CARTILHA DE RISCO OPERACIONAL

Uso Externo

Outubro/2015

SUMÁRIO

1. Apresentação

A presente **Cartilha de Risco Operacional** é destinada ao público prestador de serviços à BB DTVM e consiste numa coletânea sucinta dos principais conceitos associados ao gerenciamento de risco operacional.

Espera-se que a disseminação do conhecimento sobre o assunto funcione como um **indutor à reflexão e revisão** dos processos operacionais por partes dos agentes prestadores de serviços, com reflexos positivos sobre a mitigação dos riscos operacionais e sobre a qualidade dos serviços prestados.

2. O que é Risco Operacional

2.1 Conceitos

2.2.1 Risco Operacional

Segundo a Resolução 3.380[1], considera-se risco operacional "*a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos*".

Esta definição inclui o risco legal, que é o risco associado à inadequação ou deficiência em contratos firmados pela instituição, bem como a sanções em razão do descumprimento de dispositivos legais e a indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição.

2.2.2. Fatores de Riscos

- **Pessoas** - Relacionam-se à competência, conduta ética e desempenho das suas atribuições;
- **Processos** - Fluxos e etapas do desenvolvimento de produtos e serviços e condução de atividades da organização, definição dos normativos internos e aderência à legislação;
- **Sistemas** - Infra-estrutura e arquitetura de TI, disponibilidade de armazenamento, processamento e rede;
- **Eventos Externos** - Relacionados com as ocorrências do meio ambiente, do ambiente social e do ambiente regulatório do país.

[1] Resolução do Conselho Monetário Nacional, de 29.06.2006.

2.2.3. Categorias de Eventos de Risco Operacional[2].

- **Fraudes Internas** - perdas ocasionadas por atos com intenção de fraudar, apropriar-se indevidamente ou burlar regulamentos, leis ou as políticas da empresa, que envolvam pelo menos uma parte interna, excluindo diversidade/acontecimentos discriminatórios;
- **Fraudes e Roubos Externos** - perdas ocasionadas por atos com intenção de fraudar, apropriar-se indevidamente ou burlar leis, praticados por um terceiro;
- **Demandas trabalhistas e segurança deficiente do local de trabalho** - perdas decorrentes de atos inconsistentes com contratos ou leis trabalhistas, saúde, segurança, pagamento de reclamações por lesões corporais, ou de diversidade/eventos discriminatórios;
- **Práticas inadequadas relativas a clientes, produtos e serviços** - perdas decorrentes de uma falha não-intencional ou negligente para cumprir uma obrigação profissional com clientes específicos (incluindo exigências fiduciárias e de adequação ao perfil do cliente), ou da natureza ou desenho de um produto ou serviço;
- **Danos a ativos físicos próprios ou em uso pela empresa** - prejuízos decorrentes de perdas ou danos aos ativos físicos ocasionados por desastres naturais ou outros acontecimentos;
- **Falhas em sistemas de tecnologia da informação** - perdas decorrentes de falhas em sistema;
- **Falhas na execução, cumprimento de prazos e gerenciamento das atividades** - perdas decorrentes na administração, condução, execução e gerenciamento das atividades vinculadas aos processos internos;
- **Interrupção das atividades** - perdas decorrentes de ruptura nos negócios, ocasionadas pela ausência ou não fornecimento de serviços essenciais, seja de agentes internos ou externos à empresa.

[2] BIS – *Bank for International Settlements* – tradução livre.

2.2.4 Perdas Operacionais

2.2.4.1 Perda Efetiva

A perda efetiva decorre da manifestação de evento de risco operacional que causou perda financeira ou contábil para a empresa, refletindo diretamente no seu resultado.

2.2.4.2 Perda não Efetiva ou Quase Perda

Situação em que os eventos de risco operacional não causaram perda efetiva para a empresa, por conta da intervenção de agente interno ou externo, antes da efetivação da perda.

3. Gerenciamento do Risco Operacional

3.1 Premissas

O risco operacional está presente em todos os processos internos da empresa e pode ser decorrente de falhas operacionais em qualquer etapa destes processos, sejam estas de caráter humano, tecnológico ou de modelagem.

No mercado de prestação de serviços, em especial, entende-se que alguns fatores são essenciais para o sucesso e continuidade de uma empresa, como a qualidade, segurança e agilidade. Assim, a garantia de atendimento destes objetivos depende da eficiência dos processos operacionais e dos controles internos, os quais diminuirão a probabilidade de ocorrência de eventos de risco operacional.

Outro aspecto importante é que todos os níveis hierárquicos da empresa entendam que têm papéis e responsabilidades em relação à gestão do risco operacional em suas atividades para a eficácia na sua gestão.

O adequado gerenciamento do risco operacional está diretamente relacionado ao conhecimento dos processos internos existentes na empresa. Desse modo, a empresa deve manter-se permanentemente atualizada, especialmente naqueles considerados críticos, mantendo seus riscos operacionais identificados, avaliados, monitorados e controlados.

A implementação de controles internos é fundamental para a gestão eficiente do risco operacional. Quando bem definidos, podem auxiliar a empresa a minimizar a probabilidade de incorrer em grandes perdas financeiras, seja por meio da redução na probabilidade de erros humanos, seja na redução das falhas e irregularidades em processos e sistemas.

Dado que entre os fatores de risco existe a possibilidade de ocorrência de **eventos externos** adversos, tais como tumultos, blecautes, inundações, dentre outros, que são alheios à vontade e ao aos controles existentes e podem provocar interrupções drásticas nestes processos, a empresa deve possuir um plano de contingência e continuidade de negócios que possibilite a manutenção das operações em condições mínimas para que as consequências dessa interrupção sejam as menores possíveis.

3.2 Fases de Gestão de Risco Operacional

A estrutura de gerenciamento de risco operacional deve prever as seguintes fases:

- **identificação**: identificar eventos de risco operacional, apontando as áreas de incidência, causas e potenciais impactos financeiros.
- **avaliação**: quantificar a exposição ao risco operacional com o objetivo de avaliar o impacto nos negócios.
- **controle**: registrar o comportamento dos riscos operacionais, limites, indicadores e eventos de perda operacional, bem como implementar mecanismos de forma a garantir que os limites e indicadores de risco operacional permaneçam dentro dos níveis definidos.
- **mitigação**: criar e implementar mecanismos para mitigar o risco operacional, buscando reduzir as perdas.
- **monitoramento: identificar as deficiências do processo de gestão** do risco operacional.

3.3 Ações de Mitigação do Risco Operacional

A identificação de ações mitigadoras está associada, em cada empresa, à forma de condução dos processos internos e ao tipo e nível de controle interno utilizado, entretanto, algumas ações têm caráter genérico e se aplicam a qualquer situação, como por exemplo:

- fator de risco Pessoas: adequado processo de seleção e recrutamento, ações de treinamento, existência de Código de Ética e Normas de Conduta, política adequada de remuneração etc;
- fator de risco Processos: definição e implantação de controles internos; formalização dos procedimentos operacionais etc;
- fator de risco Sistemas: implantação de controles de acesso (físicos e lógicos), instalação de programas antivírus, becape periódico de dados, política de uso de equipamentos móveis, internet e *e-mail* etc;
- fator de risco Eventos Externos: implantação de plano de continuidade de negócios, com definição dos processos críticos.

3.4 Segurança da Informação

Segurança da Informação remete à ideia de que informações ou conhecimentos estão seguros e protegidos contra pessoas que não precisam ou não devam ter acesso a tais dados.

Os riscos de Segurança da Informação (SI) devem ser administrados para assegurar que os objetivos do negócio sejam alcançados e que os eventos indesejados sejam evitados ou detectados e endereçados satisfatoriamente.

No tratamento dos riscos, podem ser considerados como sinalizadores de vulnerabilidades:

- senha exposta ou compartilhada;
- indícios de desrespeito às normas que regem a propriedade intelectual de livros, textos, imagens e outros produtos protegidos por direito autoral;
- informações corporativas descartadas inadequadamente;
- informações corporativas guardadas inadequadamente;
- gavetas e/ou armários abertos ou chaves expostas.

Dentre os controles aplicáveis estão:

- ✓ controle de acesso aos Sistemas – pequeno ou grande portes;
- ✓ gestão de *logs*;
- ✓ restrição ao armazenamento de arquivos indevidos;
- ✓ requerimentos de autenticação de Usuário ;
- ✓ classificação da informação por nível de importância ou criticidade;
- ✓ confirmação de leitura de documentos;
- ✓ procedimentos adequados de descarte de informações (fitilhamento).

3.5 Segurança de Pessoas e Ambientes

Para a segurança física e do ambiente podem servir como sinalizadores de vulnerabilidades:

- pontos de acesso às dependências sem controle ou vigilância;
- inexistência de identificação no acesso de terceiros;
- inexistência de mecanismos de proteção física nas dependências da empresa (equipamentos contra incêndio etc).

Dentre os controles aplicáveis estão:

- ✓ controle de acesso automatizado (crachá),
- ✓ sistema de monitoramento fechado de TV (CFTV),
- ✓ elaboração de Mapa de Riscos de Acidentes do Trabalho[3].

3.6 Ferramentas na Gestão de Risco Operacional

3.6.1 Modelagem de Processos

A Modelagem de Processos é uma das ferramentas que se destaca em meio às opções utilizadas para a gestão do risco operacional. Ela utiliza a padronização nos registros e na documentação para prover uma visão uniforme dos processos operacionais.

O padrão Business *Process Modeling Notation* (BPMN) é um conjunto de objetos gráficos de notação, criado para representar os elementos de um processo, com o objetivo de oferecer suporte à sua condução tanto pelos usuários técnicos quanto pelos usuários de negócios.

[3] O Mapa de Riscos é a representação gráfica dos riscos de acidentes nos diversos locais de trabalho, inerentes ou não ao processo produtivo. O mapa de riscos é elaborado pela CIPA, segundo a NR-5.

Um processo é um grupo de atividades realizadas numa sequência lógica com o objetivo de produzir um bem ou um serviço que tem valor, ou seja, é uma sequência de passos finita que visa definir um conjunto de atividades onde se tem uma entrada, a transformação dessa entrada e uma saída.

O processo pode ser decomposto em partes menores, denominadas atividades (ou processos operacionais). As atividades são compostas por tarefas. As tarefas, por sua vez, não podem ser decompostas, ou seja, representam o último nível de execução.

Na modelagem é possível representar diferentes tipos de atividades, dependendo das características do trabalho que é executado. Cada atividade a ser utilizada no fluxo tem uma representação visual específica.

O BPMN descreve a lógica dos passos de um processo. Com a modelagem é possível ter uma notação gráfica que expressa de forma clara o processo de negócio, mesmo aqueles mais complexos se tornam de fácil compreensão/visualização para intervenientes.

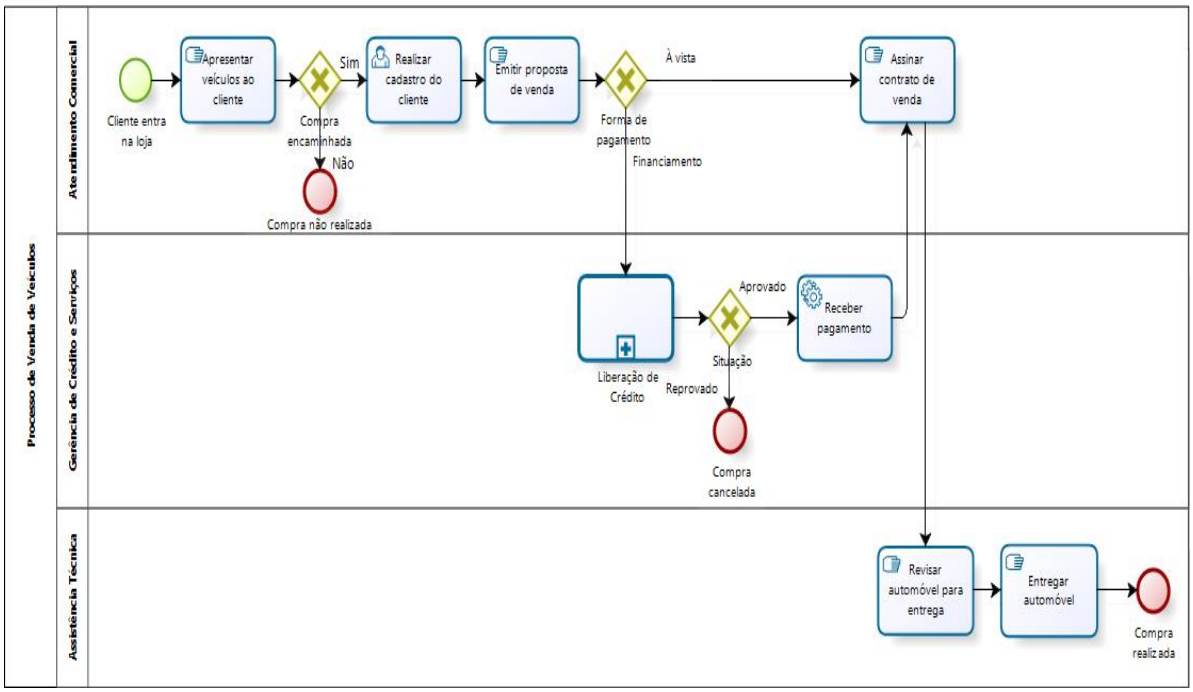
3.6.1 Outras ferramentas

Outras ferramentas que podem ser utilizadas no gerenciamento do risco operacional são:

- *Control Self Assessment* (CSA)
- Seis Sigma
- Gestão da Qualidade Total (GQT)

4. Gráficos

4.1 Exemplo de fluxograma de processo operacional[4]



[4] Exemplo extraído da internet. O fluxograma está baseado no padrão BPMN.

5. Referências Bibliográficas

1. Bank For International Settlement (BIS). *Sound Practices for the Management and Supervision of Operational Risk.*

2. Resolução 3.380, de 29.06.2006, do Conselho Monetário Nacional.

3. MELHORES PRÁTICAS NA GESTÃO DO RISCO OPERACIONAL. Febraban. 2006.

4. Análise das Ferramentas de Auto-Avaliação na Gestão do Risco Operacional. Febraban. 2004.

5. Normativos Internos no Banco do Brasil S.A.