OVA

Visão geral do gerenciamento de riscos da instituição

ouribank

Sumário

ouribank

OVA: Visão geral do gerenciamento de riscos da instituição

(a) A interação entre o modelo de negócios e o perfil de riscos da instituição, e entre esse perfil e o nível de apetite por risco estabelecido pelo CA. A descrição deve englobar os principais riscos relacionados ao modelo de negócios.

O modelo de negócios do Ouribank consiste na busca permanente do aprimoramento das suas atividades, oferecendo soluções completas, seguras e ágeis, com foco no atendimento personalizado com excelência como chave para o crescimento de forma rentável, recorrente e perene, reconhecendo a importância do gerenciamento de riscos para o atingimento de seus objetivos estratégicos, além de contribuir para o fortalecimento da governança e do ambiente de controle interno.

A declaração de apetite por riscos (*RAS- Risk Appetite Statement)* contém os tipos de riscos e os respectivos níveis que o Ouribank está disposto a assumir, bem como a capacidade de gerenciar os riscos de forma efetiva e prudente, frente às condições de competitividade e ao ambiente regulatório.

A estrutura de gerenciamento de riscos é parte integrante da governança corporativa do Ouribank, que busca avaliar e administrar, de forma adequada, a exposição de seus riscos inerentes e residuais, bem como contribuir na criação de um equilíbrio entre as tomadas de decisão das áreas de negócio, e a respectiva responsabilidade dessas pela gestão dos riscos inerentes às decisões.

O Ouribank realiza a supervisão dos riscos inerentes e residuais às suas atividades, incluindo os riscos financeiros (Risco de Mercado, Risco de Crédito e Risco de Liquidez) e os riscos não financeiros (Risco de Lavagem de Dinheiro e Financiamento ao Terrorismo, Risco no Relacionamento com Cliente e Usuários, Risco Operacional, Risco de *Compliance*, Risco Socioambiental, Risco de Tecnologia da Informação e Risco de Reputação).

(b) Governança do gerenciamento de riscos: responsabilidades atribuídas ao pessoal da instituição em seus diversos níveis (formas de controle, delegação de autoridade, divisão de responsabilidades por tipo de risco e por unidade de negócio, entre outros), e o relacionamento entre as instâncias de governança (CA, diretoria, comitês de assessoramento do CA, unidades responsáveis pela função de conformidade e pelo gerenciamento de riscos, auditoria interna, entre outros).

A atividade de Gerenciamento Integrado de Riscos e Capital (GIR) é realizada de forma centralizada e por unidade específica, em conformidade com as regulamentações vigentes.

O diretor responsável pelo Gerenciamento Integrado de Riscos e Capital (*Chief Risk Officer – CRO*) exerce suas atribuições de forma independente.

A área de GIR compreende quatro células, sob direção e gestão comum, mas com equipes próprias:

i. Riscos Financeiros;
ii. Riscos Não Financeiros;
iii. Controles Internos; e
iv. Compliance Regulatório.

Riscos Financeiros e Riscos Não Financeiros tem como responsabilidades gerais identificar, mensurar, avaliar, monitorar, reportar e mitigar os riscos financeiros, não financeiros, incluindo seus efeitos adversos resultantes das interações entre os riscos, de forma a garantir que as exposições estejam dentro dos limites de apetite por riscos fixados na *RAS*.

Controles Internos e *Compliance* tem como responsabilidades gerais planejar, implementar, operacionalizar, manter, criar controles internos e revisar os procedimentos relativos à conformidade com a legislação e regulação aplicáveis as atividades do Ouribank.

O modelo de três linhas de defesa é adotado como uma forma de gerenciamento de riscos e controles:

Primeira Linha de Defesa: representada por todos os colaboradores das áreas, enquanto proprietários diretos dos riscos inerentes às suas atividades, implementando e aperfeiçoando os controles e ações mitigatórias em conformidade com as Políticas de Gerenciamento Integrado de Riscos, Controles Internos e *Compliance*, Prevenção à Lavagem de Dinheiro e Financiamento ao Terrorismo, Relacionamento com Cliente e o Código de Ética.

Entre os colaboradores, especial responsabilidade têm os agentes de *Compliance* e Gestores de contribuir com a Segunda Linha de Defesa para a efetiva aplicação das Políticas, disseminando entre os demais colaboradores de suas áreas as diretrizes definidas, conscientizando-os da necessidade da sua observância e efetividade, além de reportar os eventos de risco das suas áreas e garantir a implementação dos procedimentos de mitigação de riscos.

Segunda Linha de Defesa: representada pelas áreas de Gerenciamento Integrado de Riscos, Controles Internos e *Compliance*, responsáveis por auxiliar a primeira linha de defesa na identificação dos riscos e sua mitigação, assegurando que os processos sejam cumpridos em conformidade com as leis e regulamentos internos, zelando pelo controle dos riscos de acordo com o apetite por riscos.

Terceira Linha de Defesa: representada pela Auditoria Interna, que tem como função revisar de modo eficiente as atividades das duas primeiras linhas de defesa e contribuir para a qualidade e efetividade dos sistemas e processos de controles internos, gerenciamento de riscos e governança das áreas por meio de uma avaliação independente, autônoma e imparcial.

As três linhas desempenham papéis independentes e complementares na governança de Riscos, Controles Internos e *Compliance*.

O Ouribank conta, ainda, em sua estrutura de governança com Comitês, que são órgãos de apoio e assessoramento ao Conselho de Administração e à Diretoria Colegiada Atualmente, Ouribank mantém os seguintes Comitês.

Comitê Estratégico de Controles Internos e *Compliance* (CECIC)

O Comitê Estratégico de Controles Internos e Compliance, se constitui em importante instância estratégica, que tem como objetivo precípuo avaliar, de forma permanente, questões e situações que permitam reforçar os Controles Internos e Compliance do Ouribank.

Há Três Comissões vinculadas ao CECIC:

i. Comissão Executiva de Gerenciamento Integrado de Risco: é composta por colaboradores das áreas de Gerenciamento Integrado de Riscos, Controles Internos, Compliance e Tecnologia da Informação. Tal Comissão tem como atribuição a execução, acompanhamento das atividades de gerenciamento de riscos e de capital, nos termos da Resolução CMN 4.557, incluindo o envolvimento e treinamento das áreas de negócios na identificação dos riscos e sua mitigação.

ii. Comissão de Detecção à Fraudes: é composta por colaboradores do Jurídico, Tecnologia de Informação, BackOffice e Gerenciamento Integrado de Riscos. Suas atribuições são relacionadas a tomadas de decisões relacionadas a prevenção, detecção, monitoramento da fraude e disseminar aos seus colaboradores e correspondentes cambiais, os procedimentos ao tema de fraude e seus métodos de prevenção.

iii. Comissão de Auditoria: é composta por Diretores que representam a Diretoria Colegiada. Sua atribuição é apoiar o Conselho de Administração na avaliação da qualidade e a efetividade dos sistemas e dos processos de controles internos, gerenciamento de riscos e governança corporativa de maneira autônoma e imparcial, conforme disposições da Resolução CMN nº 4.879/20.

Comitê de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo (Comitê de PLD/FTP)

O Comitê PLD/FTP tem como principal objetivo apoiar o Conselho de Administração e a Diretoria do Ouribank no gerenciamento de ações e políticas internas ligadas à PLDFTP,

buscando o permanente alinhamento à legislação e à regulamentação aplicáveis à matéria, além de apoiar as áreas de negócios e de controles internos na identificação, na classificação e na mitigação de riscos ligados à lavagem de dinheiro e ao financiamento do terrorismo.

Comitê de Crédito (CRE)
O Comitê de Crédito tem como principal objetivo apoiar o Conselho de Administração e a Diretoria no estabelecimento de diretrizes e políticas internas para a aprovação e monitoramento das operações de crédito, de forma a maximizar resultados e mitigar riscos a eles inerentes.

Comitê de Operações de Câmbio (CCA)
O Comitê de Operações de Câmbio tem por objetivo estabelecer diretrizes, políticas e estratégicas internas para realização de operações cambiais, nas suas diversas naturezas e aprovação de clientes e operações de maior risco.

Há uma Comissão vinculada ao CCA, sendo a Comissão Conheça Seu Cliente Câmbio ("Comissão KYC Câmbio"), que tem como atribuição a análise e aprovação do processo de KYC das operações de câmbio no mercado primário.

Comitê de Segurança da Informação (CSI)
O Comitê de Segurança da Informação tem por objetivo avaliar, de forma permanente, questões e situações relacionadas à Segurança da Informação no âmbito físico, lógico e pessoal, relacionados aos interesses, necessidades e riscos das áreas, apoiando a Diretoria no estabelecimento de diretrizes, políticas e estratégicas para assegurar a integridade, confidencialidade e disponibilidade de dados e dos sistemas de informação utilizados, de forma segura e protegida de ataques, tanto internos quanto externos, garantindo que, mesmo dentro do ambiente de continuidade de negócios, haja segurança plena em linha com a capacidade de operar todas as suas funções, salvaguardando todos os direitos e obrigações para com clientes, fornecedores e entidades reguladoras e fiscais.

Comitê de Privacidade e Proteção de Dados (CPPD)
O Comitê de Privacidade e Proteção de Dados tem como objetivo avaliar, de forma permanente, questões e situações relacionadas à Política de Privacidade e Proteção de Dados, apoiando o Encarregado de Proteção de Dados na tomada de decisão, no estabelecimento de diretrizes, políticas e estratégicas internas para manutenção da conformidade e governança da privacidade e proteção de dados.

(c) Canais de disseminação da cultura de riscos na instituição (código de conduta, manuais, processos de comunicação de riscos, entre outros).

Os principais canais de disseminação da cultura de riscos no Ouribank são:

i. Os documentos que compõem o Sistema Normativo, que é composto por Políticas, Normas e Manuais na intranet;
ii. Plataforma Ouribank Educa onde são disponibilizados os treinamentos para os colaboradores e correspondentes no país;
iii. E-mails utilizados para disseminação de "pílulas de conhecimentos";
iv. Reuniões periódicas entre agentes de *Compliance* e Segunda Linha de Defesa; e
v. Grupos de Trabalho, por meio de reuniões com troca de conhecimento entre os colaboradores.

O Ouribank também incentiva o desenvolvimento acadêmico de seus colaboradores, podendo, se aplicável, subsidiar cursos de especialização, entre outras certificações.

(d) Escopo e principais características do processo de mensuração de riscos.

O processo de mensuração de riscos é realizado por meio da utilização de sistemas e metodologias em conformidade com as regulamentações vigentes e em linha com as melhores práticas de mercado.

Risco de Mercado

O Risco de Mercado é a possibilidade de ocorrência de evento de perdas resultante da flutuação nos valores de mercado de posições proprietárias. Os riscos envolvidos são de variação das taxas de juros, preços de ações, variação cambial e dos preços de commodities para os instrumentos classificados nas Carteira de Negociação (Trading Book) e Bancária (Banking Book).

Todas as operações sujeitas à variação de preço em função das oscilações das taxas de mercado são objeto de análise e gestão do risco de mercado no Ouribank.

Os principais riscos de mercado expostos são:

a) Cambial;
b) Cupom cambial;
c) Taxas prefixadas;
d) Índices de preços;
e) Risco de crédito dos instrumentos financeiros classificados na carteira de negociação; e
f) Ajuste para Derivativos Decorrente de variação da qualidade Creditícia da Contraparte.

O processo de gerenciamento de risco de mercado é efetuado de forma contínua por meio da metodologia de *Value at Risk* (VaR) e da análise de sensibilidade. Para a carteira classificada como bancária a metodologia utilizada é o *Net Interest Income* (NII).

Como estratégia na mitigação dos riscos de mercado, principalmente do risco cambial e cupom cambial (advindos de operações de bank notes, termos, travas de moedas e contas correntes em moedas estrangeiras), são adotados instrumentos de hedge. Estes hedges normalmente são realizados através de operações de mercado de futuro.

Diariamente é efetuado o monitoramento do risco de mercado através de relatórios usando como referência os limites estabelecidos em RAS. No caso de uma extrapolação em algum limite estabelecido, o *Chief Risk Officer* (CRO) e os diretores das áreas responsáveis pelo evento são comunicados tempestivamente a fim de se tratar o evento.

Risco de Crédito

O Risco de Crédito é a possibilidade da ocorrência de evento de perdas associadas ao não cumprimento pelo tomador ou contraparte. Esse desenquadramento pode ser pelas respectivas obrigações financeiras nos termos pactuados, à desvalorização de contrato de crédito decorrente da deterioração na classificação de risco do tomador, à redução de ganhos ou remunerações, às vantagens concedidas na renegociação e aos custos de recuperação.

No gerenciamento do risco de crédito, os principais pontos de controles adotados são:

a) Avaliação da situação econômico-financeira dos envolvidos na operação. Periodicamente estes indicadores são reavaliados;
b) Avaliação periódica do grau de suficiência das garantias e sua liquidez;
c) Detecção de indícios de deterioração da qualidade das operações;
d) Ramo de atividade da contraparte;
e) Estimação das perdas esperadas;
f) Gerenciamento de ativos problemáticos;
g) Gerenciamento de exposições com características semelhantes; e
h) Gerenciamento do risco de concentração.

Risco de Liquidez

Risco de Liquidez é a possibilidade de a instituição não ser capaz de honrar eficientemente com as obrigações esperadas e inesperadas, correntes e futuras, incluindo as decorrentes de vinculação de garantias, sem afetar as operações diárias e sem incorrer em perdas significativas; e a possibilidade de a instituição não conseguir negociar a preço de mercado uma posição, devido ao tamanho elevado do volume normalmente transacionado ou em razão de alguma descontinuidade no mercado.

Diariamente é elaborado o fluxo de caixa de 90 dias a fim de monitorar eventuais descasamentos das saídas de recursos perante as entradas. Adicionalmente a relação entre ativos de alta liquidez e o colchão se liquidez é efetuada.

Os ativos de alta liquidez são compostos por disponibilidades em moeda nacional e estrangeira, aplicações de curtíssimos prazos e títulos públicos nacionais.

Em casos de cenários desfavoráveis ou o nível de ativos de alta liquidez ficar muito próximos dos limites estabelecidos ao perfil do Banco, o plano de contingência deve ser avaliado conforme estabelecido em política interna.

Risco Operacional

Risco Operacional é a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos.

A definição acima "inclui o risco legal associado à inadequação ou deficiência em contratos firmados pela entidade, bem como o risco de sanções em razão de descumprimento de dispositivos legais e de indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela entidade".

O Ouribank utiliza como ferramenta de trabalho as matrizes de riscos e controles que são elaboradas pela área de Riscos Não Financeiros em conjunto com os gestores e agentes de *Compliance* das áreas, e têm o objetivo de registrar os processos, etapas e atividades das áreas, servindo de instrumento para a avaliação da eficiência de seus métodos no gerenciamento de riscos que possam causar impactos relevantes, bem como as possíveis oportunidades de melhorias. Os possíveis eventos de risco operacional são avaliados quanto à probabilidade de frequência e o grau de severidade para mensuração do grau de impacto, sendo classificados nos seguintes níveis: Baixo, Moderado, Alto e Crítico. Mediante a definição do grau de risco são direcionadas ações para adequação dos processos e seus respectivos controles.

Adicionalmente, os eventos de riscos incorridos são reportados pelos gestores e/ ou agentes de *Compliance* à área de Riscos Não Financeiros, por meio de ferramenta GRC. A área de Riscos Não Financeiros é responsável por analisar de forma integrada os eventos relevantes de risco operacional, bem como desenvolver e monitorar os indicadores chave de risco.

Mensurados os riscos e identificadas exposições que extrapolem o perfil de risco, planos de ação são adotados visando reduzir o risco a um nível residual aceitável. As respostas incluem reduzir, mitigar, aceitar ou transferir os riscos de acordo com a avaliação do efeito, custos e benefícios.

A área de Riscos Não Financeiros constituiu uma base de dados para armazenar as informações referentes às perdas financeiras associadas ao risco operacional, com objetivo de construir uma base histórica. As informações de perdas operacionais são

conciliadas mensalmente com as informações da contabilidade. Todos os dados que compõem a base são íntegros, consistentes, originados de fontes confiáveis e passíveis de verificação.

Risco Social, Ambiental e Climático

Risco Social, Ambiental e Climático é definido como a possibilidade de ocorrência de perdas diretas e indiretas decorrentes dos danos por eles provocados. Reconhecemos a existência de riscos sociais, ambientais e climáticos, os quais são considerados como um componente das diversas modalidades de risco que estamos expostos, tais como risco de crédito, risco de compliance e risco reputacional.

O Ouribank analisa os riscos sociais, ambientais e climáticos dos seus clientes e de suas operações, conforme diretrizes estabelecidas na Política de Riscos e regulamentação vigente. Também utiliza critérios relativos à responsabilidade socioambiental corporativa no processo de cadastramento e homologação de parceiros de serviços e fornecedores relevantes, buscando sempre trabalhar com empresas que tenham boa conduta social, ambiental, ética e que incentivem a adoção de boas práticas dentro de suas empresas.

No processo de concessão de crédito, conhecendo previamente a atuação das empresas neste âmbito, por meio do preenchimento de formulário específico, com questões de cunho socioambiental e climática relacionadas à atividade e localização do cliente, licenças e autorizações ambientais de órgãos reguladores necessários para o exercício da atividade, questões de conduta social, relações trabalhistas envolvendo trabalho análogo à escravidão ou trabalho infantil, saúde e segurança ocupacional, assédio moral e sexual, discriminação de raça ou gênero.

A área de GIR é responsável pelo gerenciamento do risco social, ambiental e climático, identificando, avaliando e monitorando os riscos presentes nas atividades, bem como a avaliação prévia dos potenciais impactos negativos de novas modalidades de produtos e serviços, considerando sempre os princípios da relevância e proporcionalidade.

Risco de LD/FTP

O Risco de LD/FTP refere-se à possibilidade de utilização dos produtos e serviços oferecidos pelo Ouribank para a prática de Lavagem de Dinheiro e de Financiamento do Terrorismo, levando-se, nesse contexto, em consideração os impactos reputacional, jurídico, regulatório e socioambiental.

O gerenciamento do risco de LD/FTP é realizado conforme diretrizes estabelecidas pela Política Interna de Prevenção à Lavagem de Dinheiro e ao Financiamento do Terrorismo, que considera os perfis de risco da própria instituição, dos Clientes, Colaboradores, Parceiros e Fornecedores, produtos e serviços, abrangendo os canais de distribuição e a utilização de novas tecnologias, de forma a permitir a implementação efetiva de controles de prevenção, detecção e mitigação adequados.

O Ouribank por meio de Abordagem Baseada em Risco envida os esforços necessários para identificar, avaliar e entender os riscos de LD/FTP aos quais está exposto e fundamentar medidas proporcionais a estes riscos, a fim de mitigá-los de forma eficaz e efetiva. Desta forma, perfis considerados de maior risco de LD/FTP exigem *EDD (Enchanced Due Diligence)*, além de monitoramento reforçado, protocolos e definições de limites operacionais, adotando e exigindo alçadas de decisão que demandem, quando aplicável, aprovações em Comitês, para início ou manutenção de relacionamentos com Parceiros, Clientes, Terceiros, ou para decisões estratégicas de implementação de produtos, serviços e tecnólogas para situação de maior risco.

Todos os colaboradores são responsáveis por prevenir a utilização do Ouribank para a prática de LD/FTP, observando a legislação e regulação aplicáveis, a Política de PLDFTP e o Código de Ética Ouribank.

A área de GIR que atua identificando, avaliando, registrando e monitorando os riscos que possam impactar o Ouribank, inclusive PLDFTP, oferece subsídios para o trabalho de Controles Internos e *Compliance* destacando aspectos de controles mitigatórios dos riscos de LD/FTP.

Risco de *Compliance*

O Risco de *Compliance* é o somatório do risco reputacional e dos riscos de sanções pelos órgãos reguladores e autorreguladores, decorrentes da falta de aderência a regulamentos, políticas, código de conduta e procedimentos internos e externos.

A área Jurídica é responsável por definir a conduta por meio da qual as atividades e atitudes do Ouribank podem ser conduzidas, dentro do arcabouço regulatório e a área de Controles Internos e Compliance por efetuar abordagem nas atividades de forma rotineira e permanente, de modo a controlar e prevenir os riscos de *Compliance* envolvidos em cada atividade, sendo responsável por assegurar que as diversas áreas da instituição estejam em conformidade com a regulamentação aplicável.

Nos trabalhos de entendimento de processos (mapeamentos) e identificação de riscos realizados pela área de Riscos Não Financeiros, também são contemplados os riscos de *Compliance*, garantindo desta forma a gestão integrada dos riscos na instituição.

Risco Reputacional

O Risco Reputacional é definido como a possibilidade de perda de credibilidade aos olhos da sociedade. Ainda que baseada apenas na percepção e não em fatos, este risco pode reduzir a capacidade para estabelecer novas relações e/ ou manter as relações existentes com os seus *stakeholders* (clientes, investidores, contrapartes, mercado financeiro, órgãos reguladores, fornecedores, parceiros de negócios, funcionários e demais partes relacionadas), expondo o grupo a possíveis perdas financeiras.

O risco reputacional no Ouribank é considerado um risco secundário, pois decorre sempre dos riscos primários, sendo gerenciado por uma estrutura organizacional que se estende junto às boas práticas de governança, alinhada a visão estratégica do grupo, visando sempre garantir que os potenciais riscos sejam identificados, analisados e monitorados, tendo em vista que a imagem corporativa é um dos ativos mais importantes.

O gerenciamento do risco reputacional no Ouribank é realizado com base nas políticas corporativas, permanentemente alinhadas às legislações e às regulamentações vigentes, estabelecendo princípios e orientações, a fim de detectar, tratar, monitorar e impedir eventuais tentativas de utilização dos produtos e serviços financeiros do Ouribank para o exercício de atividades que possam ser caracterizadas como criminosas, no que tange a lavagem de dinheiro e financiamento ao terrorismo, fraudes, crimes contra a sociedade e o meio ambiente, dentre outros.

Risco de TI

O Risco de Tecnologia da Informação é definido como a possibilidade de perda ou impactos negativos que possam ser provocados pelos riscos inerentes ao emprego de recursos de TI na operacionalização dos negócios da instituição, abrangendo os dados e informações, os processos e as pessoas envolvidas.

O gerenciamento de Riscos de TI do Ouribank é realizado considerando os riscos inerentes e o nível de exposição representado, considerando os seguintes pilares:

a) Risco de Estratégia de TI;
b) Risco de Segurança da Informação;
c) Risco de Soluções de TI;
d) Risco à integridade da Informação; e
e) Risco de Continuidade de Negócios.

Nos trabalhos de mapeamento de riscos realizado pela área de Riscos Não Financeiros, também são contemplados os riscos de Tecnologia da Informação.

A gestão de Continuidade de Negócios é realizada pelas áreas de GIR e TI, de acordo com PCN (Plano de Continuidade de Negócios), que descreve as responsabilidades e as estratégias a serem adotadas diante de incidentes e eventuais crises.

(e) Processo de reporte de riscos ao CA e à diretoria.

A área de GIR realiza monitoramento contínuo dos limites de apetite por riscos fixados na RAS por meio de painéis indicadores e quando na iminência de extrapolação, os gestores das áreas envolvidas são acionados, a fim de solucionar o desvio apresentado,

entretanto, no caso de o limite extrapolado, a Diretoria envolvida e o CRO serão acionados tempestivamente.

O monitoramento é reportado à Diretoria Colegiada que orienta a tomada das medidas preventivas e/ ou corretivas, de forma a garantir que as exposições estejam dentro dos limites estabelecidos.

(f) Informações qualitativas sobre o programa de testes de estresse (portfólios considerados, cenários adotados, metodologias utilizadas e uso dos resultados no gerenciamento de riscos).

O teste de estresse é um processo de simulação de condições econômicas e de mercado extremas nos resultados, liquidez e capital da instituição. A instituição realiza este teste com o objetivo de avaliar a sua solvência em cenários plausíveis de crise, bem como de identificar áreas mais suscetíveis ao impacto do estresse que possam ser objeto de mitigação de risco.

O Ouribank utiliza a metodologia de análise de sensibilidade, simulando o impacto e a capacidade de absorção dos riscos no Capital. Adicionalmente, são calculados testes de estresse utilizando-se como premissas as orientações da Diretoria bem como os cenários disponibilizados pela B3.

Os resultados dos testes de estresse são utilizados como um dos instrumentos para a tomada das decisões estratégicas da instituição, bem como na revisão dos níveis de apetite por riscos, na revisão das políticas, das estratégias e dos limites estabelecidos para fins do gerenciamento de riscos e do gerenciamento de capital.

(g) Estratégias de mitigação de riscos e sua efetividade

Dentro da governança do processo de Gerenciamento de Riscos, são apresentados à Diretoria reportes consolidados de monitoramento, controles, planos de ação e perdas operacionais dos diferentes tipos de riscos.

Mensurados os riscos e estabelecidas as exposições que extrapolem o perfil de risco, planos de ação são adotados visando reduzir o risco a um nível aceitável. As respostas incluem reduzir, mitigar, aceitar ou transferir os riscos de acordo com a avaliação do efeito, custos e benefícios.

Os planos de ação contêm as medidas para controle, o responsável, os prazos para a realização e as estratégias adotadas, de acordo com o nível do risco identificado.

(h) Breve descrição do gerenciamento de capital, incluindo a avaliação de suficiência e adequação do Patrimônio de Referência (PR) para cobertura dos riscos das atividades atuais e projetadas da instituição.

O processo de gerenciamento de capital é realizado de forma a proporcionar condições para o alcance dos objetivos estratégicos da instituição, levando em consideração o ambiente econômico e comercial onde atua.

O processo de Adequação do Patrimônio de Referência é acompanhado diariamente e visa assegurar que o Ouribank mantenha uma sólida base de capital para apoiar o desenvolvimento das atividades e fazer face aos riscos incorridos, seja em situações normais ou em condições extremas de mercado, além de atender os requerimentos regulatórios de capital.

Anualmente é elaborado o plano de capital com base no planejamento estratégico levando em consideração os objetivos de médio e longo prazo, as oportunidades de mercado e os desafios para um horizonte de três anos. Adicionalmente é elaborado o plano de contingência de capital.