integração entre essas áreas tão distintas.

A responsabilidade pela coordenação de todas essas atividades, assim como a atribuição das responsabilidades junto aos negócios são ações que devem ser promovidas pela área responsável pela gestão de riscos.

3.1 Processo de gestão de riscos

É adotada no processo de gestão de riscos a norma da ABNT NBR ISO 31000:2009, sendo esta uma referência para a implementação e operacionalização do processo de gestão de riscos em organizações de diversos segmentos de mercado, já que o termo “risco” nos remete à incerteza, que pode levar a resultados favoráveis ou não ao indivíduo ou à organização.

Segundo essa norma, a gestão de riscos possibilita a uma organização alcançar diversos objetivos, incluindo:

- Maior probabilidade de atingir certos objetivos;
- Encorajamento de gestão proativa;
- Atentar-se à necessidade de identificar e tratar os riscos em toda a organização;
- Melhora quanto ao processo de identificação de oportunidades e respectivas ameaças;
- Atendimento às normas internacionais, requisitos legais e regulatórios pertinentes;
- Melhora quanto ao reporte das informações financeiras;
- Melhora da governança;
- Melhora em relação à confiança das partes interessadas;
- Estabelecimento de uma base confiável para a tomada de decisão e o planejamento;

- Melhora em relação aos controles (incluindo os controles em segurança da informação);
- Alocação e utilização eficaz dos recursos destinados ao tratamento de riscos;
- Melhora da eficácia e a respectiva eficiência operacional;
- Melhora do desempenho quanto à segurança da informação, podendo ainda beneficiar outros aspectos corporativos, como sistemas de qualidade, sistemas de saúde, sistemas ambientais, entre outros;
- Melhora quanto à prevenção de perdas e a respectiva gestão de incidentes;
- Minimização de perdas;
- Melhora em relação à aprendizagem organizacional; e
- Aumento da resiliência da organização.

Considerando ainda a amplitude desejada quanto ao atendimento de partes interessadas em relação ao processo de gestão de riscos, entende-se que a mesma deve incluir:

- Os responsáveis pelo desenvolvimento da política de gestão de riscos no âmbito de suas organizações;
- Os responsáveis por assegurar que os riscos serão eficazmente gerenciados na organização como um todo ou em uma área, atividade ou projeto específicos;
- Os que precisam avaliar a eficácia de uma organização em gerenciar riscos; e
- Desenvolvedores de normas, guias, procedimentos e códigos de práticas que, no todo ou em parte, estabelecem como o risco deve ser gerenciado dentro do contexto específico desses documentos.

Em termos processuais (fluxo do processo de gestão de riscos), é possível adotar os relacionamentos mostrados na imagem a seguir, que traz a relação entre princípios da gestão de riscos, estrutura e processo.

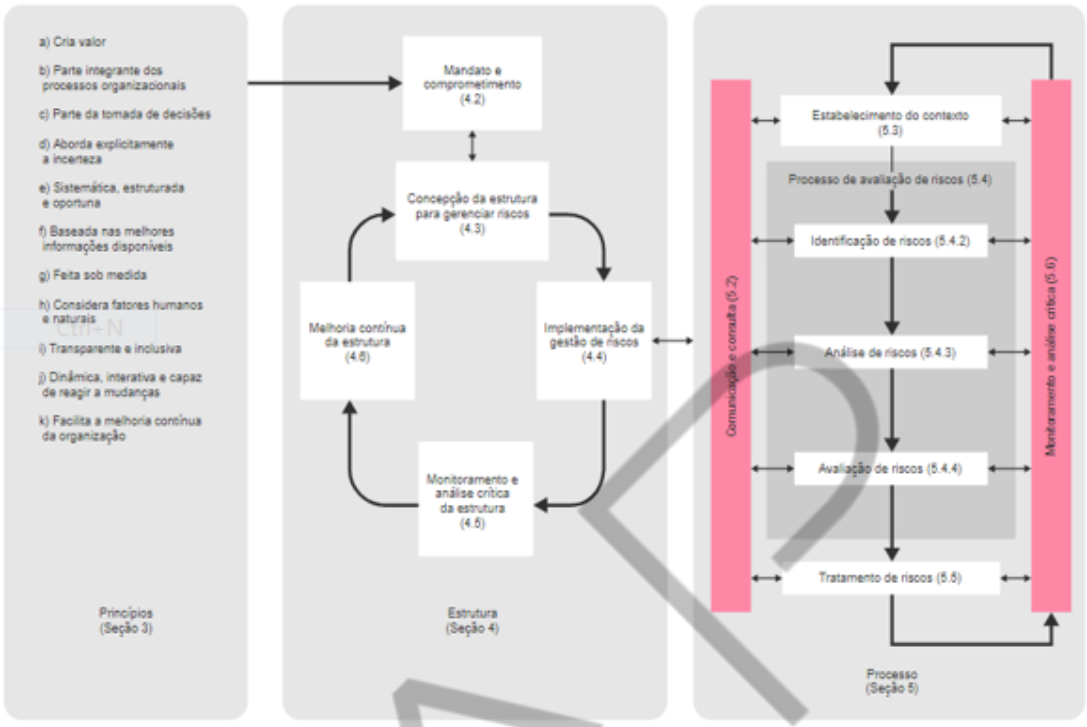

Figura 3.2 – Relação entre os princípios da gestão de riscos, estrutura e processo
Fonte: ABNT NBR ISO/IEC 31000:2009. Gestão de riscos – Princípios e diretrizes (2018)

É possível identificar na figura a menção às seções denominadas princípios, estrutura e processo, divididos respectivamente nas seções 3, 4 e 5, sendo esta a apresentação desses conteúdos na norma ABNT NBR ISO 31000:2009. Os itens apresentados a seguir visam apresentar essas seções e explaná-las.

3.2 Princípios da gestão de riscos

Para que a gestão de riscos se apresente de forma eficaz, é preciso considerar que uma organização atende todos os princípios relacionados a seguir:

- A gestão de riscos cria e protege valor;
- A gestão de riscos é parte integrante de todos os processos organizacionais;
- A gestão de riscos é parte da tomada de decisões;
- A gestão de riscos aborda explicitamente a incerteza;

- A gestão de riscos é sistemática, estruturada e oportuna;
- A gestão de riscos se baseia nas melhores informações disponíveis;
- A gestão de riscos é feita sob medida;
- A gestão de riscos considera fatores humanos e culturais;
- A gestão de riscos é transparente e inclusiva;
- A gestão de riscos é dinâmica, integrativa e capaz de reagir a mudanças; e
- A gestão de riscos facilita a melhoria contínua da organização.

Esses princípios não podem ser considerados exaustivos, sendo que devem refletir um grande engajamento de toda a organização e respectivos participantes do processo de gestão de riscos, pois o sucesso de todo o processo está calcado em assumir que estes sejam devidamente atendidos antes de se partir para a estrutura e o processo de gestão de risco, sendo os princípios, estrutura e processo de gestão de riscos intimamente interdependentes entre si.

3.3 Estrutura da gestão de riscos

O sucesso da gestão de riscos depende da eficácia da estrutura de gestão que irá apoiá-la através dos fundamentos e identificando o quanto essa estrutura está de fato incorporada em toda a organização.

Essa estrutura auxilia a gestão eficaz dos riscos através da aplicação do processo de gestão de riscos em diferentes níveis e dentro de contextos específicos em uma organização.

Na norma ABNT NBR ISO 31000:2009, há uma proposição ilustrativa que traz o relacionamento entre os componentes da estrutura destinada à gestão de riscos, conforme pode ser visto na figura a seguir:

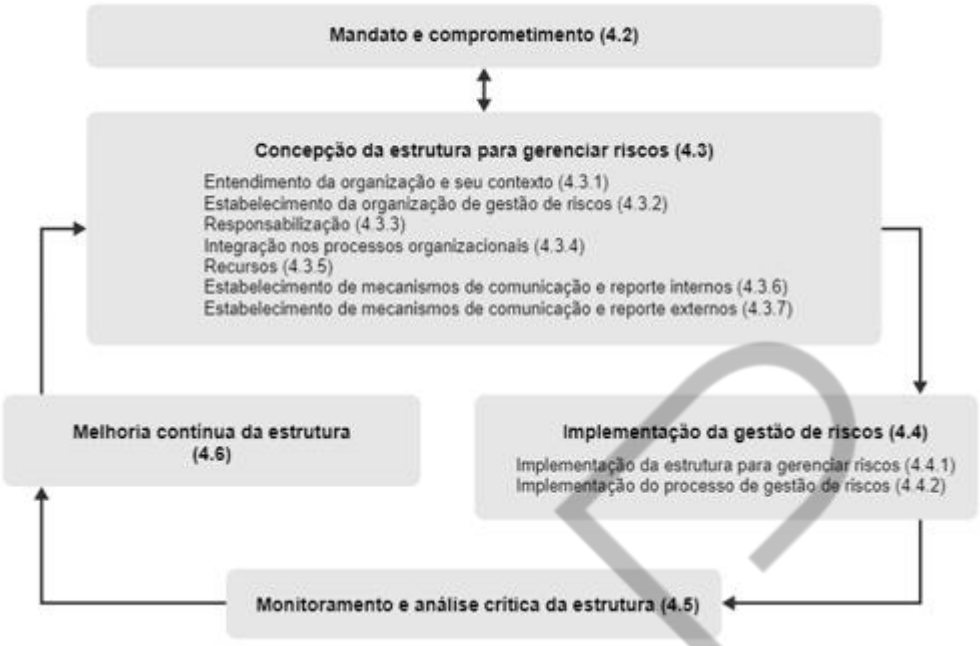

Figura 3.3 – Relacionamento entre os componentes da estrutura para gerenciar riscos
Fonte: ABNT NBR ISO/IEC 31000:2009. Gestão de riscos – Princípios e diretrizes (2018)

Essa estrutura não tem a pretensão de prescrever um sistema de gestão, entretanto, o mesmo visa auxiliar a organização a integrar a gestão de riscos em seu sistema de gestão global, possibilitando no mínimo a realização de uma reflexão sobre o quanto uma organização necessita se adaptar para que essa estrutura seja aderente aos interesses de uma empresa e eficaz do ponto de vista da gestão de riscos.

Os números indicados nessa figura, refletem itens constantes na norma ABNT NBR ISO 31000:2009, iniciando pelo item 4.2, denominado Mandato e comprometimento, e finalizando pelo item 4.6, denominado Melhoria contínua da estrutura. Esses itens serão descritos de forma sucinta a seguir.

O item denominado **Mandato** e **Comprometimento** (constante da norma como item 4.2) visa introduzir a gestão de riscos, garantindo a contínua eficácia requerida nesse processo, em que se espera um forte comprometimento sustentado e assumindo todos os responsáveis pelo processo de gestão de riscos corporativos.

O item denominado **Concepção da estrutura para gerenciar riscos** (constante da norma como item 4.3) visa, mesmo antes de iniciar a concepção e a implementação da estrutura destinada à gestão de riscos, a consideração quanto à

importância da avaliação e compreensão em relação aos contextos internos e externos da organização, já que estes podem influenciar significativamente a concepção da estrutura de gestão de riscos, nesse aspecto, esse assunto é abordado nos itens 4.3.1 a 4.3.7, nos quais são feitas considerações quanto ao ambiente cultural, social, político, legal, regulatório, financeiro, tecnológico, econômico, natural e competitivo, seja este de origem ou natureza internacional, nacional, regional ou local.

A **concepção da estrutura para gerenciar riscos** ainda considera a necessidade de estabelecimento de uma política de gestão de riscos, em que se espera que a organização de fato se comprometa com a gestão de riscos, trazendo base e justificativa para que esse processo seja legítimo em uma organização, dessa forma, além de ser concebida, espera-se que uma política seja atualizada periodicamente e comunicada às partes interessadas do processo, lembrando que papéis e responsabilidades precisam ser bem definidos.

Nesse item ainda estão previstas necessidades, como a integração dessa estrutura aos processos organizacionais já estabelecidos ou mesmo planejados em uma organização, sendo que uma estrutura consumirá recursos durante seu processo de concepção, implementação e manutenção da gestão de riscos, vale aqui detalhar os recursos exigidos para que uma estrutura como esta atenda às necessidades da organização, sendo estes:

- Pessoas, habilidades, experiências e competências;
- Recursos necessários para cada etapa do processo de gestão de riscos;
- Processos, métodos e ferramentas da organização que serão utilizados para gerenciar riscos;
- Processos e procedimentos documentados;
- Sistemas da gestão da informação e do conhecimento; e
- Programas de treinamento.

Todo sucesso relacionado à Concepção da estrutura para gerenciar riscos se pauta na existência de eficazes mecanismos de comunicação e reporte internos e externos. Nesse caso, alinhamentos devem ser constantes e periódicos, pois

problemas de eficácia atrelados à gestão de riscos em geral resultam de uma comunicação ineficaz ou inapropriada.

O item denominado **Implementação da gestão de riscos** (constante da norma como item 4.4) visa considerar a implementação da estrutura responsável pela gestão de riscos e a implementação do processo de gestão de riscos (algo que é descrito na seção 5 da norma ABNT NBR ISO 31000:2009), que serão mais bem explicadas neste material.

Itens que ainda complementam a **estrutura da gestão de riscos** são os itens 4.5 (Monitoramento e análise crítica da estrutura) e 4.6 (Melhoria contínua da estrutura), que trazem especificamente a necessidade de se adotar processos de gestão de riscos de forma eficaz e contínua, com o objetivo de apoiar o desempenho organizacional, para isso, medidas devem ser desenvolvidas e realizadas, visando a realização de análise crítica sobre o processo de gestão de riscos, sendo que a crítica vale à política, plano e estrutura da gestão de riscos.

No caso do processo de **melhoria contínua**, espera-se que as atividades de monitoramento e análises críticas venham a demandar decisões que devem ser tomadas sobre a política, o plano e a estrutura de gestão de riscos, visando o aprimoramento da mesma de acordo com necessidades diversas, incluindo a atualização do processo de gestão de riscos, alterações políticas, sociais, econômicas, entre outras, vale destacar necessidades atuais a novos regulamentos, como a GDPR (*General Data Protection Regulation*), em que todas as empresas envolvidas na manipulação e no tratamento de dados pessoais dos cidadãos da Comunidade Europeia precisam ter requisitos legais, estabelecidos na regulamentação. Esse regulamento foi promulgado em abril de 2016 e entrou em vigor em maio de 2018, com o objetivo de que as organizações estivessem em conformidade com essa regulamentação.

3.4 Processo da gestão de riscos

Espera-se que a gestão de riscos seja parte integrante da gestão corporativa, seja algo incorporado na cultura organizacional e esteja refletida em boas práticas, além de estar devidamente adaptada aos processos de negócios da organização,

sendo compreendida pelo diagrama contido na norma ABNT NBR ISO 31000:2009, apresentado a seguir:

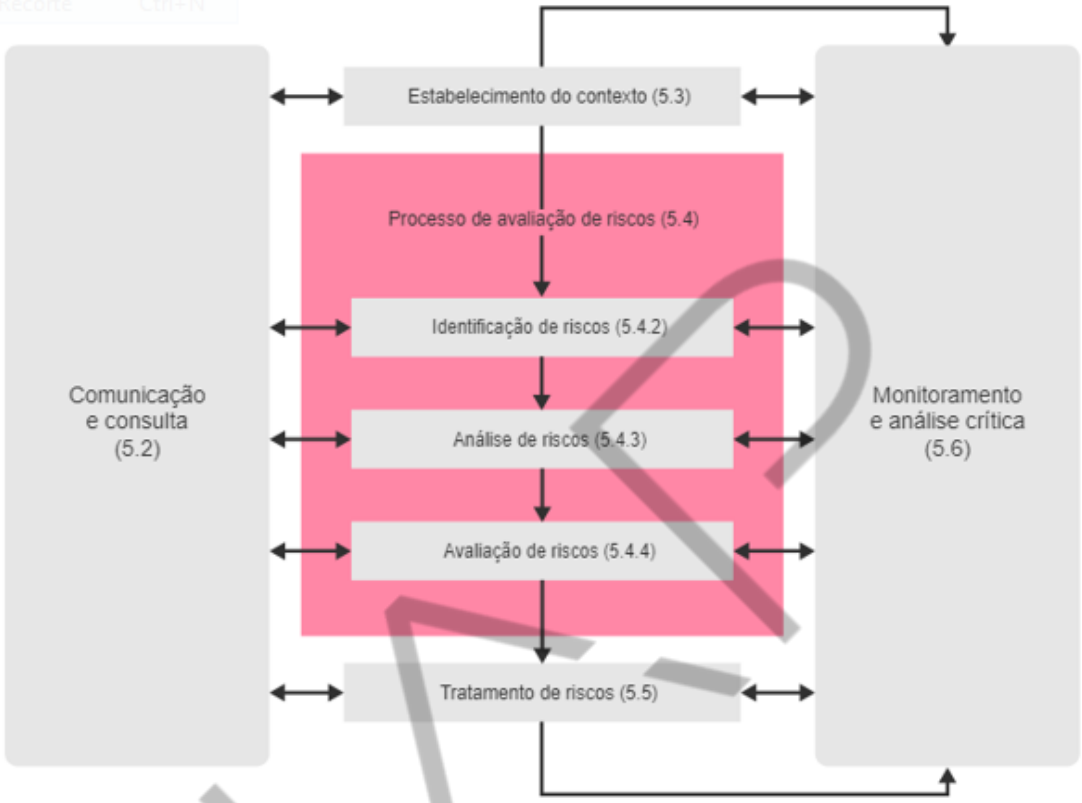

Figura 3.4 – Processo de gestão de riscos
Fonte: ABNT NBR ISO/IEC 31000:2009. Gestão de riscos – Princípios e diretrizes (2018)

Os números indicados nessa figura refletem itens constantes na norma ABNT NBR ISO 31000:2009, iniciando pelo item 5.2, denominado Comunicação e consulta, e finalizando o processo pelo item 5.6, denominado Monitoramento e análise crítica. Esses itens serão descritos de forma sucinta a seguir.

O item denominado **Comunicação e consulta** (constante da norma como item 5.2) visa identificar e realizar o alinhamento das partes interessadas no processo de gestão de risco, sendo essas partes internas e/ou externas à organização. Convém que um plano de comunicação seja estabelecido desde os estágios iniciais, visando assegurar que todos os responsáveis pelo processo compreendam adequadamente as decisões e estratégias adotadas no processo de gestão de riscos.

O item denominado **Estabelecimento do contexto** (constante da norma como item 5.3) visa estabelecer o escopo e os critérios de risco, esse contexto pode

ser interno e/ou externo, devendo ser considerados aspectos como questões ambientais, culturais, sociais, políticas, além dos objetivos da organização. Apesar de esta não ser uma relação exaustiva quanto aos contextos, diversos elementos devem ser considerados para a delimitação do escopo, pois isso tornará o processo de gestão de riscos mais ou menos complexo e/ou completo em relação às necessidades da organização.

O item denominado **Processo de avaliação de riscos** (constante da norma como item 5.4) é composto pelos processos de identificação de riscos (que envolve identificar as fontes de risco, áreas de impactos, eventos, suas causas e consequências potenciais), análise de riscos (que envolve a identificação das causas, as fontes de risco, consequências, sejam estas positivas ou negativas, probabilidade e consequências relacionadas à concretização dos riscos) e avaliação de riscos (que auxilia a tomada de decisões).

O item denominado **Tratamento de riscos** (constante da norma como item 5.5) visa a seleção de uma ou mais opções para modificar os riscos, envolvendo a avaliação do tratamento de riscos já realizado, a decisão dos níveis de risco residual que são toleráveis e, no caso de não serem toleráveis, a definição e implementação de um novo tratamento para os riscos e a respectiva avaliação da eficácia em relação a essa decisão de tratamento.

O item denominado **Monitoramento e análise crítica** (constante da norma como item 5.6) visa garantir que os controles sejam eficazes e eficientes, além de aprimorar o processo de avaliação de riscos por meio da análise de eventos, mudanças, tendências, sucessos, fracassos; assim como potenciais mudanças no contexto interno e externo, considerando que a segurança da informação é um tema dinâmico, isso inclui a identificação de riscos emergentes.

Ainda se espera que todo processo descrito apresente evidências (rastreabilidade) exigidas em processo de auditoria em segurança da informação, considerando que tais evidências também deverão ser protegidas de acordo com as mesmas exigências quanto à disponibilidade, integridade e confidencialidade.

Independentemente das ações previstas e planejadas para o processo de gestão de riscos em segurança da informação, é importante atentar-se que os custos são elementos em geral limitantes para uma completude do processo de

gestão de riscos em segurança da informação, pois o retorno de investimento é algo que precisa ser quantificado (uma vez que esse cálculo nem sempre é fácil de ser obtido ou mesmo realizado), já que alguns desses parâmetros se baseiam em elementos e benefícios intangíveis.

REFERÊNCIAS

ABNT. **ABNT NBR ISO 31000:2018. Gestão de riscos – Diretrizes**. Disponível em: <https://www.abntcatalogo.com.br/norma.aspx?ID=392334>. Acesso em: 01 jul. 2020.