| gerencianet | POLÍTICA DE GESTÃO DO RISCO OPERACIONAL | Emissão<br>21/02/2020 | Classificação<br>Pública |
|---|---|---|---|
| Identificação<br>PUB POL RIO | | Versão<br>1.0 | Tipo Documento<br>Política |

## 1. INTRODUÇÃO

A política de gestão do risco operacional da Gerencianet foi construída baseando-se nas diretrizes do Banco Central do Brasil que, por meio da Circular 3.681/13, dispõe sobre gerenciamento de riscos (dentre outros temas) para instituições de pagamento.

O risco operacional é definido como a possibilidade de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos que impactem na realização dos objetivos da Gerencianet.

Salienta-se também que, conforme art. 2º, parágrafo único da Circular 3.681/13, a definição do risco operacional também inclui o risco legal associado à:

- Inadequação ou deficiência em contratos firmados pela Gerencianet;
- Sanções em razão de descumprimento de dispositivos legais;
- Indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela Gerencianet.

## 2. OBJETIVO

Esta política é o instrumento formal para definição das diretrizes a serem observadas na concepção, implantação e manutenção de estratégias, processos e controles do risco operacional.

## 3. ABRANGÊNCIA

Esta política é aplicável e deverá ser cumprida, obrigatoriamente, por todos os colaboradores da Gerencianet, prestadores de serviços que atuem em nome da empresa ou participem em operação de processos críticos de sua cadeia produtiva.

## 4. DEFINIÇÕES

Para os efeitos deste documento, aplicam-se os termos e definições contidos no "Anexo I".

## 5. ESTRUTURA DO GERENCIAMENTO DO RISCO OPERACIONAL

O gerenciamento do risco operacional está centralizado no "Controles Internos e Gestão de Riscos", subordinado diretamente à Presidência da instituição. Desta forma, resultando em uma estrutura mais enxuta e ágil na tomada de decisões.

A estrutura de gerenciamento de riscos operacionais deve prever, de acordo com os incisos I ao XVIII do art. 4º da Circular 3.681/13, no mínimo, os seguintes aspectos:

- Plano de contingência e outros mecanismos que garantam a continuidade dos serviços prestados pela instituição;
- 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;
- Mecanismos que permitam ao usuário final verificar se a transação foi executada corretamente;
- Critérios de decisão quanto à terceirização de serviços e de seleção de seus prestadores;
- Avaliação, gerenciamento e monitoramento do risco operacional decorrente de serviços terceirizados relevantes para o funcionamento regular da instituição de pagamento.

## 6. ABRANGÊNCIA

Para a efetividade do gerenciamento, são adotados processos para identificar, analisar e avaliar, monitorar e controlar a exposição aos riscos operacionais que a instituição está exposta.

Esta estrutura está formalizada em política e norma que define a metodologia, processos e responsabilidades na gestão de riscos na instituição. O controle do risco operacional permite a atuação preventiva e corretiva, evitando a ocorrência de novos eventos e reincidência de falhas.

Alinhado ao conceito apresentado nas melhores práticas de gestão de riscos, como a norma ISO 31000 e ao artigo 4º da Circular 3.681/13, a estrutura de gerenciamento do risco operacional atua de forma a:

- *Identificar:* eventos internos e externos que influenciam o risco operacional são identificados e classificados;

- *Analisar e Avaliar:* os riscos são analisados e avaliados considerando a probabilidade e o impacto para determinar o modo pelo qual deverão ser tratados e administrados;
- *Controlar e Mensurar:* a política, os limites, os indicadores e os procedimentos são estabelecidos e implementados para mensurar o risco e seus impactos, assegurando respostas eficazes;
- *Monitorar:* o monitoramento é realizado através de atividades gerenciais contínuas ou de avaliações específicas;
- *Mitigar:* mitigação através de atividades gerenciais contínuas e de avaliações independentes;
- *Reportar:* fornecimento de tempestivas informações e análises sobre o risco de operacional, bem como as conclusões e providências adotadas.

## 7. GESTÃO DO RISCO OPERACIONAL

A gestão do risco operacional integra-se aos objetivos da instituição, de forma a alinhar os processos existentes e praticados com as políticas e normas vigentes.

A estrutura de gerenciamento do risco operacional favorece uma ação compartilhada e multidisciplinar, na qual os colaboradores de cada área são os especialistas do processo e desempenham importante papel em uma gestão integrada de riscos.

A eficiência do processo de gestão do risco operacional é um fator determinante para um adequado mecanismo de análise de riscos e definição de controles, uma vez que permite atuação tempestiva da instituição com decisões equilibradas, evitando desperdícios de recursos ou perdas associadas ao risco operacional.

### 7.1. Metodologia e Instrumentos

Em linha com as melhores práticas de gestão de riscos, a Gerencianet adota uma abordagem qualitativa que consiste no estabelecimento e na disseminação de políticas claras, métodos e técnicas padronizados e aplicáveis à Gerencianet, tendo como objetivo a adoção de processos da ISO 31000, como identificação, análise, avaliação e tratamento de riscos.

A metodologia contempla, mas não se limita, aos seguintes instrumentos:

- Mapeamento de processos críticos para a instituição;
- Matriz de riscos e controles;
- Testes de controles;
- Planos de ação para mitigação dos riscos;
- Base histórica de ocorrências.

### 7.2. Classificação dos Eventos de Risco Operacional

A Gerencianet considera, dentre outros aspectos possíveis, as classificações de seus eventos de risco operacional de acordo com o art. 2º da Circular 3.681/13, a saber:

- 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;
- Falhas na identificação e autenticação do usuário final;
- Falhas na autorização das transações de pagamento;
- Fraudes internas;
- Fraudes externas;
- Demandas trabalhistas e segurança deficiente do local de trabalho;
- Práticas inadequadas relativas a usuários finais, produtos e serviços de pagamento;
- Danos a ativos físicos próprios ou em uso pela Gerencianet;
- Ocorrências que acarretem a interrupção das atividades da Gerencianet ou a descontinuidade dos serviços de pagamento prestados;
- Falhas em sistemas de TI (Tecnologia da Informação);
- Falhas na execução, cumprimento de prazos e gerenciamento das atividades desenvolvidas pela Gerencianet.

## 7.3. Três Linhas de Defesa

A estrutura de gestão de riscos da Gerencianet considera a atuação conjunta de todos os departamentos e colaboradores da instituição, de acordo com o conceito das "Três Linhas de Defesa". Por tal abordagem, as linhas de defesa são envolvidos com o gerenciamento de riscos conforme explanado a seguir:

- *1ª Linha de Defesa:* composta por todos os gestores das áreas da instituição, os quais são responsáveis pela gestão primária dos riscos e responsáveis diretos pelos processos presentes em sua área.
- *2ª Linha de Defesa:* composta pelas áreas de "Controles Internos e Gestão de Riscos", sendo responsáveis por determinar as metodologias e políticas de risco que a Gerencianet deverá seguir, bem como avaliar de forma independente a efetividade da gestão de risco realizada pelo primeiro nível de defesa. A atuação é segregada e independente das atividades e da gestão das áreas negócio e da Auditoria Interna, reportando-se diretamente à Presidência da instituição.
- *3ª Linha de Defesa:* composta pela área de "Auditoria Interna", responsável por avaliar, de forma independente, a adequação e eficácia do modelo geral de gestão de risco, da adequação dos controles internos e das estruturas de governança, reportando eventuais deficiências encontradas diretamente à Presidência da instituição.

Embora a Alta Administração não esteja considerada entre as três linhas de defesa, nenhuma consideração sobre gestão de riscos estaria completa sem levar em conta, em primeiro lugar, o papel primordial exercido por tal instância, que é uma das principais partes interessadas e que está em melhor posição para instituir e assegurar o bom funcionamento das três linhas de defesa no processo de gestão de riscos e controles da instituição.

## 7.4. Comunicação e Reporte

O processo de avaliação dos riscos operacionais engloba a contínua comunicação entre todos os gestores das áreas da Gerencianet com o departamento de "Controles Internos e Gestão de Riscos".

A comunicação deve ser feita por um processo estruturado contemplando reportes periódicos de avaliação, bem como relatório de andamento e relatório final anual.

Complementa o processo de comunicação e reporte as divulgações de atualização das políticas relacionadas, do andamento de ações corretivas e da divulgação de melhores práticas.

## 7.5. Gestão de Terceiro Relevante

Para fins desta política, entende-se por "terceiro relevante" aquele prestador de serviço cuja atividade profissional, dada a sua relevância e imprescindibilidade, constitui elemento essencial para a Gerencianet e que, se malconduzida e/ou não fiscalizada de forma adequada, pode trazer riscos sistêmicos de alto custo para a instituição.

A Gerencianet possui mecanismos definidos para a gestão de terceiros relevantes, incluindo cláusulas de prestação de serviços conhecidas pelas partes envolvidas.

# 8. AÇÕES DE MITIGAÇÃO DO RISCO OPERACIONAL

A adoção de ações de mitigação do risco operacional na instituição está associada à forma de condução dos processos internos e ao tipo e nível de controle interno utilizado, todavia, algumas ações possuem caráter genérico e podem se aplicar a qualquer situação, como por exemplo, mas não se limitando a:

- *Fator de risco "pessoas":* adequado processo de seleção e recrutamento, ações de treinamentos periódicos, existência de Código de Ética e Conduta, políticas institucionais acessíveis por qualquer colaborador em qualquer momento etc.;
- *Fator de risco "processos":* identificação e mapeamento de processos e riscos, definição e implantação de controles internos, endereçamento de controles a riscos, formalização de procedimentos operacionais etc.;
- *Fator de risco "sistemas":* implantação de controles de acesso (físicos e lógicos), utilização de softwares antivírus/antimalware, backups periódicos, política de uso aceitável de ativos de informação, proteção contra códigos maliciosos, política de acesso à Internet etc.;
- *Fator de risco "eventos externos":* implantação do plano de continuidade de negócios (PCN), com definição e mapeamento dos processos críticos, aplicação do BIA (Business Impact Analysis) para visualização de prováveis impactos dos principais processos de negócio mapeados da instituição em caso de interrupção dos mesmos etc.

## 9. REVISÃO E ATUALIZAÇÃO

Esta política será revisada anualmente, e sua alteração acontecerá caso seja constatada necessidade de atualização do seu conteúdo. Poderá, ainda, ser alterada a qualquer tempo em razão de circunstâncias que demandem tal providência, conforme entendimento da Gestão da Gerencianet.

## 10. CONSIDERAÇÕES FINAIS

Outras políticas, normas, procedimentos ou termos, bem como outros complementares que detalhem ou evidenciem esta matéria, serão mantidas à disposição dos colaboradores, reguladores e auditorias.

## ANEXO I – GLOSSÁRIO COM DEFINIÇÕES E TERMOS

**EVENTO:** incidente ou ocorrência, a partir de fontes internas ou externas a uma entidade, capaz de afetar a realização dos objetivos.

**RISCO OPERACIONAL:** a Circular BCB 3.681/13 dispõe sobre o gerenciamento de riscos, dentre outros aspectos. Por isso, para os efeitos desta política, o conceito de risco operacional será o descrito na referida Circular, em seu art. 2º define o risco operacional como a possibilidade de ocorrência de perdas resultantes dos seguintes eventos:

- 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;
- Falhas na identificação e autenticação do usuário final;
- Falhas na autorização das transações de pagamento;
- Fraudes internas;
- Fraudes externas;
- Demandas trabalhistas e segurança deficiente do local de trabalho;
- Práticas inadequadas relativas a usuários finais, produtos e serviços de pagamento;
- Danos a ativos físicos próprios ou em uso pela Gerencianet;
- Ocorrências que acarretem a interrupção das atividades da Gerencianet ou a descontinuidade dos serviços de pagamento prestados;
- Falhas em sistemas de TI (Tecnologia da Informação);
- Falhas na execução, cumprimento de prazos e gerenciamento das atividades desenvolvidas pela Gerencianet.

Salienta-se também que, conforme art. 2º, parágrafo único da Circular 3.681/13, a definição do risco operacional também inclui o risco legal associado à:

- Inadequação ou deficiência em contratos firmados pela Gerencianet;
- Sanções em razão de descumprimento de dispositivos legais;
- Indenizações por danos a terceiros decorrentes das atividades desenvolvidas pela Gerencianet.