POLÍTICA CORPORATIVA

DE GESTÃO DE RISCO OPERACIONAL

DO SISTEMA BNDES

BNDES

Aprovada pela Resolução CA nº 14/2024-BNDES, de 20.09.2024. Vigente desde 23.09.2024.

1. OBJETIVOS

1.1. Orientar a gestão de risco operacional, de forma integrada aos demais tipos de riscos aos quais o Sistema BNDES está exposto;

1.2. Proteger o Sistema BNDES colaborando para que os seus objetivos sejam atingidos com segurança; e

1.3. Adequar o Sistema BNDES aos normativos relativos a risco operacional emanados dos órgãos de regulação e controle, bem como às melhores práticas e aos referenciais de mercado.

2. ABRANGÊNCIA E ESCOPO

2.1. Esta Política é aplicável às atividades do BNDES e de suas subsidiárias, a BNDES Participações S/A (BNDESPAR) e a Agência Especial de Financiamento Industrial S.A. (FINAME).

2.1.1 Esta Política se aplica a todos os Participantes do Sistema BNDES e aos seus prestadores de serviço.

2.2. Esta Política, alinhada à missão e aos objetivos da Instituição, estabelece objetivos, princípios e responsabilidades aplicáveis à gestão de risco operacional.

2.3. A gestão de risco operacional do Sistema BNDES orienta-se essencialmente pelo disposto na Resolução CMN nº 4.557, de 23.02.2017.

2.4. A gestão de risco operacional abarca os riscos à segurança da informação (incluindo os riscos cibernéticos), os riscos à proteção de dados pessoais e os riscos à continuidade de negócios, bem como os controles internos para a mitigação destes riscos.

2.4.1. A gestão de risco operacional à segurança da informação, à proteção de dados pessoais e à continuidade de negócios é complementada pelo disposto, respectivamente, na Política Corporativa de Segurança da Informação do Sistema BNDES (PCSI), na Política Corporativa de Proteção de Dados Pessoais do Sistema BNDES (PCPD) e na Política Corporativa de Gestão de Continuidade de Negócios do Sistema BNDES (PGCN) e suas normas complementares.

2.4.2. O escopo da gestão de riscos operacionais abrange todas as atividades executadas pelo Sistema BNDES. Especificamente com relação à segurança da informação, à proteção de dados pessoais e à continuidade de negócios, a limitação de escopo abrange:

i) Segurança da Informação: preservação da confidencialidade, integridade, disponibilidade e autenticidade dos ativos de informação sensíveis e dados sensíveis mantidos nos sistemas principais, conforme definição da PCSI;

ii) Proteção de Dados Pessoais: operações de tratamento de dados pessoais realizadas nas atividades do Sistema BNDES; e

iii) Continuidade de Negócios: processos críticos para a continuidade de negócios do Sistema BNDES.

3. DEFINIÇÕES OU ABREVIATURAS

Termo	Conceituação
Agente de Conformidade	Empregado, ocupante de cargo de nível superior, indicado pelo Superintendente para atuar como interlocutor da sua Unidade Fundamental perante as unidades responsáveis pelos temas compliance, risco operacional e controle interno.
Alta Administração	Presidente, Diretores e membros dos demais órgãos colegiados estatutários das empresas do Sistema BNDES.
CRO	Diretor responsável pelo gerenciamento de riscos (*Chief Risk Officer*).
Evento de Risco Operacional (Evento)	Materialização de um risco operacional que possa causar um dos seguintes efeitos: i) Perda: valor quantificável associado a um Evento, incluindo provisões e despesas; ii) Quase perda: perda que não foi consumada em função de um controle exercido, de uma norma preventiva cumprida, de um ato defensivo ou de questões circunstanciais; iii) Receita perdida: valor monetário relativo a direitos previstos em normativos, internos ou externos, ou em contratos firmados pelo Sistema BNDES, e que não foram exercidos, nem registrados contabilmente, devido a um Evento; e iv) Ganho operacional: ganhos inesperados recebidos em virtude da ocorrência de um Evento.
PAINT	Plano Anual de Auditoria Interna.
Participantes do Sistema BNDES	Empregados integrantes dos quadros de pessoal permanente ou temporário, ainda que se encontrem cedidos ou requisitados ou liberados no âmbito do Acordo Coletivo de Trabalho do Sistema BNDES ou legislação específica, ou em gozo de licença ou em outro afastamento equivalente, com ou sem remuneração, os cedidos às empresas do Sistema BNDES, os estagiários e os membros dos órgãos colegiados estatutários das empresas do Sistema BNDES.

Termo	Conceituação
PGIRC	Política Corporativa de Gestão Integrada de Riscos e Capital do Sistema BNDES.
RAS	Declaração de Apetite por Riscos do Sistema BNDES (*Risk Appetite Statement*).
Risco Operacional	Possibilidade de ocorrência de perdas resultantes de eventos externos ou de falha, deficiência ou inadequação de processos internos, pessoas ou sistemas. Esta definição inclui 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, conforme previsto na Resolução CMN nº 4.557, de 2017. São categorias de Eventos de risco operacional: i) fraudes internas, decorrentes de atos intencionais destinados à defraudação, à apropriação indevida de bens e/ou à burla de regulação, de leis e de políticas internas, que envolva pelo menos uma parte interna; ii) fraudes externas, decorrentes de atos intencionais destinados à defraudação, à apropriação indevida de bens e/ou à burla de leis ou normas, praticados por terceiros; iii) demandas trabalhistas e segurança deficiente do local de trabalho; iv) práticas inadequadas relativas a usuários finais, clientes, produtos e serviços; v) danos a ativos físicos próprios ou em uso; vi) situações que acarretem a interrupção de atividades ou a descontinuidade dos serviços prestados; vii) falhas em sistemas, processos ou infraestrutura de tecnologia da informação; e viii) falhas na execução, no cumprimento de prazos ou no gerenciamento de atividades.
Risco à Continuidade de Negócios	Possibilidade de perdas financeiras, impactos reputacionais e/ou regulatórios decorrentes de incidentes, contingências ou crises no escopo da continuidade de negócios.
Risco à Proteção de Dados Pessoais	Possibilidade de vazamento de dados pessoais ao ocorrer acesso, coleta, divulgação ou repasse a terceiros de tais informações ou o uso de dados pessoais em finalidade diversa à definida previamente, independente de causar dano ao seu titular.

Termo	Conceituação
Risco à Segurança da Informação	Potencial de violação da integridade, confidencialidade, disponibilidade ou autenticidade da informação de propriedade ou custodiada pelo Sistema BNDES em decorrência da exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo às empresas do Sistema BNDES. Esta definição inclui o risco cibernético, que é o risco à segurança da informação que envolve ativo de tecnologia da informação.
Terceiro relevante	Prestador de serviço terceirizado ao Sistema BNDES que pode ocasionar e/ou contribuir para a materialização de Evento de risco operacional relevante.
UF	Unidade Fundamental

4. PRINCÍPIOS E DIRETRIZES

4.1. A execução dos processos e atividades do Sistema BNDES deve ser norteada pelos seguintes princípios:

a. tom do topo: a Alta Administração deve demonstrar comprometimento com todos os atos e medidas necessários para a implementação, aplicação e efetividade do processo de gestão de risco operacional;

b. abrangência: a gestão de risco operacional deve ser parte integrante de todos os processos do Sistema BNDES;

c. avaliação: os riscos operacionais e os controles internos associados devem ser continuamente analisados pelos gestores dos respectivos processos, inclusive quanto à adoção de novos produtos, serviços e sistemas;

d. formalização: os processos devem ser mapeados e formalizados, com a devida identificação dos riscos, controles internos e normativos associados;

e. responsabilização: as normas e procedimentos devem ser definidos com a identificação clara da responsabilidade pela condução de determinada atividade, observando a prevenção de potenciais conflitos de interesse; e

f. custo-benefício: os custos associados aos controles internos não devem ser superiores aos benefícios esperados em decorrência de sua implementação.

5. PROCESSO DE GESTÃO

5.1. São objetivos dos processos de gestão de risco operacional:

a. agregar valor à Instituição a partir da adequada mitigação dos riscos operacionais e da limitação dos impactos decorrentes de sua materialização;

b. assegurar que os responsáveis pela tomada de decisão tenham acesso a informações compreensíveis, confiáveis, tempestivas e relevantes sobre os riscos operacionais aos quais a Instituição está exposta, para realizar suas tarefas e cumprir suas responsabilidades; e

c. apoiar a sustentabilidade financeira da Instituição por meio da avaliação da necessidade de capital para fazer face aos riscos operacionais.

5.2. O processo de gestão de risco operacional deve ser compatível com a natureza, porte, complexidade, estrutura, perfil de risco e modelo de negócio do Sistema BNDES e observar, no mínimo, a estrutura organizacional, processos internos, requisitos legais, objetivos e controles internos, incluindo controles para segurança da informação, proteção de dados pessoais e continuidade de negócios.

5.3. O processo de gestão de risco operacional deve compreender as etapas de identificação, análise, avaliação, tratamento, monitoramento e reporte, devendo ser orientado por metodologias definidas pela unidade gestora de risco operacional.

5.4. São modalidades possíveis para o tratamento de um risco operacional, respeitado o disposto na RAS:

a. aceitar: decisão consciente de assumir o risco operacional, seja por se enquadrar no apetite por riscos definido na RAS, seja porque os custos para a adoção de controles internos adicionais superam os benefícios esperados;

b. transferir: distribuição acordada do risco operacional com outras partes, de forma total ou parcial;

c. mitigar: adoção de medidas que minimizem a probabilidade e/ou o impacto esperados de ocorrência de um Evento de risco operacional; ou

d. eliminar: adoção de medidas que impliquem a exclusão de determinado risco operacional, podendo envolver a mudança, suspensão ou término de uma atividade.

5.4.1. Para a seleção da modalidade de tratamento mais adequada deve-se equilibrar, de um lado, os custos e esforços de implementação e, de outro, os benefícios decorrentes de sua adoção, bem como observar restrições técnicas, físicas estruturais, operacionais, organizacionais e legais.

5.5. Os processos executados pela Instituição devem prever controles internos condizentes e proporcionais aos respectivos riscos operacionais.

5.6. O processo de gestão de risco operacional deve ser continuamente monitorado para a identificação e implementação de oportunidades de melhoria.

6. PAPÉIS E RESPONSABILIDADES

6.1. O Sistema BNDES adota o conceito de linhas para a gestão de risco operacional:

a. a primeira linha é constituída pelos gestores dos processos das diversas unidades do Banco, que têm a responsabilidade de gerir os riscos operacionais dos processos nos quais atuam, bem como de definir e manter controles internos adequados;

b. a segunda linha é composta pela Área de Integridade e Compliance, que tem o papel de apoiar os gestores na identificação e avaliação dos riscos operacionais e dos respectivos controles internos, de disseminar a cultura destes temas e de reportar-se à estrutura de governança; bem como por outras unidades que executam atividades de natureza semelhante, no âmbito de suas respectivas atribuições; e

c. a terceira linha compreende a Auditoria Interna, que tem por finalidade avaliar de forma objetiva a integridade e adequação do sistema de controle interno, da gestão de riscos e da governança corporativa do Sistema BNDES, bem como realizar a interlocução com os órgãos externos de controle e fiscalização, fazendo parte do Sistema de Controle Interno do Poder Executivo Federal e sendo órgão técnico de assessoramento e consultoria dos membros dos Conselhos de Administração e Fiscal do Sistema BNDES.

6.2. Os papéis e responsabilidades relacionados nesta seção não são exaustivos, devendo ser observado o disposto nos demais normativos pertinentes.

6.3. Cabe ao Conselho de Administração (CA):

a. aprovar e revisar, anualmente, a PRO, determinando a implantação e supervisionando o sistema de gestão de risco operacional estabelecido para a prevenção e mitigação dos principais riscos a que está exposta a empresa estatal;

b. assegurar a aderência da Instituição às políticas, às estratégias e aos limites de gerenciamento de risco operacional e autorizar exceções, quando aplicável;

c. promover a disseminação da cultura de gerenciamento de risco operacional no Sistema BNDES; e

d. garantir que a estrutura remuneratória adotada pela Instituição não incentive comportamentos incompatíveis com o apetite por risco operacional do Sistema BNDES.

6.4. Cabe ao Comitê de Auditoria (COAUD):

a. supervisionar as atividades desenvolvidas nas unidades de controle interno do Sistema BNDES; e

b. avaliar e monitorar as exposições a risco operacional do Sistema BNDES, de forma sinérgica com o CRi, bem como a qualidade e a integridade dos mecanismos de controle interno.

6.5. Cabe ao Comitê de Riscos (CRi):

a. propor, com periodicidade mínima anual, recomendações ao Conselho de Administração sobre políticas, estratégias e limites de gerenciamento de risco operacional e capital e o programa de teste de estresse;

b. avaliar os níveis de apetite por riscos fixados na RAS e as estratégias para o seu gerenciamento, considerando o risco operacional individualmente e de forma integrada aos demais tipos de riscos;

c. analisar o ambiente de riscos operacionais do Sistema BNDES, mediante informações produzidas pela AIC;

d. supervisionar a atuação e desempenho do Diretor responsável pela AIC;

e. supervisionar a observância, pela Diretoria Executiva, dos termos da RAS; e

f. avaliar o grau de aderência dos processos da estrutura de gerenciamento de risco operacional às políticas estabelecidas.

6.6. Cabe ao Presidente atuar como principal responsável pela formulação da estratégia da organização e da estrutura de gerenciamento de risco operacional, incluindo o estabelecimento, a manutenção, o monitoramento e o aperfeiçoamento dos controles internos da gestão.

6.7. Cabe à Diretoria Executiva:

a. manifestar-se acerca da proposta de aprovação desta Política, submetendo-a anualmente à deliberação do Conselho de Administração;

b. conduzir, em conformidade com as políticas e estratégias para o gerenciamento de risco operacional, as atividades que impliquem a assunção de risco; e

c. fomentar a cultura de gestão de risco operacional e a integração das práticas de gestão deste risco aos negócios e aos objetivos estratégicos da Instituição.

6.8. Cabe ao Diretor designado como *Chief Risk Officer* (CRO):

a. supervisionar o desenvolvimento, a implementação e o desempenho da estrutura de gerenciamento de risco operacional, incluindo seu aperfeiçoamento;

b. garantir a adequação das políticas, dos processos, dos relatórios, dos sistemas e dos modelos utilizados no gerenciamento de risco operacional à RAS e aos objetivos estratégicos da Instituição;

c. garantir a adequada capacitação dos integrantes da AIC acerca das políticas, dos processos, dos relatórios, dos sistemas e dos modelos da estrutura de gerenciamento de risco operacional, mesmo que desenvolvidos por terceiros; e

d. subsidiar e participar no processo de tomada de decisões estratégicas relacionadas à gestão de risco operacional e, quando aplicável, à gestão de capital, auxiliando a Diretoria Executiva e o Conselho de Administração.

6.9. Cabe ao Comitê de Gestão de Riscos (CGR):

a. avaliar o processo de gestão do risco operacional e dos limites de exposição a este risco e propor seu encaminhamento à Diretoria Executiva;

b. monitorar a exposição ao risco operacional, os instrumentos de mitigação deste risco e a alocação de capital;

c. monitorar o atendimento aos limites de exposição ao risco operacional definidos na PGIRC;

d. analisar as propostas de alteração da PRO, bem como dos demais normativos dela decorrentes, e encaminhá-las à alçada competente para validação ou deliberação;

e. apreciar relatos de Eventos de perda de risco operacional que, pelo seu valor, devam ser apresentados também à Diretoria Executiva e ao Comitê de Riscos (perdas atípicas), e outros Eventos que, a critério da Superintendência da AIC, mereçam apreciação do colegiado, desde que o valor da perda seja superior ao Limite por Evento; e

f. apoiar a disseminação da cultura de gestão de risco operacional no Sistema BNDES.

6.10. Cabe à Unidade de Auditoria Interna (AT):

a. avaliar de forma objetiva a integridade e a adequação do sistema de controles internos, da gestão de riscos e da governança corporativa, o que inclui a avaliação da confiabilidade e da integridade das informações e os meios usados para identificar, mensurar, classificar e reportar tais informações;

b. considerar no PAINT, de acordo com sua abordagem de riscos e com a rotação de ênfase e escopo, a realização de trabalho de avaliação dos processos relativos ao gerenciamento de riscos e ao gerenciamento de

capital da Instituição; e outros aspectos sujeitos à avaliação da auditoria interna por determinação da legislação em vigor e da regulamentação emanada do Conselho Monetário Nacional e do Banco Central do Brasil; e

c. acompanhar as ações de fiscalização do Tribunal de Contas da União, da Controladoria Geral da União e do Banco Central do Brasil, bem como monitorar e reportar o andamento da implementação das recomendações, determinações e apontamentos oriundas de tais ações.

6.11. Cabe ao Departamento de Gestão de Risco Operacional da Área de Integridade e Compliance (AIC/DEROP):

a. elaborar e rever esta Política, anualmente, e encaminhar a proposta para aprovação do Conselho de Administração, após manifestação da Diretoria Executiva, do Comitê de Riscos e do Comitê de Gestão de Riscos, garantindo que as versões aprovadas sejam comunicadas para todo o Sistema BNDES;

b. coordenar o processo de gestão de risco operacional, apoiando a atuação da primeira linha, por meio da orientação aos gestores na aplicação das metodologias, visando mitigar os riscos e aprimorar os controles internos;

c. desenvolver e gerir procedimentos e metodologias de gestão de risco operacional, incluindo, entre outros requisitos estabelecidos à luz dos melhores guias de práticas para gestão de riscos de segurança da informação e da regulamentação em vigor, a previsão de elaboração do plano para gestão de riscos de segurança da informação e cibernéticos e dos relatórios para identificação, análise, avaliação e tratamento de riscos de segurança da informação e cibernéticos;

d. submeter procedimentos e metodologias de gestão de risco operacional à deliberação da Superintendência da AIC;

e. desenvolver e gerir metodologia para a definição, análise e acompanhamento de cenários de risco operacional, apoiando as UFs na sua aplicação;

f. desenvolver e gerir metodologia para definição de limites de risco operacional, monitorando e reportando seu cumprimento às instâncias pertinentes;

g. calcular o capital regulatório e econômico referente ao risco operacional e gerir o seu consumo;

h. manter processo consistente e abrangente de captura e análise de informações sobre perdas operacionais, incluindo aquelas associadas ao risco de crédito, ao risco de mercado, ao risco social, ao risco ambiental e ao risco climático, visando subsidiar a identificação, avaliação, registro, classificação e agregação de perdas em base de dados de risco operacional, bem como efetuar a análise da causa raiz de cada perda operacional relevante; e reportá-las à estrutura de governança, conforme procedimento aprovado, além de remeter as informações exigidas pelo Banco Central do Brasil;

i. desenvolver e monitorar indicadores de risco operacional;

j. manter processo estruturado e contínuo de comunicação e treinamento, visando à disseminação da cultura de gestão de risco operacional, inclusive no âmbito da gestão de risco operacional associado a terceiro relevante;

k. manter processo estruturado para registro e monitoramento dos planos de ação relativos à gestão de risco operacional, prioritariamente por meio de interlocução com a equipe de Agentes de Conformidade, reportando o seu andamento em relatórios periódicos;

l. encaminhar ao CGR e, quando pertinente, ao CRi questões relativas à gestão de risco operacional e monitorar a implementação de suas recomendações; e

m. elaborar relatórios periódicos de suas atividades, reportando-os à Diretoria Executiva, aos Comitês de Riscos e de Auditoria e aos Conselhos de Administração e Fiscal.

6.12. Cabe às Unidades Fundamentais e seus executivos:

a. observar, na execução de suas atividades, as disposições desta Política;

b. avaliar continuamente seus processos, visando identificar, analisar, avaliar, tratar, monitorar e reportar os riscos operacionais associados e implementar os controles internos necessários à adequada mitigação dos respectivos riscos operacionais, de acordo com esta Política e demais normas relacionadas;

c. realizar análise de riscos operacionais previamente à criação ou alteração relevante de produtos e serviços, conforme metodologia específica aprovada pela AIC;

d. reportar tempestivamente ao AIC/DEROP informações relativas aos riscos operacionais dos seus processos e aos Eventos deles oriundos, conforme procedimento específico aprovado pela AIC;

e. gerir os planos de ação para mitigação de risco operacional conforme procedimento específico aprovado pela AIC e reportar tempestivamente ao AIC/DEROP informações sobre o andamento dos planos ou outras iniciativas para a mitigação desses riscos, prioritariamente por meio dos Agentes de Conformidade;

f. incentivar a participação dos empregados da UF nas ações de capacitação relacionadas à gestão de risco operacional, bem como providenciar para que conheçam integralmente e atuem em conformidade com esta Política; e

g. fornecer tempestivamente as informações solicitadas pelo AIC/DEROP, observando os procedimentos vigentes para classificação de informações e restrição de acesso.

6.13. Cabe aos empregados:

a. comunicar tempestivamente ao AIC/DEROP a ocorrência de Evento de risco operacional em atividade que execute;

b. participar dos treinamentos relacionados a risco operacional, quando solicitado pelo AIC/DEROP; e

c. orientar os terceiros contratados sob sua responsabilidade quanto à gestão de risco operacional relacionados à prestação do serviço ou entrega do produto, caso seja gestor de contrato.

7. DISPOSIÇÕES FINAIS

7.1. Havendo modificação na nomenclatura ou na competência das Unidades Fundamentais e Unidades Administrativas Principais da estrutura organizacional do Sistema BNDES, ou a atualização de normativos, o presente ato normativo permanecerá em vigor, adequando-se a sua aplicação às novas normas da organização interna.

7.2. O presente ato normativo entrará em vigor na data de sua publicação e, em conformidade com a Resolução CMN Nº 4.557, de 2017, deverá ser objeto de revisão anual.

7.3. A revisão anual será submetida diretamente à deliberação do Conselho de Administração do BNDES, para revalidação da Política em vigor, quando não houver necessidade de alteração de seu conteúdo. Igualmente, a revisão anual será encaminhada diretamente ao Conselho de Administração do BNDES quando:

a. a alteração tiver como finalidade mera adequação a normativo externo de reprodução obrigatória;

b. a alteração tiver como finalidade a correção de erro material; e/ou

c. a alteração tiver como finalidade adequar a redação da Política às modificações realizadas na estrutura organizacional do Sistema BNDES, desde que a proposta se limite a alterar siglas/nomes de unidades e/ou sugira a redistribuição dos papéis e responsabilidades já previstos no normativo, de forma a adaptar a Política ao disposto na Organização Interna Básica do Sistema BNDES em relação às atribuições das Unidades Fundamentais e/ou das Unidades Administrativas Principais.

7.3.1 Previamente à manifestação do Conselho de Administração, será feito comunicado à Diretoria Executiva, ao CRi, ao CGR e, eventualmente, a outro órgão colegiado, sempre que exigido por normativo externo.

7.3.2 A proposta de revisão não seguirá este trâmite nos casos em que, ao se manifestar sobre a matéria, o Conselho de Administração entenda pela impossibilidade de adoção do fluxo de aprovação simplificada.

8. REFERÊNCIAS EXTERNAS

- Lei nº 13.709, de 14.08.2018 (Lei Geral de Proteção de Dados Pessoais – LGPD)
- Resolução CMN nº 4.557, de 23.02.2017 (Dispõe sobre a estrutura de gerenciamento de riscos e a estrutura de gerenciamento de capital das instituições financeiras)
- Resolução CMN nº 4.893, de 26.02.2021 (Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem)
- Resolução CGPAR nº 48, de 06.09.2023 (Estabelece diretrizes e parâmetros de governança para as áreas de auditoria interna, corregedoria, ouvidoria, gestão de riscos internos das empresas estatais federais)
- Instrução normativa GSI/PR nº 03, de 28.05.2021 (Dispõe sobre processos relacionados à gestão de segurança da informação nos órgãos e entidades da administração pública federal)

9. REFERÊNCIAS INTERNAS[1]

- Declaração de Apetite por Riscos (Resolução CA nº 01/2024-BNDES)
- Política de Gestão Integrada de Riscos e Capital (Resolução CA nº 10/2023-BNDES)
- Política de Gestão de Continuidade de Negócios (Resolução CA nº 15/2024-BNDES)
- Política de Segurança da Informação (Resolução CA nº 20/2023-BNDES)
- Política de Proteção de Dados Pessoais (Resolução CA nº 14/2021-BNDES)
- Procedimento de gestão de planos de ação relacionados a risco operacional controle interno e compliance (Instrução de Serviço SUP/AIC nº 01/2024-BNDES)
- Procedimento de gestão da base de dados de risco operacional (Instrução de Serviço SUP/AIC nº 02/2024-BNDES)

[1] Referências internas foram atualizadas após a aprovação da Política.

Aprovada pela Resolução CA nº 14/2024-BNDES, de 20.09.2024. Vigente desde 23.09.2024.

PALAVRAS-CHAVE

Gestão de Riscos; Risco Operacional; PRO

O conteúdo deste documento não pode ser reproduzido sem a devida autorização. Todos os direitos pertencem ao BNDES – Banco Nacional de Desenvolvimento Econômico e Social.