

POLÍTICAS REGULADAS

POLÍTICA DE SISTEMA DE CONTROLES INTERNOS

DATA DE CRIAÇÃO

23/09/2024

CÓDIGO

POR.RISC NAO FIN E CI.006

ÁREA

Riscos Nao Financeiros E

Ci

EMPRESAS

TODAS

DATA DE ATUALIZAÇÃO

21/09/2026

VERSÃO

3.0

CLASSIFICAÇÃO

Políticas Reguladas

PUBLICADO POR

Marcia Angelica
Coutinho Moura

1. OBJETIVO

Estabelecer as diretrizes, princípios e responsabilidades para o Sistema de Controles Internos (SCI) do Conglomerado BS2, assegurando a eficácia operacional, mitigação de riscos, conformidade regulatória e confiabilidade das informações, conforme regulamentações aplicáveis.

O Sistema de Controles Internos (SCI) integra a estrutura de governança corporativa do Conglomerado BS2, estando alinhado às diretrizes estratégicas, ao apetite a riscos, às instâncias de decisão e aos mecanismos de supervisão exercidos pela Alta Administração e pelo Conselho de Administração

2. APLICAÇÃO

Esta política aplica-se a todas as empresas do Conglomerado BS2, incluindo colaboradores, prestadores de serviços e terceiros, abrangendo todas as atividades, processos, produtos, serviços e sistemas que possam impactar a integridade, segurança, conformidade e continuidade das operações.

Os requisitos específicos decorrentes da regulamentação aplicável a cada entidade deverão ser observados adicionalmente às diretrizes estabelecidas nesta Política.

3. REFERÊNCIAS

- Resolução CMN nº 4.968/2021 – Sistema de Controles Internos
- Resolução CMN nº 4.557/2017 – Estrutura de gerenciamento de riscos
- Resolução CMN nº 4.943/2021 – PRSAC
- Resolução BCB nº 260/2022 – Sistema de Controles Internos
- Resolução CVM nº 21/2021

- Resolução CNSP nº 416/2021 – Dispõe sobre o Sistema de Controles Internos, Estrutura de Gestão de Riscos e Auditoria Interna das sociedades supervisionadas pela SUSEP.
- COSO – Internal Control Framework (2013)
- ISO 31000:2018 – Gestão de Riscos
- Modelo das Três Linhas – IIA 2020
- NO.RISC NAO FIN E CI.006 – SISTEMA DE CONTROLES INTERNOS
- IT.RISC NAO FIN E CI.007 – TESTES DOS CONTROLES INTERNOS
- IT.RISCOSNF&CI.002 – MAPEAMENTO DE RISCOS OPERACIONAIS E CONTROLES INTERNOS

4. GLOSSÁRIO

- **Sistema de Controles Internos (SCI):** Conjunto estruturado e integrado de governança, políticas, pessoas, processos, estruturas e mecanismos de monitoramento, destinado a organizar, coordenar e supervisionar os controles internos, fornecendo segurança razoável quanto ao alcance dos objetivos operacionais, informacionais e de conformidade da instituição.
- **Controles Internos:** são os mecanismos específicos (planos, ferramentas, rotinas, métodos) que compõem esse sistema, visando proteger o patrimônio, prevenir fraudes e erros e alcançar objetivos de forma segura e eficiente.
- **Risco Operacional:** Possibilidade de perdas decorrentes de falhas em processos, pessoas, sistemas ou eventos externos.
- **1ª Linha:** Gestores e áreas de negócio responsáveis pela execução das atividades e dos controles.
- **2ª Linha:** Riscos Não Financeiros, Compliance, Riscos Financeiros, Segurança da Informação, Controladoria.
- **3ª Linha:** Auditoria Interna, responsável pela avaliação independente.

- **Segregação de Funções:** Distribuição adequada de atividades para reduzir riscos de erros, fraudes e conflitos de interesse.

5. DIRETRIZES

Essa política tem como diretrizes:

- **Gestão de Riscos:** o Sistema de Controles Internos deve estar integrado ao processo de identificação, avaliação, monitoramento e mitigação dos riscos, assegurando que os controles sejam compatíveis com o perfil de risco, a complexidade e a natureza das operações do Conglomerado BS2, não se limitando a um risco específico, abrangendo, entre outros, riscos operacionais, de conformidade, tecnológicos, de segurança da informação, socioambientais e climáticos, incluindo, de forma expressa, a análise do potencial de ocorrência de fraudes, internas e externas, em todos os níveis de negócio, processos, produtos e sistemas.
- **Inventário de Riscos e Controles:** as entidades integrantes do Conglomerado BS2 devem elaborar, manter atualizado e monitorar inventário dos riscos materiais identificados e das respectivas atividades de controle, contemplando, no mínimo, seus objetivos e responsáveis, observadas a natureza, o porte, a complexidade, o perfil de risco e a regulamentação aplicável a cada entidade.
- **Aderência Regulatória:** os controles internos devem estar alinhados às normas do CMN, Banco Central, CVM, SUSEP e demais órgãos reguladores, bem como às melhores práticas de mercado.
- **Proporcionalidade e Adequação:** os controles devem ser compatíveis com a natureza, complexidade e perfil de risco das atividades, sendo revisados periodicamente para manter sua efetividade.

- **Segregação de Funções:** atividades críticas devem ser segregadas para reduzir riscos de erros, fraudes e conflitos de interesse.
- **Documentação e Formalização:** processos, riscos e controles devem ser formalizados, atualizados e mantidos acessíveis para auditorias, supervisões e consultas internas.
- **Monitoramento e Avaliação de Controles:** os controles internos devem ser submetidos a monitoramento e avaliações periódicas de sua adequação e efetividade, observados os critérios e procedimentos estabelecidos em normativo interno específico.
- **Ação Corretiva:** não conformidades devem gerar planos de ação, acompanhados até sua resolução, seguindo as regras da gestão de não conformidades.
- **Cultura de Controles e Capacitação:** deve ser mantido programa periódico de capacitação relacionado a riscos, Compliance e ao Sistema de Controles Internos, contemplando, quando aplicável, a Estrutura de Gestão de Riscos e observando atenção especial aos colaboradores em posições de maior responsabilidade ou envolvidos em atividades de maior risco.
- **Metas e Incentivos:** é vedado o estabelecimento de metas de desempenho, incentivos ou mecanismos de remuneração que incentivem a assunção de riscos em desacordo com os níveis de risco definidos pela Alta Administração e pelo Conselho de Administração.
- **Proteção da Informação:** devem ser preservadas a confidencialidade, integridade e disponibilidade das informações, com controles de acesso físico e lógico adequados.
- **Transparência:** incidentes, riscos relevantes e deficiências de controles devem ser reportados de forma tempestiva e consistente à Alta Administração e aos Comitês.

- **Melhoria Contínua:** o Sistema de Controles Internos deve ser atualizado continuamente, incorporando lições aprendidas, recomendações de auditoria e mudanças regulatórias ou tecnológicas.

6. MECANISMOS DE CONTROLE

Controles Preventivos

- Limites e alçadas de aprovação.
- Automação e validação sistêmica.
- Segregação de funções.
- Treinamentos periódicos.
- Políticas de acesso físico e lógico.

Controles Detectivos

- Monitoramento contínuo de operações e indicadores de risco.
- Avaliações periódicas da adequação e efetividade dos controles, conforme normativo interno específico.
- Reconciliações automáticas.
- Auditorias internas/externas.

Controles Corretivos

- Planos de ação para falhas identificadas.
- Comunicação de incidentes à Alta Administração.
- Revisão dos controles após eventos adversos.

Controles Regulatórios

- Monitoramento de normas e atualizações regulatórias.
- Adequação dos normativos internos
- Controles destinados à prevenção, detecção e comunicação de operações suspeitas relacionadas à lavagem de dinheiro,

ao financiamento do terrorismo e a outros ilícitos, em conformidade com a regulamentação vigente.

Controles de Segurança da Informação

- Proteção de dados e privacidade (LGPD).
- Testes periódicos de segurança.
- Monitoramento de acessos e incidentes.

Controles de Continuidade e Contingência

- Planos de continuidade de negócios e contingência para situações de interrupção de serviços críticos;
- Testes periódicos dos planos de continuidade;
- Previsão de utilização de instalações remotas e de serviços prestados por terceiros, quando aplicável.

7. RESPONSABILIDADES

Conselho de Administração

- Aprovar esta política e revisões.
- Garantir estrutura adequada de governança e recursos.
- Supervisionar o SCI.

Diretoria de Governança e Gestão

- Assegurar a efetividade do Sistema de Controles Internos (SCI).
- Promover a cultura de controles internos no Conglomerado BS2.
- Garantir a independência da área responsável pelo SCI.

- Reportar periodicamente o funcionamento e a efetividade do SCI ao Comitê de Riscos e às instâncias competentes.
- Assegurar recursos, autonomia e capacitação adequados às atividades relacionadas aos controles internos.
- Garantir a adequada segregação de funções.
- Atuar como diretor(a) responsável pelo Sistema de Controles Internos das entidades para as quais estiver formalmente designado(a), observadas as atribuições, designações e comunicações requeridas pelo Banco Central do Brasil, pela SUSEP e pelos demais órgãos reguladores aplicáveis.
- Validar o Relatório Anual de Controles Internos, previamente à sua submissão às instâncias competentes, conforme a regulamentação e a governança aplicáveis a cada entidade.

Riscos Não Financeiros e Controles Internos

- Propor, revisar e disseminar esta Política.
- Coordenar a metodologia de identificação, avaliação, monitoramento e reporte dos riscos não financeiros e controles internos.
- Manter e monitorar o inventário de riscos e controles, em conjunto com as áreas responsáveis.
- Avaliar periodicamente a adequação e a efetividade dos controles internos, conforme normativo interno específico.
- Elaborar o planejamento periódico de avaliação dos controles internos, observados os critérios estabelecidos no normativo interno aplicável.
- Executar as avaliações dos controles internos com independência em relação às áreas responsáveis por sua execução.
- Documentar e reportar os resultados das avaliações e deficiências identificadas às instâncias competentes.

- Acompanhar os respectivos planos de ação até sua conclusão.
- Incorporar à metodologia e ao processo de monitoramento, quando aplicável, mudanças regulatórias, recomendações de auditoria, incidentes e lições aprendidas.
- Elaborar e submeter o Relatório Anual de Controles Internos às instâncias competentes, observados os requisitos regulatórios e a governança aplicável a cada entidade.

Compliance

- Reportar não conformidades
- Acompanhar adequação das não conformidades.
- Promover e apoiar ações de orientação e capacitação relacionadas a ética, conduta e conformidade.

Jurídico Regulatório

- Identificar, avaliar e monitorar os riscos de conformidade, em conjunto com as demais áreas responsáveis, conforme aplicável.
- Orientar as áreas quanto às medidas necessárias para assegurar a conformidade regulatória.

Tecnologia e Segurança da Informação

- Definir, implementar e manter controles de tecnologia e segurança da informação alinhados ao Sistema de Controles Internos.

- Assegurar a confidencialidade, integridade e disponibilidade das informações e dos sistemas.
- Monitorar, tratar e reportar incidentes de segurança da informação e vulnerabilidades relevantes.
- Monitorar, tratar e reportar incidentes de tecnologia relevantes.

Atuar de forma integrada às áreas de Riscos, Controles Internos e Compliance.

Áreas de Negócio (1ª Linha)

- Executar e manter controles atualizados.
- Avaliar riscos e reportar incidentes.
- Executar planos de ação.
- Garantir segregação de funções.

Auditoria Interna (3ª Linha)

- Avaliar, de forma independente, a efetividade do SCI.
- Emitir recomendações e acompanhar correções.
- Reportar ao COAUD e Conselho de Administração.

8. CONSIDERAÇÕES FINAIS

Esta política entra em vigor na data de sua aprovação e deve ser amplamente divulgada, sendo revisada anualmente ou quando houver alterações regulatórias relevantes.