## Tabela ORA: Informações qualitativas sobre o gerenciamento do risco operacional

**Devem ser descritas as políticas e estratégias de gerenciamento do risco operacional conforme estabelecido na Resolução nº 4.557, de 23 de fevereiro de 2017, e na Resolução BCB nº 265, de 25 de novembro de 2022, destacando: ração 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.**

### A. As políticas e estratégias para o gerenciamento do risco operacional.

A gestão do risco operacional integra o Sistema Integrado de Controles Internos do BRDE, atualizado pela Resolução CA nº 2.894/2025. As políticas e diretrizes seguem a Declaração de Apetite a Risco (RAS) e estruturam-se na identificação, mensuração, monitoramento e controle dos riscos, com registros efetuados pela Superintendência de Gestão de Gestão de Riscos, Controles Internos e *Compliance* (SURIS) nas Matrizes de Risco Operacional e de Controles Internos.

A SURIS realiza de forma contínua o acompanhamento dos processos internos mais relevantes para o funcionamento normal das atividades do BRDE, em conformidade com as exigências regulatórias. O acompanhamento visa identificar potenciais fatores geradores de riscos, fragilidades e práticas a aprimorar nas rotinas do Banco. O modelo privilegia controles contínuos, revisão periódica e integração com o Planejamento Estratégico, garantindo aderência entre o perfil de riscos do negócio e os limites definidos pelo Conselho de Administração.

### B. A estrutura organizacional, incluindo papéis e responsabilidades do pessoal da instituição no gerenciamento e controle do risco operacional.

A SURIS, subordinada à Diretoria de Planejamento, exerce o papel de unidade central do gerenciamento de riscos no BRDE. Cabe à Superintendência conduzir a implementação das diretrizes do Sistema Integrado de Controles Internos, monitorar os riscos relevantes e encaminhar os respectivos reportes aos órgãos de governança. Sua estrutura contempla departamentos especializados, incluindo aqueles dedicados aos riscos de mercado (DERIS) e aqueles responsáveis pelo risco operacional, controles internos e *compliance*. A Auditoria Interna mantém atuação independente, realizando avaliações contínuas sobre a aderência e a efetividade das políticas e controles adotados pela instituição, assegurando a execução adequada das diretrizes aprovadas.

No âmbito operacional, o Departamento de Risco Operacional e Controles Internos (DEROC) é responsável pela gestão do risco operacional. O departamento conta atualmente com quatro analistas — com 2 economistas, um administrador e um engenheiro — além de dois estagiários e um Chefe de Departamento, o que permite uma abordagem multidisciplinar na identificação, avaliação e mitigação dos riscos inerentes às atividades do Banco.

## C. Sistemas, rotinas e procedimentos utilizados para mensurar o risco operacional.

A mensuração do risco operacional utiliza as Matrizes de Risco Operacional e de Controles Internos, atualizadas pela SURIS, em apuração junto às áreas de negócio. Trata-se um instrumento de gestão que organiza, de forma sistemática, os riscos inerentes aos processos de uma instituição, permitindo sua identificação, análise e classificação segundo critérios de probabilidade e impacto.

Ele descreve os eventos que podem gerar perdas, suas causas, as vulnerabilidades associadas e os controles existentes, possibilitando avaliar o nível de risco residual e a necessidade de ações de mitigação. O processo envolve identificação de novos riscos, avaliação de severidade, adequação de controles e verificação de conformidade com os limites estabelecidos na RAS.

Outras ferramentas institucionais como o GLPI são utilizadas para registro e reporte de incidentes que podem causar perdas operacionais para o banco. Com periodicidade bimestral, a SURIS publica os relatórios de Riscos Operacionais e de Atividades de *Compliance*, onde apresenta as principais atualizações desse escopo de monitoramento. As perdas efetivadas são registradas na Base de Perdas Operacionais, bem como o nível de exposição a essa modalidade de risco, de acordo com os parâmetros estabelecidos pela RAS.

## D. O escopo e contexto dos relatórios gerenciais enviados para a diretoria, o comitê de riscos, e o conselho de administração, incluindo sua periodicidade, os critérios para inclusão de informações referentes às perdas operacionais relevantes e os incidentes que tenham ensejado reportes extraordinários.

A SURIS elabora, em base bimestral, os Relatórios de Riscos Operacionais e de Atividades de *Compliance*, nos quais consolida as principais ocorrências, tendências e atualizações referentes ao monitoramento contínuo desses temas. As perdas já materializadas são registradas na Base de Perdas Operacionais, juntamente com a indicação do nível de exposição associado, sempre em conformidade com os parâmetros definidos na Declaração de Apetite a Risco (RAS). A classificação dos eventos e os critérios que determinam sua inclusão nos relatórios seguem as diretrizes da Resolução CMN nº 4.557, preservando a mesma lógica de subcategorias de risco operacional adotada pelo regulador.

Embora a metodologia de classificação siga o padrão regulatório, o escopo informativo dos relatórios é mais amplo: além de perdas efetivamente incorridas, são também registrados incidentes que não resultaram em prejuízo financeiro, mas que representam sinalização de vulnerabilidade ou mudança de padrão de risco. Um exemplo é a tentativa de fraude cibernética por meio de e-mail malicioso. Mesmo sem impacto econômico, o evento é registrado para fins de aprendizado institucional, e disseminação de alerta aos colaboradores, contribuindo para o fortalecimento da cultura de controle e para a resposta tempestiva a potenciais ameaças.

Os reportes extraordinários mais recentes foram realizados ao longo de 2024, motivados por dois eventos de natureza excepcional. O primeiro decorreu dos episódios de eventos climáticos extremos registrados no Rio Grande do Sul, que ocasionaram danos físicos a instalações do BRDE, incluindo a perda de mobiliário e outros ativos de valor. O segundo refere-se a um incidente cibernético que, conforme exigido pela regulamentação vigente, foi prontamente comunicado ao Banco Central. Esse episódio demandou a adoção de medidas emergenciais e gerou despesas extraordinárias relacionadas ao reforço das soluções e infraestruturas de segurança da informação.

## E. Estratégias de mitigação do risco operacional, como políticas de disseminação da cultura de gerenciamento de riscos e de terceirização, programas de capacitação, e o estabelecimento de controles do risco operacional.

O BRDE adota um conjunto estruturado de estratégias de mitigação do risco operacional, que abrangem a disseminação contínua da cultura de controles, a capacitação dos colaboradores e o fortalecimento dos mecanismos de prevenção a perdas.

Essas estratégias incluem a manutenção de controles internos atualizados, a segregação adequada de funções, a realização de treinamentos regulares sobre conduta, conformidade e segurança da informação, além do monitoramento sistemático de incidentes e vulnerabilidades.

O BRDE vem ampliando seus investimentos na capacitação do corpo funcional, promovendo formações complementares em temas diretamente relacionados ao risco operacional, como segurança cibernética, segurança do trabalho e demais áreas que influenciam a resiliência operacional do banco. Essas iniciativas reforçam a cultura de prevenção e de compartilhamento de conhecimento, em linha com as diretrizes do Planejamento Estratégico 2030, que contempla o fortalecimento contínuo das práticas de gestão de riscos e de controles internos como eixo estruturante da atuação institucional.