ITAÚ UNIBANCO HOLDING S.A.

CNPJ 60.872.504/0001-23 Companhia Aberta NIRE 35300010230

RELATÓRIO DE ACESSO PÚBLICO - GERENCIAMENTO INTEGRADO DE RISCO OPERACIONAL E CONTROLES INTERNOS

OBJETIVO

Estabelecer as diretrizes e responsabilidades associadas ao gerenciamento de risco operacional e controles internos, observando as boas práticas de mercado, normas e regulamentações aplicáveis.

INTRODUÇÃO

Todos somos gestores de risco. Riscos são elementos inerentes a todas as atividades da Instituição e fazem parte do dia a dia dos colaboradores, estando presentes nos processos, produtos e serviços existentes ou novos, inclusive nos serviços terceirizados. Gerenciar adequadamente os riscos operacionais é condição essencial para a sustentabilidade dos negócios do Itaú Unibanco.

O Banco Central do Brasil define risco operacional como “a possibilidade da ocorrência de perdas resultantes de evento externos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas. Inclui também o risco legal associado à inadequação ou deficiência em contratos firmados pela Instituição, às sanções em razão de descumprimento de dispositivos legais e às indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela Instituição. ”

O gerenciamento adequado do risco operacional pressupõe a identificação dos riscos inerentes às atividades, projetos, produtos ou serviços e a sua priorização, em função do nível de criticidade (importância), levando-se em conta seus impactos nos objetivos do processo ou organização. Uma vez priorizados os riscos, são tomadas medidas de resposta, ou seja, ações que enderecem cada um dos riscos identificados, de modo a enquadrá-los em patamares aceitáveis de exposição. Tais ações podem contemplar a implantação de controles preventivos, a fim de reduzir a possibilidade de materialização do risco, ou envolver controles direcionados à detecção de materialização. Pode haver a decisão de compartilhar um risco, transferindo a atividade de forma parcial ou total, como a terceirização da atividade, por exemplo. Os riscos mencionados podem também ser evitados, simplesmente optando-se pela descontinuidade da atividade geradora do risco, ou assumidos, caso em que a decisão é a de não adotar medidas adicionais de controle em relação às já existentes

DIRETRIZES

O Conselho de Administração aprova as diretrizes, estratégias e políticas referentes ao risco operacional e controles internos, garantindo que haja claro entendimento dos papéis e responsabilidades para todos os níveis do conglomerado.

A seguir são definidas as diretrizes específicas relacionadas à gestão do risco operacional e controles internos

Modelo de gerenciamento de riscos operacionais

O Itaú Unibanco adota a estratégia das três linhas de defesa para operacionalizar sua estrutura de gerenciamento de riscos.

Identificação dos riscos operacionais

Os riscos operacionais que podem influenciar o cumprimento dos objetivos estratégicos e operacionais definidos pelo Conglomerado devem ser continuamente identificados e atualizados. O escopo da identificação contempla os riscos operacionais inerentes às atividades do Conglomerado, aos produtos e serviços existentes ou novos, inclusive nos serviços terceirizados.

A identificação de riscos pode ocorrer a qualquer momento, no desenho de um novo processo, projeto ou produto, bem como durante sua existência. Para isso, deve-se avaliar o risco inerente, ou seja, desconsiderar do contexto a existência de qualquer atividade de controle, avaliando quais falhas o escopo da identificação do risco está sujeito e que, portanto, poderiam afetar o resultado planejado (objetivos).

A exposição a eventos de riscos operacionais raros e de alta severidade, porém considerados plausíveis, é avaliada por meio da criação de cenários, fornecendo informações sobre o risco potencial, gerando estimativas de perdas e considerando, quando necessário, o impacto da ocorrência simultânea de múltiplos eventos de risco operacional.

Priorização dos riscos operacionais
Os riscos operacionais identificados são priorizados em função do seu nível de impacto na Diretoria e/ou no Conglomerado. Para auxiliar na adequada avaliação de impacto, é importante considerar as diversas possibilidades de impacto e sua abrangência, como por exemplo:

- Financeiro: avaliar a representatividade do impacto financeiro que a exposição ao risco operacional pode gerar no negócio e/ou na Organização. Riscos que possam levar a erros significativos nas demonstrações contábeis são classificados como Lei Sarbanes-Oxley (SOX).
- Imagem/Reputação: avaliar a possível repercussão negativa nas mídias nacionais e internacionais (visibilidade e divulgação), bem como os danos na marca e sua possibilidade de reversão.
- Legal/Regulatório: avaliar as possibilidades de gerar descumprimento regulatório, assim como a possibilidade de acarretar multas, advertências, fiscalizações, processos administrativos ou perdas de licenças de operação.
- Clientes: avaliar o volume de clientes impactados, as segmentações ou canais de distribuição envolvidos.

Resposta ao risco operacional
Responder ao risco operacional significa definir qual será a ação adotada em relação ao risco identificado. Algumas ações possíveis:

- Mitigar: são estabelecidas ações que reduzem a probabilidade do risco operacional se materializar no processo ou ações que diminuem o impacto produzido.
- Compartilhar: são estabelecidas ações que visam reduzir o impacto e/ou a probabilidade de ocorrência do risco através da transferência ou, em alguns casos, do compartilhamento de uma parte do risco. Pode envolver a terceirização de atividades ou a contratação de seguro, por exemplo.
- Evitar: são estabelecidas ações que eliminam a probabilidade do risco se materializar. Pode envolver a descontinuidade da atividade/operação sujeita ao risco.
- Assumir: nenhuma ação é estabelecida para reduzir o impacto e/ou a probabilidade de ocorrência do risco. Neste caso, deve ser observada a governança de assunção de risco.

Ações que demandam desenvolvimento tecnológico devem ser validadas, pela segunda linha de defesa, quanto à sua classificação de risco e devem estar associados a apontamentos de risco, apontamento de Compliance e/ou apontamentos de Auditoria Interna.

Monitoramento do nível de exposição aos riscos operacionais

Exposição aos riscos operacionais relevantes deve ser monitorada pela Organização por meio de indicadores de risco, de acordo com os níveis de tolerância estabelecidos.

Os apontamentos de Risco Operacional, Auditorias Interna e Externa devem ser executados e, periodicamente, acompanhados pela primeira linha de defesa.

A segunda linha de defesa deve validar a implantação dos planos de ação dos apontamentos de risco operacional de nível moderado e elevado, de acordo com a política de gerenciamento de apontamento de risco operacional, bem como os pontos de auditoria interna moderados, conforme políticas internas.

Reporte dos riscos operacionais

Os apontamentos de nível de risco elevado identificados pelas linhas de defesa, reguladores ou auditoria externa devem ser comunicados às comissões superiores, aos executivos das unidades de negócio, aos Chief Risk Officers (CROs), ao Comitê de Auditoria, ao Conselho de Administração e ao Comitê de Riscos. A comunicação de apontamentos da Auditoria Interna deve obedecer a políticas interna.

Divulgação das ações de gerenciamento dos riscos operacionais

A descrição da estrutura de gerenciamento de Risco Operacional é disponibilizada por meio de relatório de acesso público, aprovado pelo Conselho de Administração. Adicionalmente, um resumo da descrição da estrutura de gerenciamento de Risco Operacional e Controles Internos é publicado em conjunto com as demonstrações contábeis.

As decisões, políticas e estratégias definidas para o gerenciamento do risco operacional das unidades internacionais são divulgadas aos *Chief Risk Officers (CROs)*.

Gerenciamento da base de perdas de riscos operacionais

Todas as áreas do Itaú Unibanco estão expostas a eventos de risco operacional, sendo responsabilidade das Unidades de Negócio (primeira linha de defesa) a identificação de tais eventos e os valores de perda associados, para compor a Base de Dados de Perdas Operacionais (BDPO).

Despesas e provisões relacionadas a eventos de risco operacional que impactem as contas de resultado do Banco devem ser reportadas à BDPO.

Alocação de capital para risco operacional

O conglomerado utiliza a Abordagem Padronizada Alternativa (ASA) no cálculo e alocação do capital regulatório para risco operacional. Adicionalmente, é efetuado o cálculo e a alocação de capital econômico para risco operacional (ICAAP).

A adequação do nível de Patrimônio de Referência (PR), com relação ao risco operacional assumido pelo Conglomerado, deve ser periodicamente monitorado.

PRINCIPAIS PAPÉIS E ATRIBUIÇÕES
Conselho de Administração:
- Aprovar as diretrizes, estratégias e políticas referentes ao risco operacional e controles internos, garantindo que haja claro entendimento dos papéis e responsabilidades para todos os níveis do conglomerado.

Comitê de Auditoria:
- Supervisionar os processos de controles internos e de administração de risco.

Comissão Superior de Risco Operacional:
- Conhecer os riscos dos processos e negócios do Itaú Unibanco, definir as diretrizes para gestão dos riscos operacionais e avaliar os resultados dos trabalhos realizados.

Comitê de Compliance e Risco Operacional:
- Acompanhar e promover o desenvolvimento e implementação das diretrizes aprovadas e definidas pela CSRO em cada Área Executiva, discutir os principais riscos existentes e potenciais das Áreas de Negócio, bem como os planos de ação propostos para mitigação.

Comitê de Interno de Risco Operacional:
- Discutir assuntos relativos a Riscos Operacionais e Controles Internos de cada Unidade de Negócio, que serão levados a uma alçada superior de decisão nos Comitês de Compliance e Risco Operacional.

Chief Risk Officer:
- Responsável pela gestão de risco operacional na instituição.

Controles Internos e Risco Operacional:
Inserida na segunda linha de defesa, a estrutura é representada pelos superintendentes que atuam como Oficiais de Controles Internos e Riscos (OCIRs) e, em conjunto com suas equipes, são responsáveis por:
Apoiar a primeira linha de defesa na observação de suas responsabilidades diretas.

- Desenvolver e disponibilizar as metodologias, ferramentas, sistemas, infraestrutura e governança necessárias para suportar o gerenciamento integrado de Risco Operacional e Controles Internos nas atividades do conglomerado e terceirizadas relevantes;
- Coordenar as atividades de Risco Operacional e Controles Internos junto às áreas de Negócio e Suporte, sendo independente no exercício de suas funções e possuindo comunicação direta com qualquer administrador ou colaborador, bem como acesso a quaisquer informações necessárias no âmbito de suas responsabilidades. Por esse motivo, é vedada a essa área realizar a gestão de qualquer negócio que possa comprometer a sua independência.

Áreas de Negócio/Suporte:

- Responsáveis primárias por identificar, priorizar, responder ao risco, monitorar e reportar os eventos de risco operacional que podem influenciar o cumprimento dos objetivos estratégicos e operacionais definidos.

Auditoria Interna:

- Verificar, de forma independente e periódica, a adequação dos processos e procedimentos de identificação e gerenciamento dos riscos, conforme as diretrizes estabelecidas nas políticas internas.

Aprovado pelo Conselho de Administração de 14/12/2018.