CARTILHA DE RISCO OPERACIONAL,

COMPLIANCE E ÉTICA

Uso Externo

Novembro/2022

SUMÁRIO

1 Apresentação

Esta Cartilha de Risco Operacional, Compliance e Ética é destinada aos parceiros e terceirizados do Bandes, e consiste numa compilação dos principais conceitos associados ao risco operacional, Compliance e código de ética do banco.

Espera-se que a disseminação do conhecimento sobre o assunto funcione como um indutor à reflexão e revisão dos processos operacionais por parte dos parceiros e terceirizados, com reflexos positivos sobre a mitigação dos riscos operacionais e sobre a qualidade dos serviços prestados.

2 Risco Operacional

2.1 O que é Risco Operacional?

Conforme explicitado na Política de Gerenciamento de Risco Operacional e Controles Internos, considera-se risco operacional ***"a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos"***.

Esta definição inclui o risco legal, que é o risco associado à inadequação ou deficiência em contratos firmados pela instituição, bem como a sanções em razão do descumprimento de dispositivos legais e a indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela instituição.

2.2 Fatores de Riscos

- **Pessoas** - Relacionam-se à competência, habilidades, atitudes, bem como conduta ética no desempenho das suas atribuições;
- **Processos** - Fluxos e etapas do desenvolvimento de produtos e serviços e condução de atividades da organização, definição dos normativos internos e aderência à legislação;
- **Sistemas** - Infra-estrutura e arquitetura de TI, disponibilidade de armazenamento, processamento e rede; e
- **Eventos Externos** - Relacionados com as ocorrências do meio ambiente, do ambiente social e do ambiente regulatório do país.

2.3 Categorias de Eventos de Risco Operacional

- **Fraudes Internas** - perdas ocasionadas por atos com intenção de fraudar, apropriar-se indevidamente ou burlar regulamentos, leis ou as políticas da empresa, que envolvam pelo menos uma parte interna, excluindo diversidade/acontecimentos discriminatórios;
- **Fraudes e Roubos Externos** - perdas ocasionadas por atos com intenção de fraudar, apropriar-se indevidamente ou burlar leis, praticados por um terceiro;
- **Demandas trabalhistas e segurança deficiente do local de trabalho** - perdas decorrentes de atos inconsistentes com contratos ou leis trabalhistas, saúde, segurança, pagamento de reclamações por lesões corporais, ou de diversidade/eventos discriminatórios;
- **Práticas inadequadas relativas a clientes, produtos e serviços** - perdas decorrentes de uma falha não-intencional ou negligente para cumprir uma obrigação profissional com clientes específicos (incluindo exigências fiduciárias e de adequação ao perfil do cliente), ou da natureza ou desenho de um produto ou serviço;

- **Danos a ativos físicos próprios ou em uso pela empresa** - prejuízos decorrentes de perdas ou danos aos ativos físicos ocasionados por desastres naturais ou outros acontecimentos;
- **Falhas em sistemas de tecnologia da informação** - perdas decorrentes de falhas em sistema;
- **Falhas na execução, cumprimento de prazos e gerenciamento das atividades** - perdas decorrentes na administração, condução, execução e gerenciamento das atividades vinculadas aos processos internos; e
- **Interrupção das atividades** - perdas decorrentes de ruptura nos negócios, ocasionadas pela ausência ou não fornecimento de serviços essenciais, seja de agentes internos ou externos à empresa.

3 Gerenciamento do Risco Operacional

O risco operacional está presente em todos os processos internos da empresa e pode ser decorrente de falhas operacionais em qualquer etapa destes processos, sejam estas de caráter humano, tecnológico ou de modelagem.

Todos os níveis hierárquicos da empresa devem entender que têm papéis e responsabilidades em relação à gestão do risco operacional em suas atividades para a eficácia na sua gestão.

A implementação de controles internos é fundamental para a gestão eficiente do risco operacional. Quando bem definidos, auxiliam a empresa a minimizar a probabilidade de incorrer em grandes perdas financeiras, seja por meio da redução na probabilidade de erros humanos, seja na redução das falhas e irregularidades em processos e sistemas.

Dado que entre os fatores de risco existe a possibilidade de ocorrência de **eventos externos** adversos, tais como tumultos, blecautes, inundações, epidemias, dentre outros, que são alheios à vontade e ao aos controles existentes e podem provocar interrupções drásticas nestes processos, a empresa deve possuir um plano de contingência e continuidade de negócios que possibilite a manutenção das operações em condições mínimas para que as consequências dessa interrupção sejam as menores possíveis.

3.1 Ações de Mitigação do Risco Operacional

A identificação de ações mitigadoras está associada à forma de condução dos processos internos e ao tipo e nível de controle interno utilizado, entretanto, algumas ações têm caráter genérico e se aplicam a qualquer situação, como por exemplo:

- **Pessoas**: adequado processo de seleção e recrutamento, ações de capacitação e treinamento, existência de Código de Ética e Normas de Conduta, política adequada de remuneração e outros;
- **Processos**: mapeamento de processos, definição e implantação de controles internos; formalização dos procedimentos operacionais, política de *compliance* e outros;

- **Sistemas**: implantação de controles de acesso (físicos e lógicos), instalação de programas antivírus, backup periódico de dados, política de uso de equipamentos móveis, internet e *e-mail,* dentre outros;
- **Eventos Externos**: implantação de plano de continuidade de negócios, com definição dos processos críticos, processos alternativos, tempo de reestabelecimento, dentre outros.

3.2 Segurança da Informação

Segurança da Informação remete à ideia de que informações ou conhecimentos estão seguros e protegidos contra pessoas que não precisam ou não devam ter acesso a tais dados.

Os riscos de Segurança da Informação (SI) devem ser administrados para assegurar que os objetivos do negócio sejam alcançados e que os eventos indesejados sejam evitados ou detectados e endereçados satisfatoriamente.

No tratamento dos riscos, podem ser considerados como sinalizadores de vulnerabilidades:

- senha exposta ou compartilhada;
- indícios de desrespeito às normas que regem a propriedade intelectual de livros, textos, imagens e outros produtos protegidos por direito autoral;
- informações corporativas descartadas inadequadamente;
- informações corporativas guardadas inadequadamente;
- gavetas e/ou armários abertos ou chaves expostas.

Dentre os controles aplicáveis estão:

- ✓ controle de acesso aos Sistemas – pequeno ou grande portes;
- ✓ gestão de *logs*;
- ✓ restrição ao armazenamento de arquivos indevidos;
- ✓ requerimentos de autenticação de Usuário;
- ✓ classificação da informação por nível de importância ou criticidade;
- ✓ confirmação de leitura de documentos; e
- ✓ procedimentos adequados de descarte de informações.

3.3 Segurança de Pessoas e Ambientes

Para a segurança física e do ambiente podem servir como sinalizadores de vulnerabilidades:

- pontos de acesso às dependências sem controle ou vigilância;
- inexistência de identificação no acesso de terceiros; e
- inexistência de mecanismos de proteção física nas dependências da empresa.

Dentre os controles aplicáveis estão:

- ✓ controle de acesso automatizado;
- ✓ equipamento contra incêndio;
- ✓ sistema de monitoramento fechado de TV; e
- ✓ elaboração de Mapa de Riscos de Acidentes do Trabalho.

4 Compliance e Ética

4.1 O que é Compliance?

Deriva do verbo inglês "to comply", que significa dever de cumprir, isto é, estar em conformidade e fazer cumprir leis, decretos, regulamentos e instruções aplicáveis à atividade da Instituição, que, na hipótese de não cumprimento, podem gerar sanções, perda financeira e danos à reputação/imagem.

4.2 Programa de Compliance Bandes

O Programa de Compliance consiste na definição de mecanismos para prevenir, detectar e responder a desvios de conduta e atos ilícitos, atuando preventivamente e reparando eventuais danos à imagem do Bandes. . Para atingir os objetivos propostos o Programa de Compliance do Bandes apresenta três pilares:

a) Prevenção: A etapa de Prevenção contra atos de desvio de conduta traduz-se como o conjunto de mecanismos de proteção desenvolvidos para redução da ocorrência de fraude e corrupção no contexto organizacional, sendo adotadas as seguintes medidas preventivas:
   - Estabelecimento e divulgação do Código de Ética, Conduta e Integridade
   - Disseminação da Cultura da Ética e Integridade
   - Definição de um Programa de Due Diligence para Funcionários, Clientes e Fornecedores
   - Estabelecimento de uma Política de Prevenção Lavagem de Dinheiro e Combate ao Financiamento do Terrorismo
   - Monitoramento das Mudanças Regulatórias

b) Detecção
   - Constituição de um Canal de Denúncias
   - Desenvolvimento de um plano de Auditoria Interna
   - Testes de Compliance

c) Resposta
   - Desenvolvimento do processo de investigação
   - Estabelecimento de medidas corretivas

4.3 Código de Conduta para Fornecedores e Parceiros de Negócios

O Bandes possui Código de Conduta para Fornecedores e Parceiros de Negócios que deve ser conhecido e observado pelos seus prestadores de serviços e parceiros de negócios, observando-se os seguintes aspectos fundamentais:

- Qualidade dos Produtos e Serviços -
- Saúde e Segurança
- Respeito às Leis Trabalhistas
- Relacionamento com os empregados do Bandes

4.4 Orientações de Conduta

São orientações de conduta aplicáveis aos prestadores de serviços e parceiros de negócios do Bandes:

- Promover apenas negociações relacionadas ao atendimento de interesses corporativos.
- Manter a confidencialidade e o sigilo de todas as informações do Bandes que venham a ter acesso, ou que lhes sejam confiadas, em razão das atividades executadas no âmbito dos contratos
- Não utilizar softwares não homologados ou não licenciados nos equipamentos do Bandes ou ainda que os nossos fornecedores utilizem softwares não homologados e não licenciados para a prestação de serviços
- não oferecer brindes, presentes, convites, empréstimos, jantares, viagens ou qualquer outro benefício que possa afetar o julgamento ou estimular tratamentos diferenciados entre si.
- Não é permitida a utilização da imagem, nome ou marca do Bandes, exceto se previamente e formalmente autorizada para uso exclusivo no desenvolvimento de sua atividade profissional.

O Bandes atua com tolerância zero em relação a quaisquer atos de corrupção. Espera-se que todos os fornecedores e parceiros de negócio mantenham a preocupação com este tema e reportem quaisquer preocupações para o Canal de Denúncias e Comissão de Ética.

O Bandes se reserva o direito de, a qualquer tempo, auditar se os fornecedores e parceiros de negócios estão cumprindo as diretrizes deste Código ou da legislação aplicável às suas operações.

4.5 Canais de Comunicação e denúncia

O Bandes disponibiliza um Canal de Denúncias que possibilita o recebimento de denúncias internas e externas relativas ao descumprimento deste Código das demais normas da Instituição.

Em caso de dúvida quanto à aplicação do presente Código de Conduta, poderá ser feita uma consulta à Comissão de Ética, também por meio de um registro no Canal de Denúncias.

São disponibilizadas as seguintes formas de comunicação:

Website:
https://www.bandes.com.br/Site/CanalDeDenuncia/CanalDeDenuncia;

Telefone: 0800 283 4202.

5 Referências Bibliográficas

- Resolução nº 4.557, de 23.02.2017, do Conselho Monetário Nacional
- Resolução nº 4.595, de 28.08.2017, do Conselho Monetário Nacional
- Política Institucional de Gerenciamento de Risco Operacional e Controles Internos
- Política Institucional de Compliance (Compliance)
- Política Institucional de Código de Conduta para Fornecedores e Parceiros de Negócio