BPP-007
POLÍTICA DE GESTÃO DE RISCOS E CONTROLES INTERNOS

Sumário

1. Objetivo
2. Público Alvo
3. Diretrizes
4. Definições
4.1. COSO* (Committee of Sponsoring Organizations of the Treadway Commission)
4.2. Controles Internos
4.3. Riscos
4.4. Gestão de Riscos
4.5. Risco Operacional
4.6. Risco de Liquidez
5. Sobre a Estrutura de Gerenciamento de Riscos
5.1. Risco Operacional
5.1.1. Risco operacional deve prever *(Circular 3.681 - BACEN):*
5.2. Risco de Liquidez
5.2.1. Risco de liquidez deve prever *(Circular 3.681 - BACEN):*
5.2.2. Controles Internos deve prever *(Circular 2.554 - BACEN):*
6. Papéis e Responsabilidades
6.1. 1ª Linha de Defesa
6.2. 2ª Linha de Defesa
6.3. 3ª Linha de Defesa - Caberá a Auditoria Interna
6.4. Comitê BPP
6.5. Demais áreas da BPP

1. Objetivo

Em conformidade com a Circular nº 3.681, Resolução nº 2.554 e seu Código de Conduta da BPP, a BPP Instituição de Pagamento S/A estabelece as diretrizes e padrões de controles que garantam a adequação, fortalecimento e o funcionamento do Sistema de Gestão de Riscos e Controles Internos da BPP Instituição de Pagamento S/A.

2. Público Alvo

Todos os colaboradores da BPP.

3. Diretrizes

Esta política tem como diretriz divulgar as atividades de **controle** e **monitoramento** que visem mitigar os **riscos** de acordo com a complexidade dos negócios da BPP. Os riscos são identificados e avaliados de acordo com a probabilidade de ocorrência e impacto nos resultados.

4. Definições

4.1. COSO* (Committee of Sponsoring Organizations of the Treadway Commission)

COSO* Termo em inglês que em sua tradução significa Comitê de Organizações Patrocinadoras da Comissão de Monitoramento.

Refere-se a uma proposta de trabalho em controles internos que resulte numa estrutura integrada de gerenciamento de riscos corporativos. Formado por elementos mínimos de uma estrutura de controle, que se propõe a controlar melhor suas atividades visando o cumprimento dos objetivos estabelecidos pela estratégia das organizações.

4.2. Controles Internos

São ações que devem permitir às **áreas de controles** e a estrutura de Governança da BPP monitorar os processos operacionais e financeiros, assim como os riscos de desconformidade estabelecidos na Circular 3.681 (BACEN).

4.3. Riscos

São eventos externos e internos que podem ocorrer e afetar positivamente ou negativamente, os objetivos, processos ou projetos da BPP.

4.4. Gestão de Riscos

Tem como objetivo adotar medidas com o potencial de prevenir ou eliminar tais riscos, identificando os processos falhos e riscos de alto impacto, possibilitando uma mitigação eficaz dos riscos.

4.5. Risco Operacional

Segundo a Circular 3.681 (BACEN), considera-se risco operacional "a possibilidade de ocorrência de perdas resultantes dos seguintes eventos:

a) falhas na proteção e na segurança de dados sensíveis relacionados tanto às credenciais dos usuários finais quanto a outras informações trocadas com o objetivo de efetuar transações de pagamento;
b) falhas na identificação e autenticação do usuário final;
c) falhas na autorização das transações de pagamento;
d) fraudes internas;
e) fraudes externas;
f) demandas trabalhistas e segurança deficiente do local de trabalho;
g) práticas inadequadas relativas a usuários finais, produtos e serviços de pagamento;
h) danos a ativos físicos próprios ou em uso pela instituição;
i) ocorrências que acarretem a interrupção das atividades da instituição de pagamento ou a descontinuidade dos serviços de pagamento prestados;
j) falhas em sistemas, processos ou infraestrutura de tecnologia da informação; e
k) falhas na execução, cumprimento de prazos e gerenciamento das atividades envolvidas em arranjos de pagamento.

4.6. Risco de Liquidez

Segundo a Circular 3.681 (BACEN), considera-se risco de liquidez "a possibilidade de a instituição de pagamento:

a) não ser capaz de honrar eficientemente suas obrigações esperadas e inesperadas, correntes e futuras sem afetar suas operações diárias e sem incorrer em perdas significativas; e

b) não ser capaz de converter moeda eletrônica em moeda física ou escritural no momento da solicitação do usuário.

5. Sobre a Estrutura de Gerenciamento de Riscos

5.1. Risco Operacional

A **estrutura de gerenciamento de risco operacional** é composta pela Diretoria, Comitê Executivo BPP e pelas áreas de controles:

- Áreas de Negócio;
- Segurança da Informação;
- Riscos & Compliance;

A **Auditoria Interna** é responsável pela verificação do gerenciamento de risco operacional e do funcionamento de sua estrutura.

5.1.1. Risco operacional deve prever *(Circular 3.681 - BACEN):*

- Plano de contingência e outros mecanismos que garantam a continuidade dos serviços de pagamento prestados;
- mecanismos de proteção e segurança dos dados armazenados, processados ou transmitidos;
- mecanismos de proteção e segurança de redes, sítios eletrônicos, servidores e canais de comunicação com vistas a reduzir a vulnerabilidade a ataques;
- procedimentos para monitorar, rastrear e restringir acesso a dados sensíveis, redes, sistemas, bases de dados e módulos de segurança;
- monitoramento das falhas na segurança dos dados e das reclamações dos usuários finais a esse respeito;
- revisão das medidas de segurança e de sigilo de dados, especialmente depois da ocorrência de falhas e previamente a alterações na infraestrutura ou nos procedimentos;
- elaboração de relatórios que indiquem procedimentos para correção de falhas identificadas;
- realização de testes que assegurem a robustez e a efetividade das medidas de segurança de dados adotadas;
- segregação de funções nos ambientes de tecnologia da informação destinados ao desenvolvimento, teste e produção;
- identificação adequada do usuário final;

- mecanismos de autenticação dos usuários finais e de autorização das transações de pagamento;
- processos para assegurar que todas as transações de pagamento possam ser adequadamente rastreadas;
- mecanismos de monitoramento e de autorização das transações de pagamento, com o objetivo de prevenir fraudes, detectar e bloquear transações suspeitas de forma tempestiva;
- avaliações e filtros específicos para identificar transações consideradas de alto risco;
- notificação ao usuário final acerca de eventual não execução de uma transação; e
- mecanismos que permitam ao usuário final verificar se a transação foi executada corretamente.

5.2. Risco de Liquidez

A **estrutura de gerenciamento de risco de liquidez** é composta pela Diretoria, Comitê Executivo BPP e pelas áreas de controles:

- Tesouraria;
- Controladoria;
- Riscos & Compliance;

A **Auditoria Interna** é responsável pela verificação do gerenciamento de risco de liquidez e do funcionamento de sua estrutura.

5.2.1. Risco de liquidez deve prever *(Circular 3.681 - BACEN):*

- Processos para identificar, avaliar, monitorar e controlar a exposição ao risco de liquidez em diferentes horizontes de tempo;
- plano de contingência de liquidez que estabeleça responsabilidades e procedimentos para enfrentar situações de estresse de liquidez;
- evidenciar a estrutura de gerenciamento do risco de liquidez em relatório de acesso público, com periodicidade mínima anual.

5.2.2. Controles Internos deve prever *(Circular 2.554 - BACEN):*

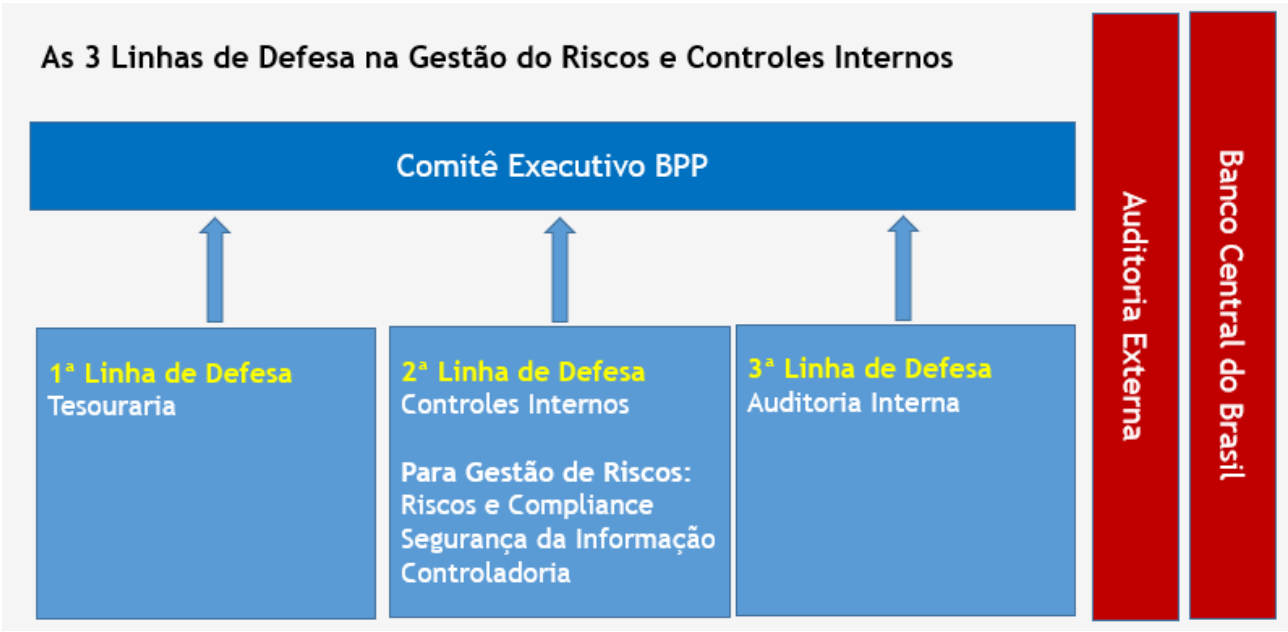
- A definição de responsabilidades dentro da instituição;
- A segregação das atividades atribuídas aos integrantes da instituição de forma a que seja evitado o conflito de interesses, bem como meios de minimizar e

monitorar adequadamente áreas identificadas como de potencial conflito da espécie;

- Meios de identificar e avaliar fatores internos e externos que possam afetar adversamente a realização dos objetivos da instituição;
- A existência de canais de comunicação que assegurem aos funcionários, segundo o correspondente nível de atuação, o acesso a confiáveis, tempestivas e compreensíveis informações consideradas relevantes para suas tarefas e responsabilidades;
- A contínua avaliação dos diversos riscos associados às atividades da instituição;

6. Papéis e Responsabilidades

A BPP adota a metodologia das 3 (três) linhas de defesa para operacionalizar sua estrutura de gerenciamento de Riscos e Controles Internos, de forma a assegurar o cumprimento das diretrizes definidas neste documento.



6.1. 1ª Linha de Defesa:

Risco Operacional

- A 1ª Linha de Defesa é composta por todas as áreas da BPP IP SA exceto Riscos e Compliance e de Segurança da Informação que compõem a 2ª Linha de Defesa.

- É papel da 1ª Linha a identificação e avaliação de riscos, criação e manutenção de controles internos, comunicação dos riscos ao Comitê Executivo BPP, 2ª Linha de Defesa e Auditoria Interna

Risco de Liquidez

- A 1ª Linha de Defesa é composta pelas áreas de Tesouraria e de Controladoria da BPP.
- É papel da 1ª Linha o monitoramento, acompanhamento diário dos saldos das contas e aplicações, tal como, da comunicação à Diretoria BPP quanto aos desenquadramentos identificados, que possam materializar o risco de liquidez (contingência).

6.2. 2ª Linha de Defesa:

Controles Internos:

- É papel da 2ª Linha a avaliação periódica dos controles internos, da comunicação com o Comitê Executivo BPP e Auditoria Interna.

Risco Operacional

- É papel da 2ª Linha o apoio a 1ª Linha de Defesa na identificação e avaliação de riscos, a criação e manutenção de controles internos, da comunicação com o Comitê Executivo BPP e Auditoria Interna.

- Além disso, cabe a 2ª Linha de Defesa a avaliação de conformidade com regras do Bacen, mapeamento e monitoramento dos riscos.

Risco de Liquidez

- A 2ª Linha de Defesa é composta por Riscos e Compliance.
- É papel da 2ª Linha o apoio a 1ª Linha de Defesa na identificação e avaliação de riscos, a criação e manutenção de controles internos, da comunicação com o Comitê Executivo BPP e Auditoria Interna.
- Além disso, cabe a 2ª Linha de Defesa a avaliação de conformidade com regras do Bacen, avaliação dos controles internos, mapeamento e monitoramento dos riscos.

6.3. 3ª Linha de Defesa - Caberá a Auditoria Interna:

I - a efetividade e a eficiência dos sistemas e processos de controles internos e de governança corporativa;
II - a efetividade das políticas e das estratégias para o gerenciamento dos riscos relevantes, considerando os riscos atuais e potenciais riscos futuros;
III - a confiabilidade, a efetividade e a integridade dos processos e sistemas de informações gerenciais;
IV - a observância ao arcabouço legal, à regulamentação infralegal, às recomendações dos organismos reguladores e aos códigos e normas internos aplicáveis aos membros do quadro funcional da instituição;
V - a salvaguarda dos ativos e as atividades relacionadas à função financeira da instituição; e
VI - as atividades, os sistemas e os processos recomendados ou determinados pelo Banco Central do Brasil, no exercício de suas atribuições de supervisão.

6.4. Comitê BPP:

Aprovar e revisar:

a. Política de Gestão do Riscos e Controles Internos.
b. Política de Segurança da Informação.
c. Política de Segurança Cibernética.
d. Política de Continuidade de Negócios.
e. Tratativas, transferências ou aceite de riscos.
f. Acompanhar mensalmente o controle orçamentário.
g. Deliberar sobre a movimentação necessária de recursos financeiros para correção do desencaixe identificado pela Tesouraria.
h. Acionar o Plano de Contingência quando necessário.
i. Deliberar sobre as recomendações feitas por Controles Internos a respeito de eventuais deficiências, com o estabelecimento de cronograma de saneamento das mesmas, quando for o caso;
j. Deliberar sobre a manifestação dos responsáveis pelas correspondentes áreas a respeito das deficiências encontradas em verificações anteriores e das medidas efetivamente adotadas para saná-las;
k. Promover elevados padrões éticos e de integridade e de uma cultura organizacional que demonstre e enfatize, a todos os funcionários, a importância dos controles internos e o papel de cada um no processo.

6.5. Demais áreas da BPP:

Caberá à todos os **colaboradores**:

- Informar tempestivamente riscos não mapeados, sejam eles novos ou não identificados anteriormente;
- Registrar no **Formulário para Registro de Ocorrências / Incidentes** ocorrências que de alguma maneira impactaram a BPP, tendo ou não perda financeira, bem como descrever as ações corretivas e planos de ação (quando cabível) para mitigar futuras materializações.