ITAÚ UNIBANCO HOLDING S.A.

CNPJ 60.872.504/0001-23 Companhia Aberta NIRE 35300010230

RELATÓRIO DE ACESSO PÚBLICO – POLÍTICA DE GERENCIAMENTO INTEGRADO DE RISCO OPERACIONAL E CONTROLES INTERNOS

1. OBJETIVO

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

2. PÚBLICO-ALVO

Todos os colaboradores do Itaú Unibanco *Holding* e suas empresas controladas no Brasil e no exterior.

3. INTRODUÇÃO

Riscos estão presentes em todas as atividades exercidas na Instituição, inclusive nos serviços terceirizados, e é necessário gerenciá-los. Todos os colaboradores devem exercer o papel de gestor de risco, de acordo com suas funções e atribuições, cumprindo as regras estabelecidas e mantendo-se atentos a mudanças que impactem adversamente os negócios da Instituição.

O Conselho Monetário Nacional, através da Resolução 4.557 de 23 de fevereiro de 2017, define risco operacional como “a possibilidade da ocorrência de perdas resultantes de eventos externos ou de falhas, deficiências ou inadequação de processos internos, pessoas ou sistemas”, incluindo o risco legal associado às inadequações ou deficiências 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 risco operacional, diferentemente de grande parte dos riscos aplicáveis ao setor financeiro, não é tomado em contrapartida a uma recompensa esperada, mas existe no curso natural das atividades corporativas.

O gerenciamento adequado do risco operacional pressupõe o entendimento dos processos existentes na Organização e 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 dos processos ou da Organização. Uma vez priorizados os riscos, são adotadas medidas de resposta, ou seja, ações para mitigação, 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 da materialização. Também é possível compartilhar um risco, transferindo-o de forma parcial ou total, por exemplo, com a contratação de um seguro. Os riscos mencionados podem também ser evitados, simplesmente optando-se pela descontinuidade da atividade geradora do risco, ou assumidos, quando a decisão é pela não adoção de medidas de controle em relação às já existentes.

4. DIRETRIZES

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

4.1. Modelo de gerenciamento de riscos operacionais

Para gerenciar adequadamente os seus riscos, inclusive os operacionais, o Itaú Unibanco utiliza a estratégia das Linhas, descrita em política interna.

4.2. Identificação dos riscos operacionais

A identificação de riscos operacionais inerentes às atividades do Conglomerado deve ser realizada a qualquer momento em produtos e serviços existentes; no desenho de um novo processo, projeto ou produto; em atividades realizadas internamente ou terceirizadas; e durante toda a existência do produto ou serviço, de forma a garantir a avaliação contínua de fatores internos e externos que possam afetar adversamente o Conglomerado e sua respectiva mitigação.

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

4.3. Priorização dos riscos operacionais

Os riscos operacionais identificados são priorizados em função da mensuração do seu nível de impacto nos objetivos do Conglomerado. Para auxiliar na adequada avaliação, é importante considerar as diversas possibilidades de impacto e sua abrangência:

- Relação com Clientes: volume de clientes impactados, as segmentações ou canais de distribuição envolvidos.
- Reputacional: repercussão negativa nas mídias nacionais e internacionais (visibilidade e divulgação), bem como os danos na marca e sua possibilidade de reversão.
- Regulatório: descumprimento regulatório, multas, advertências, sanções, processos administrativos ou perdas de licenças de operação.
- Legal: descumprimento de cláusulas contratuais firmadas com terceiros que possam acarretar discussões judiciais.
- Financeiro: representatividade do impacto financeiro que pode ocorrer no negócio e/ou na Organização, em decorrência da exposição ao risco operacional. Riscos que possam levar a erros significativos nas demonstrações contábeis são classificados de acordo com a Lei *Sarbanes-Oxley* (SOx).
- Social, Ambiental e Climático: impacto social, ambiental ou climático por falha de processo que possa afetar a Organização e suas entidades controladas na relação com seus clientes, fornecedores e prestadores de serviço, a sociedade e/ou o meio ambiente.

4.4. Resposta ao risco operacional

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

- Mitigar: são estabelecidos mecanismos ou controles que visam a redução do impacto e/ou a probabilidade de o risco operacional materializar-se no processo ou ações que diminuem o impacto produzido.
- Compartilhar: transferência ou compartilhamento de parte do risco, por exemplo, a contratação de seguro.
- Evitar: 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 descrita em procedimento interno.

4.5. Monitoramento do nível de exposição aos riscos operacionais

A exposição ao risco operacional deve ser monitorada pela Organização por meio de indicadores de risco, de acordo com os níveis de tolerância estabelecidos.

Quando for observada tendência de deterioração dos indicadores de risco deve ser registrado apontamento de risco (ARI) ou vínculo a apontamento existente para tratamento da causa raiz pela primeira linha, com nível de risco adequado à exposição. Para mais informações, deve-se consultar o manual “Indicadores de Riscos”, sob gestão da DRO.

Vale ressaltar, que os times Dedicados de Risco Operacional devem validar a implantação dos planos de ação dos Apontamentos de Risco de nível moderado e elevado com origem de Risco Operacional, inclusive os oriundos de indicadores desenquadrados. As regras e responsabilidades relacionadas aos apontamentos estão descritas em procedimento interno

4.6. Reporte dos riscos operacionais

Os Apontamentos de Risco podem ser identificados pelas 1ª, 2ª e 3ª Linhas, órgãos reguladores ou auditoria externa e devem ser comunicados conforme nível de risco:

- Elevado: enviar para Membros do Comitê Executivo do negócio, ao Chief Risk Officer (CRO), ao Head de Auditoria Interna, aos diretores de Risco Operacional, de Auditoria Interna e de Compliance, ao diretor de negócio e ao Comitê de Auditoria, este último, órgão assessoramento e consultoria do Conselho de Administração do Conglomerado. O reporte dos apontamentos de Risco Operacional Elevado das Unidades Internacionais é realizado nos fóruns competentes de cada Unidade.
- Moderado: enviar para área owner e gestores de plano de ação.
- Baixo possui classificação de risco avaliado pela 2ª Linha e o acompanhamento das próximas etapas são de responsabilidade da 1ª Linha, com autonomia para reportar evolução e status em colegiado de risco.

Em adição, os resultados dos trabalhos de Risco Operacional que avaliam os sistemas de controles internos classificam os ambientes de controle em Adequado, Moderado (+), Moderado (-) ou Insuficiente e devem ser comunicados para:

- Se o resultado for Moderado(+) ou Adequado: Superintendente e diretor de Negócio, superintendentes de Risco Operacional, Compliance e Auditoria Interna.
- Se o resultado for Moderado(-): Acrescenta-se a lista acima os Membros do Comitê Executivo de Negócio, o Comitê de Auditoria, os diretores de Risco Operacional e de Compliance Corporativo, o diretor executivo e diretores da Auditoria Interna.
- Em caso de resultado Insuficiente: Acrescenta-se a lista acima o *Chief Risk Officer* (CRO).

Para o reporte regular e acompanhamento dos sistemas de controles internos e estrutura de gerenciamento de risco operacional, também há a realização periódica de Comitês e Colegiados, sendo eles, Comitê de Gestão de Risco e Capital, CSRO, Comitê de Auditoria com Risco Operacional e Comitê de Compliance e Risco Operacional. Para mais detalhes, como frequência, lista de participantes obrigatórios e escopo, consultar procedimento interno.

4.7. Divulgação das ações de gerenciamento dos riscos operacionais

A descrição da estrutura de gerenciamento de Risco Operacional, bem como a avaliação sobre a adequação e efetividade dos sistemas de controles internos, é disponibilizada por meio de relatório revisado e aprovado pelo Comitê de Auditoria, órgão estatutário que se reporta ao Conselho de Administração, e permanece, pelo prazo normativo, à disposição do Banco Central do Brasil e da Superintendência de Seguros Privados. 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)* locais.

4.8. 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 Operacionais (primeira linha) 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 do Conglomerado devem ser reportadas na BDPO.

4.9. 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), sendo um dos insumos os cenários de risco operacional, que têm como objetivo a mensuração da exposição financeira, considerando a severidade e probabilidade de ocorrências de eventos de perdas operacionais. Para mais detalhes, consultar procedimento interno.

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

5. PRINCIPAIS PAPÉIS E ATRIBUIÇÕES

Conselho de Administração – CA:

- 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 Gestão de Risco e de Capital – CGRC:

- Apoiar o Conselho de Administração no desempenho de suas responsabilidades relativas à gestão de riscos e de capital do Conglomerado, submetendo relatórios e recomendações sobre estes temas à deliberação do Conselho de Administração.

Comitê de Gestão de Risco e de Capital Seguridade – CGRC–S:

- Apoiar o Conselho de Administração no desempenho de suas responsabilidades relativas à gestão de riscos e de seguridade do Conglomerado, através da avaliação periódica da efetividade da estrutura de gerenciamento de risco, do plano de negócio do Conglomerado e seu apetite de risco; e auxílio na tomada de decisão submetendo relatórios e recomendações à deliberação do Conselho de Administração.

Comitê de Auditoria – CAUD:
De acordo com seu Regulamento Interno, compete ao Comitê de Auditoria supervisionar:
- Os processos de controles internos e da administração de risco;
- As atividades da auditoria interna;
- As atividades das empresas de auditoria independente do Conglomerado;
- Os relatórios e recomendações para deliberação do Conselho de Administração.

Comissão Superior de Risco Operacional – CSRO:
- 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 sobre o funcionamento do Sistema Itaú Unibanco de Controles Internos e *Compliance.*

Comitê de Compliance e Risco Operacional – CCRO:
- Acompanhar e promover nas áreas executivas do Conglomerado, o desenvolvimento e implementação das diretrizes aprovadas e definidas pela CSRO. Subsidiar a CSRO com os principais assuntos que requerem uma alçada superior de discussão. Discutir os principais riscos das Áreas de Negócio e os planos de ação propostos para mitigação dos riscos.

***Chief Risk Officer* (CRO):**
- Responsável pela gestão de riscos na Instituição.
As responsabilidades dos CROs Local e Regional nas Unidades internacionais estão descritas em procedimento interno.

Diretoria de Risco Operacional:
Inserida na segunda linha, com o papel Dedicado de Risco Operacional, garante a atuação e integridade dos Sistemas de Controles Internos de forma independente, sendo responsáveis por:
- Apoiar a primeira linha na gestão dos riscos operacionais associados à suas atividades
- 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, com comunicação direta com qualquer administrador ou colaborador, e acesso a quaisquer informações necessárias no âmbito de suas responsabilidades. Por esse motivo, é vedada a essa área realizar a gestão de qualquer negócio ou atividade que possa comprometer a sua independência.
- Comunicar os apontamentos (ARIs) de riscos moderado e elevado as alçadas, públicos e fóruns competentes.

Áreas de Negócio/Suporte e Comunidade:
- Responsáveis primários por identificar, priorizar, responder ao risco, monitorar e reportar os eventos de risco operacional, que podem impactar adversamente o cumprimento dos objetivos estratégicos e operacionais definidos.
- Alguns escopos bem definidos e de acordo com estágio de maturidade na gestão de riscos, como Compliance Corporativo e Prevenção a Fraudes, atuam com responsabilidade de segunda linha para seus respectivos escopos, descrita no item acima.
- Os Executivos da área de negócio devem apresentar diagnóstico de eventos de indisponibilidade relevantes que gerem impactos significativos em nossos clientes, no sistema financeiro e/ou no mercado.

Auditoria Interna:
- Verificar, de forma independente e periódica, a adequação dos processos e procedimentos de identificação e gerenciamento dos riscos, conforme diretrizes estabelecidas em política interna.

6. GLOSSÁRIO

Ambiente de controle: representa o conjunto de políticas, processos, procedimentos, pessoas e sistemas utilizados pelo Conglomerado para gerenciar sua exposição ao risco operacional inerente à complexidade, diversidade, frequência e volume de suas operações.

Apontamento de Risco: é o registro, no Conglomerado, das falhas operacionais identificadas e situações não previstas de risco em potencial.

Área owner: é a área que tem maior capacidade de mobilizar a organização para mitigar o risco.

Atividade terceirizada: prestação de serviços por empresa especializada contratada para realização de quaisquer atividades da contratante.

Causa: motivo que levou (ou pode levar) o risco operacional a se materializar. Representa a origem do problema e pode ser de natureza organizacional, comportamental, sistêmica, processual ou externa. Os eventos de risco operacional podem ter uma ou mais causas associadas.

Controle: atividades realizadas com o objetivo de reduzir, a níveis aceitáveis, a exposição aos riscos que podem impactar os objetivos de uma organização. As atividades de controle são realizadas pelas áreas de negócio/suporte em todos os níveis da Organização e podem ser detectivas ou preventivas e contemplar atividades manuais ou automatizadas.

Controle detectivo: controle executado com o objetivo de detectar a materialização de um determinado risco, permitindo a redução de seu impacto ou a remediação de suas consequências. É de natureza reativa.

Controle preventivo: controle executado com o objetivo de reduzir a probabilidade ou prevenir a materialização de um determinado risco. É de natureza proativa.

Evento de risco operacional: concretização do risco operacional. São situações que, quando materializadas, causam consequências reais em processos de negócio ou suporte e que diferem dos resultados esperados, podendo ter um impacto direto (exemplo: perdas financeiras) ou indireto (exemplos: custo de oportunidade e danos à reputação/imagem). Para fins de categorização, o Itaú Unibanco utiliza as mesmas definições adotadas pelo Comitê de Basileia e pelo Banco Central do Brasil.

Exposição ao risco: volumetria financeira que representa a exposição às perdas operacionais inesperadas associadas às atividades do Conglomerado.

Falhas: situações em que o risco já foi materializado devido a sistemas inadequados, má administração, controles inefetivos, falha humana ou fraude interna/externa, que podem resultar ou não em perda financeira.

ICAAP: Processo Interno de Avaliação da Adequação de Capital.

Impacto (consequência): montante da perda derivado do risco operacional resultante de custo direto, ressarcimentos a terceiros, indenizações, restituição, despesas judiciais, multas legais, perda de recurso, aumento de passivos e redução do valor de ativos.

Materialização do Risco: circunstância na qual o risco deixa de ser uma incerteza, transformando-se em situação com efeito adverso e consequências não desejadas.

Risco inerente: risco existente em razão do tipo ou natureza do negócio, área, produto, processo, projeto ou sistema novo ou existente, ao qual se está exposto independentemente da estrutura de controles ou outros fatores atenuantes implementados. É o risco bruto ou risco antes dos controles estarem implementados.

Risco residual: parcela do risco inerente que permanece exposta após considerar os controles e ações mitigadoras existentes.

Aprovado pelo Conselho de Administração de outubro de 2022.