

Definição de Risco Operacional

Riscos Operacionais cobrem as instancias aonde a corretora pode sofrer perdas inerentes direta ou indiretamente a processos internos falhos ou inadequados, atividade de pessoas e sistemas e eventos externos. Os eventos são intrínsecos a todas as atividades da corretora e compreendem vastos e diversos tipos de riscos. Em particular as perdas podem ser provenientes de:

- Falhas significativas e amplas de sistemas e aplicações de TI
- Falha na segurança da informação, incluindo dados corrompidos devido a invasão da rede, violação dos acessos de rede ou falhas na segurança dos sistemas.
- Risco de projeto relacionado a desenvolvimentos críticos de TI.
- Perda de pessoas chaves.
- Erro dos assessores.
- Eventos externos, incluindo falha em sistemas de liquidação.
- Falha ou rompimento de fluxo de processos operacionais.
- Interrupção do negócio devido a eventos naturais ou provocados por ação humana.
- Introdução de novos produtos ou acesso a novos mercados e as consequentes questões de impostos, legais, contabilidade, regulatória, de liquidações e tecnológicas.

Soma-se também à definição de Risco Operacional, os riscos de fraude e de lavagem de dinheiro. Tais perdas podem ainda ser decorrentes de eventos externos à Corretora, no caso de serviços terceirizados.

Outro âmbito do Risco Operacional também existe na forma de Risco Legal, associado tanto à inadequação de contrato com contrapartes, quanto ao descumprimento de dispositivos legais obrigatórios. Neste caso, as perdas podem ocorrer na forma de sanções e multas previstas pela legislação vigente.

Vale ressaltar que a ICAP Brasil considera que todos os tipos de perdas supracitadas podem ser tanto financeiras como de imagem.

Classificação de Evento de Risco Operacional

Um evento de Risco Operacional é entendido como um incidente que resulta em perdas ou impactos decorrentes de erro, falha, deficiência ou inadequação de processos relacionados a risco operacional.

A Corretora contempla em sua gestão de Risco Operacional eventos diretamente e não diretamente mensuráveis como eventos com impacto reputacional, que podem acarretar em perdas financeiras para a Instituição. Ainda que os eventos não diretamente mensuráveis também sejam contemplados na gestão de Risco Operacional da Corretora, deve haver uma distinção no tratamento de tais eventos, devido ao seu caráter intangível.

Desta forma, eventos não diretamente mensuráveis são qualitativamente avaliados pela ICAP Brasil; enquanto que eventos diretamente mensuráveis são avaliados qualitativa e quantitativamente.

Classifica-se evento de Risco Operacional como:

Fraudes Internas

Atos com intenção de fraudar, apropriar-se indevidamente, burlar regulamentos, a lei ou política da Instituição, excluindo diversidade/acontecimentos discriminatórios que envolvam pelo menos uma parte interna. Nessa situação, entre os envolvidos, existe ao menos um indivíduo que pertence ao corpo funcional da Instituição.

Fraudes Externas

Atos intencionais caracterizando fraude, apropriação indevida ou violação de regulamentações, lei ou políticas da Instituição, excluindo eventos relativos à diversidade/discriminação. Nesta situação não há nenhum indivíduo envolvido que pertence ao corpo funcional da Instituição.

Demandas Trabalhistas e Segurança Deficiente do Local de Trabalho

Atos que não correspondem com leis e/ou contratos de serviço, saúde ou segurança, oriundos dos pagamentos relativos a danos pessoais ou eventos relativos à diversidade/discriminação. Nesta categoria incluem-se processos judiciais trabalhistas julgados cujo veredicto impacta diretamente a Instituição.

Práticas Inadequadas Relativas a Clientes, Produtos e Serviços

Não cumprimento, intencional ou não intencional, de uma obrigação com clientes específicos (incluindo requisitos fiduciários e de adequação) ou devido à natureza ou desenho de um produto.

Danos a Ativos Físicos Próprios ou em Uso Pela Instituição

Perdas ou danos de ativos físicos ou intangíveis (incluindo dados) decorrente de eventos internos ou externos, incluindo desastres naturais, atos de terrorismo ou problemas com serviços de utilidade pública.

Danos que Acarretem a Interrupção das Atividades da Instituição

Perdas ou danos de ativos físicos ou intangíveis (incluindo dados) devido a eventos internos ou externos, incluindo desastres naturais, atos de terrorismo ou problemas com serviços de utilidade pública que acarretem na interrupção das atividades da instituição.

Falhas em Sistemas de Tecnologia da Informação

Erros de processamento ou falhas decorrentes de sistemas ou de canais de comunicação que impactam negativamente a Instituição, causando perdas com potencial interrupção de suas atividades.

Falhas na execução, cumprimento de prazos e gerenciamento das atividades na Instituição

Gerenciamento e execução de processos ou processamento deficiente de transações, oriundos de relações com contrapartes e/ou provedores.

Causas de Risco Operacional

As causas de Risco Operacional podem ser segregadas em quatro categorias distintas: pessoas, processos, sistemas e ocorrências externas.

Pessoas

Falhas humanas, intencionais ou não, que podem causar distintas perdas de caráter operacional (seja em função da insuficiência de recursos ou capacitação técnica). Este fator de risco está associado à falta de treinamento, conduta indevida, pouca experiência ou falta de capacitação profissional, e/ou número de funcionários abaixo do necessário, etc. Alguns eventos ocasionados por este fator de risco são: erros gerais com operações (sejam internos ou externos), falhas quando das admissões e/ou demissões, danos ao corpo, saúde e segurança, difamação, discriminação, assédio, ações mal intencionadas como fraudes e negociações escusas, entre outros.

Processos

Potencial interrupção, falha/falta de controle, ou desenho inadequado de processos dentro das linhas de negócio ou em processos de apoio. Este fator de risco está associado à formalização acerca da execução de processos e utilização de

ferramentas, com o intuito de garantir a execução segura das atividades relacionadas à negociação e condução de um negócio, elaboração de produtos, prestação de serviços, ou atividades que suportam as linhas de negócios.

Sistemas

Deficiências relacionadas aos sistemas com baixo desempenho, escolha de sistemas, inadequados, sistemas obsoletos, falhas de comunicação externa, alterações inadequadas nos sistemas. Este fator de risco contempla uma potencial interrupção de comunicação a terceiros.

Dentre as deficiências de sistemas mais comuns estão: tecnologia insuficiente ou obsoleta ao negócio, o uso não autorizado ou inadequado da tecnologia, falhas nos equipamentos, hardware inadequado, invasões por hackers, falha na proteção da rede, vírus de computadores, falhas de programação, etc.

Ocorrências Externas

O Risco Operacional pode ser ocasionado por eventos externos como: atos de vandalismo, desastres naturais, desastres não naturais, terrorismo, mudança na legislação capaz de interromper a atividade da instituição (parcial ou totalmente), fraudes externas, lavagem de dinheiro por parte de terceiros, controle de capital, etc.

Impactos decorrentes de Evento de Risco Operacional

Perdas financeiras

Impacto negativo nas receitas ou nos lucros da Instituição devido a um evento de Risco Operacional.

Impactos Reputacionais

Impacto negativo sobre a imagem da Instituição afetando a reputação da Instituição perante os “stakeholders” (clientes, mercado financeiro, órgãos reguladores, fornecedores, acionistas e demais partes relacionadas).

Impactos Indiretos

Impactos negativos de difícil mensuração financeira ou gastos decorrentes de ações tomadas em função de algum evento ocorrido.

Racional da Estratégia de Risco Operacional

Em conformidade com as boas práticas de mercado, e em atendimento aos regulamentos internos do mercado financeiro brasileiro, a Corretora realiza o gerenciamento de Risco Operacional com base na relação existente entre riscos e controles. Esta estrutura contempla uma gama de controles internos que são praticados por todas as áreas geradoras de riscos da Instituição.

Avaliações periódicas são realizadas sobre os processos e controles existentes, com o intuito de identificar novos riscos inerentes aos processos e avaliar a eficácia dos controles em uso. Com base nos resultados das avaliações periódicas, são definidos os planos de ação, para mitigar os riscos identificados, as necessidades de implantação de novos controles, ou aprimoramento dos controles existentes.

O processo de Gerenciamento de Risco Operacional tem como objetivo: identificar processos, descrever objetivos, identificar riscos, propor controles, avaliar riscos, responder a eventos de riscos e monitorar riscos relacionados às falhas em processos internos, em sistemas e pessoas que representem perda financeira, ou a possibilidade de perda à Instituição, incluindo o Plano de Continuidade de Negócios.

O Plano de Continuidade de Negócios da ICAP Brasil prevê ações paliativas para remediar situações de falhas em processos internos causadas por danos inesperados, permitindo à Corretora dar rápida continuidade às suas atividades rotineiras minimizando os impactos decorrentes de tais danos. Atualmente, o Plano de Continuidade de Negócios da Corretora é definido e aprovado pelo Comitê Executivo com devido suporte do Comitê de Gestão de Riscos com revisões periódicas semestrais. Para maior detalhamento consultar o documento “Plano de Gerenciamento de Continuidade”.

É importante mencionar que a definição descrita acima está relacionada a risco negativo, mas tal atividade operacional pode contemplar o risco positivo, ou seja, o risco sob uma perspectiva de oportunidade.

Um adequado processo de gestão de riscos facilita a realização de uma alocação de capital em conformidade com os requisitos estabelecidos pelos princípios de Basiléia II.

Identificação do Risco Operacional

O processo de identificação do Risco Operacional é feito inicialmente a partir do agrupamento das atividades da Instituição em processos de negócios que contemplam os sub-processos. Desta forma, é possível realizar a identificação dos processos de negócios, procedimentos internos e respectivos objetivos. É de responsabilidade de cada área ou departamento descrever e manter atualizada a descrição de suas atividades, incluindo sistemas, pessoas, ativos físicos, dentre outros.

Uma vez estabelecidos os objetivos dos processos, os riscos operacionais aos quais a Corretora está exposta são identificados com a utilização das técnicas descritas a seguir:

- Auto-avaliação – “Risk Control Self Assessment (RCSA)”: visão dos Gerentes dos Departamentos e dos demais envolvidos quanto à execução dos processos considerando os objetivos previamente definidos de cada processo, visando agregar a experiência e conhecimento destes na revisão. Anualmente é feita com auxílio da área de risco o mapeamento e análise dos riscos e controles internos da Corretora. Com base nesta análise, é possível identificar a necessidade de novos controles e/ou ajustes nos controles já existentes.
- Análise do fluxograma do processo: combinação das informações de entrada, atividades, responsabilidades e saídas que se interligam para constituir o processo. A análise destas combinações é realizada com o objetivo de identificar os riscos operacionais inerentes aos componentes do processo.
- Análise do escopo regulatório e operacional: análise dos normativos referentes ao(s) processo(s) ora analisados a fim de constituir os objetivos de controle a serem cumpridos (sob demanda).
- Base de Perdas Internas: identificação das tendências, frequências e causas dos eventos de Risco Operacional; categorização das principais causas dos eventos de perdas operacionais incorridos e identificação de melhorias necessárias no ambiente de controles internos da Corretora.

Estas técnicas devem ser aplicadas constantemente pela Corretora, de acordo com os eventos observados, com o intuito de identificar os eventos de Risco Operacional, suas causas, impactos e controles necessários para mitigar tais riscos. É de responsabilidade da área de Risco a definição dos riscos, impactos e controles ou melhorias a serem implantadas.

Cabe às respectivas áreas a responsabilidade por implantar os controles e/ou melhorias sugeridas pela área de Risco para mitigar os riscos identificados em cada área.

A área de Risco é, por sua vez, responsável pelo monitoramento quanto ao cumprimento de tais controles implantados pelas áreas cabíveis.

Monitoramento do Risco Operacional

O monitoramento do Risco Operacional da Corretora é realizado inicialmente através da identificação e mapeamento dos riscos e controles internos da Instituição (RCSA), além do acompanhamento de indicadores de risco inerentes do mercado (Key Risk Indicators - KRI). Estes indicadores fornecem uma importante integração entre as operações rotineiras da Corretora e o Gerenciamento do Risco Operacional (GRO).

Além do acompanhamento dos KRI, a Corretora também monitora seu Risco Operacional a partir de um relatório de monitoramento de perdas diretas e indiretas. As perdas diretas são ocasionadas por quaisquer falhas operacionais, e incorrem em perdas efetivas e mensuráveis. As perdas indiretas são aquelas relacionadas a custos de oportunidade e de perdas não diretamente precificáveis.

O monitoramento periódico destes indicadores está a cargo dos Gerentes da Corretora, que são incumbidos de comunicar tempestivamente à Diretoria de Risco quaisquer oscilações significativas. Cabe à Diretoria de Risco tomar providências consistentes ao problema em questão.

Controle do Risco Operacional

Para avaliar o controle do Risco Operacional, a Corretora é submetida a revisões independentes de auditoria que identifica e analisa as atividades de controle existentes a fim de monitorar a adequação do ambiente de controles internos e sua respectiva eficácia operacional.

Este monitoramento é suportado por avaliações mensais qualitativas e quantitativas, realizadas pela área de Risco, com devido reportes das perdas observadas e respectivas áreas.

Avaliação e Gerenciamento do Risco Operacional

A identificação do evento e classificação do risco operacional deve ser feita pelo Gerente da área responsável pela atividade ou processo causador do evento, contando com o suporte de outras áreas ou departamentos envolvidos, caso necessário.

Após a identificação inicial do evento, análise e classificação dos riscos inerentes, os Gerentes das áreas envolvidas discutem e sugerem as ações remediadoras a serem adotadas. Os Gerentes de cada área devem elaborar relatório contendo os eventos identificados em suas áreas, classificação do risco e sugestão de ações remediadoras. Tal relatório deve ser submetido ao Comitê de Gestão de Riscos para aprovação da classificação do risco e das ações preventivas e/ou corretivas, sempre que necessário.