POLÍTICA DE GESTÃO INTEGRADA DE RISCOS

Nome do Documento	Política de Gestão Integrada de Riscos
Descrição	Política cujo objetivo é estabelecer as diretrizes gerais, critérios e procedimentos adotados para o gerenciamento dos riscos integrados.
Tipo	Política
Versão	3.0
Nível de Confidencialidade	Público
Acesso Reservado ao	Público
Área Responsável	Diretoria Operacional
Data da Aprovação	01/07/2024

Histórico das alterações			
Data	**Versão**	**Criado por**	**Descrição da alteração**
29/11/2021	1.0	Barcellos & Tucunduva Advogados	Versão Inicial do Documento
11/11/2022	2.0	Lauriney Leite dos Santos	Revisão e Atualização
04/01/2024	3.0	Mariana Dutra de Morais	Revisão e Atualização
15/06/2024	4.0	Mariana Dutra de Morais e Lucas Pereira da Silva	Revisão, Atualização e Ampliação

SUMÁRIO

1. OBJETIVO

Esta Política de Gerenciamento de Riscos tem o objetivo de estabelecer as diretrizes gerais, critérios e procedimentos adotados para o gerenciamento dos riscos, a salvaguarda dos recursos mantidos em contas de pagamento e o tratamento de incidentes relevantes relacionados ao ambiente cibernético, a fim de possibilitar a identificação, avaliação, monitoramento, tratamento, comunicação dos riscos da **BEETELLER INSTITUIÇÃO DE PAGAMENTO LTDA** (BEETELLER), em atendimento à regulamentação do Banco Central do Brasil e às melhores práticas.

2. ABRANGÊNCIA

A Política se aplica a todos os administradores (coletivamente "Alta Administração" ou "Diretoria"), funcionários e prestadores de serviços[1] da BEETELLER (coletivamente, inclusive a Alta Administração ou Diretoria, denominados simplesmente por, "Colaboradores").

O gerenciamento de riscos é inerente à atividade da BEETELLER e, portanto, é dever de todos o cumprimento desta Política. Cabe à Alta Administração ou Diretoria, ou à área por ela determinada, a divulgação e implementação de suas medidas e procedimentos.

3. REFERÊNCIAS

- **Lei nº 12.865/2013:** dispõe sobre os Arranjos de Pagamento e as Instituições de Pagamento integrantes do Sistema de Pagamentos Brasileiro (SPB).
- **Resolução BCB n° 25/2020:** Altera a Circular nº 3.681, de 4 de novembro de 2013, que dispõe sobre o gerenciamento de riscos, os requerimentos mínimos de patrimônio, a governança de instituições de pagamento, a preservação do valor e da liquidez dos saldos em contas de pagamento, e dá outras providências.
- **Resolução BCB n° 80/2021**: Disciplina a constituição e o funcionamento das instituições de pagamento, estabelece os parâmetros para ingressar com pedidos de autorização de funcionamento por parte dessas instituições e dispõe sobre a prestação de serviços de pagamento por outras instituições autorizadas a funcionar pelo Banco Central do Brasil.
- **Resolução BCB nº 81/2021**: Disciplina os processos de autorização relacionados ao funcionamento das instituições de pagamento e à prestação de serviços de pagamento por parte de outras instituições autorizadas a funcionar pelo Banco Central do Brasil.
- **Resolução Conjunta nº 01/2020**: dispõe sobre a implementação do Sistema Financeiro Aberto (Open Finance).
- **Resolução BCB nº 01/2020**: institui o arranjo de pagamentos PIX e aprova o seu Regulamento.
- **Resolução BCB n° 197/2022**: Classifica o conglomerado prudencial integrado por ao menos uma instituição que realize serviço de pagamento e estabelece a segmentação

[1] Quaisquer terceiros que atuem em nome da BEETELLER, tais como Auditoria Externa, Assessoria Jurídica, Tecnologia da Informação, Infraestrutura de TI, dentre outras.

para os conglomerados prudenciais classificados como Tipo 3 para fins de aplicação proporcional da regulação prudencial.

- **Resolução BCB n° 198/2022**: Dispõe sobre o requerimento mínimo de Patrimônio de Referência de Instituição de Pagamento (PRIP) de conglomerado do Tipo 2, nos termos da Resolução BCB nº 197/2022, e de instituição de pagamento não integrante de conglomerado prudencial, e sobre a metodologia de apuração desses requerimentos e a respectiva estrutura de gerenciamento contínuo de riscos.
- **Resolução CMN nº 3.919/2010**: Altera e consolida as normas sobre cobrança de tarifas pela prestação de serviços de pagamento aos usuários finais, inclusive para efeitos de remuneração.

4. DEFINIÇÕES

- **Alta Administração**: gestores que integram o nível mais elevado da companhia com poderes para estabelecer as políticas, os objetivos e conduzir a implementação da estratégia para realizar os objetivos da organização;
- **Arranjo de Pagamento**: conjunto de regras e procedimentos que disciplina a prestação de determinado serviço de pagamento ao público pela Lei nº 12.865/2013.
- **Bacen:** Banco Central do Brasil.
- **Conta de Pagamento:** conta de titularidade do Usuário, destinada ao carregamento, transferência e resgate de recursos, cujos valores, convertidos em moeda eletrônica, serão geridos e custodiados pela BEETELLER.
- **Instituição de Pagamento:** para fins desta Política, é a BEETELLER como emissora de moeda eletrônica, cuja atividade consiste em gerenciar a Conta de Pagamento de Usuários, utilizada para o pagamento de transações pré-pagas.
- **Open Finance:** compartilhamento padronizado de dados e serviços por meio de abertura e integração de sistemas**.**
- **Pix:** arranjo de pagamentos instituído pelo Bacen que disciplina a prestação de serviços de pagamento relacionados com as Transações de pagamentos instantâneos no âmbito do arranjo.
- **Risco:** possibilidade de materialização de evento que resulte em impactos negativos à operação dos negócios da BEETELLER.
- **Risco Operacional:** possibilidade de ocorrência de perdas resultantes de falhas, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos. A abrangência dessa definição inclui também o risco legal associado à inadequação ou deficiência em contratos firmados, além de sanções que possam ser impostas em razão do descumprimento de dispositivos legais e indenizações por danos a terceiros.
- **Risco de Liquidez:** potencialidade de descasamento de fluxos financeiros de ativos e passivos, bem como de seus reflexos sobre a capacidade financeira da BEETELLER em obter recursos e honrar suas obrigações.
- **Risco Ambiental**: a possibilidade de ocorrência de perdas para a instituição ocasionadas por eventos associados à degradação do meio ambiente, incluindo o uso excessivo de recursos naturais;

- **Risco Climático:** o risco climático tem duas vertentes, a saber, risco de transição e de risco físico.
- **Risco Climático de Transição**: é possibilidade de ocorrência de perdas para a instituição ocasionadas por eventos associados ao processo de transição para uma economia de baixo carbono, em que a emissão de gases do efeito estufa é reduzida ou compensada e os mecanismos naturais de captura desses gases são preservados;
- **Risco Climático Físico:** é a possibilidade de ocorrência de perdas para a instituição ocasionadas por eventos associados a intempéries frequentes e severas ou a alterações ambientais de longo prazo, que possam ser relacionadas a mudanças em padrões climáticos;
- **Risco Social**: a possibilidade de ocorrência de perdas para a instituição ocasionadas por eventos associados à violação de direitos e garantias fundamentais ou a atos lesivos a interesse comum.
- **Sistema de Pagamentos**: serviços relacionados à abertura de Conta de Pagamento e realização de Transações de carregamento, transferência e resgate de recursos pelo Usuário, incluindo a disponibilização de informações sobre a movimentação e fornecimento de extratos.
- **Transação**: operação em que o Usuário realiza a movimentação de sua Conta de Pagamento, realizando o carregamento de recursos, a transferência de recursos para a Conta de Pagamento de titularidade de outros usuários, ou o resgate de recursos para a conta bancária do Usuário ou de terceiro por ele indicado.
- **Usuário**: pessoa física ou jurídica, titular da Conta de Pagamento que, ao aderir ao termo de abertura de Conta de Pagamento, está habilitada a realizar Transações por meio do Sistema de Pagamentos.
- **Matriz de Risco:** diretriz para a avaliação qualitativa e/ou quantitativa do efeito dos riscos nos objetivos estratégicos da BEETELLER.
- ***Risk Appetite Statements* (“RAS”)**: trata-se do Apetite de Tolerância ao Risco, definido como o nível de variação aceitável quanto à realização de um determinado objetivo.
- **Plano de Resposta aos Riscos**: conjunto de medidas adotadas para diminuir o risco inerente a um nível que esteja em consonância com a Tolerância ao Risco da BEETELLER.
- **Incidente:** trata-se da materialização do risco.
- **Perda:** É a consequência da materialização dos riscos, seja ela esperada ou inesperada.

5. PRINCIPIOS DA GESTÃO DE RISCOS

Conforme a ISO 31000:2018 o gerenciamento de riscos tem como propósito a criação e proteção de valor, de maneira eficaz e eficiente baseada em princípios que permitam a organização a gerenciar os efeitos da incerteza nos seus objetivos. Os princípios desta política de gestão de riscos estão são permeados em linha com os melhores guias de referência, para promoção da melhoria contínua de forma inclusiva, dinâmica e integrada, com base na melhor informação disponível, respeitando as

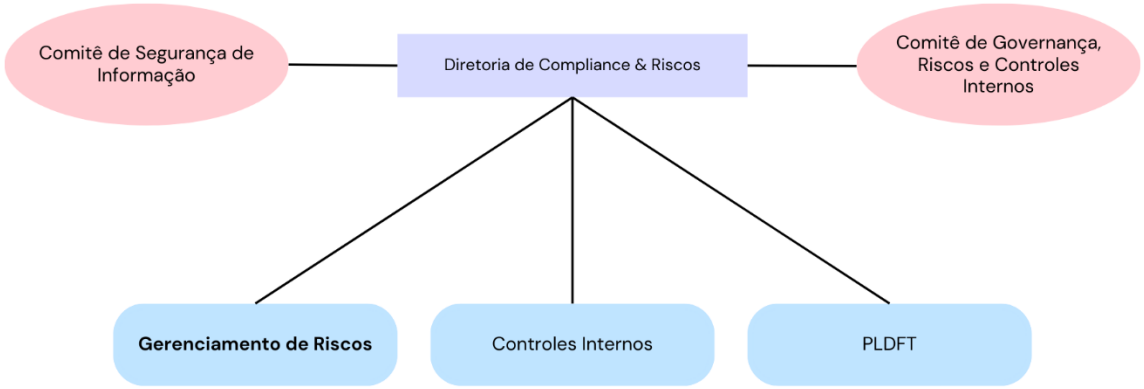
peculiaridades existentes nos processos da Organização, bem como os aspectos culturais e humanos.

6. ESTRUTURA DE GERENCIAMENTO DE RISCOS

Para assegurar a efetividade desta Política, a Estrutura de Gerenciamento de Riscos (“Estrutura de Riscos”) prevê uma atuação compartilhada para a gestão de cada risco. Todos os Colaboradores que desempenham atividades correlatas aos riscos objeto desta Política têm o dever de zelar pela conformidade dos processos de gerenciamento de riscos.

A Estrutura de Gerenciamento de Riscos deverá prever políticas e estratégias aprovadas e revisadas, periodicamente, pela Alta Administração e/ou Diretoria, para determinar sua compatibilidade com os objetivos da BEETELLER e com as condições de mercado; e deverá manter esta documentação acerca das políticas, estratégias de gerenciamento de riscos e governança à disposição do Bacen, com critérios de decisão quanto à terceirização de serviços e de seleção de seus prestadores, incluindo as condições contratuais mínimas necessárias para mitigar o risco operacional, e a continuidade dos serviços de pagamento prestados.

O envolvimento da Alta Administração e Diretores é contínuo e se dá na condução da gestão e na participação de comitês, notadamente o Comitê de Risco e Comitê de Segurança da Informação. Aos comitês deverão ser apresentados relatórios periódicos demonstrando o desempenho da estrutura de gerenciamento de riscos, os planos de mitigação de riscos, continuidade de negócios, relatórios de avaliação de riscos sobre produtos e serviços, novas tecnologias, também caberá a manutenção das RAS e outras demandas, respectivamente as suas atribuições e responsabilidades.



7. PROCESSO DE GESTÃO DE RISCOS

Com as devidas reservas às técnicas de gestão de riscos financeiros e não financeiros, o processo de gestão de riscos da Beeteller é pautado no guia de referência ISO 31000:2018, observando o contexto, identificação, análise, avaliação, tratamento, monitoramento e comunicação. Uma vez identificados os riscos financeiros, deverão ser avaliados a partir de técnicas reconhecidas pela literatura, evitando avaliações subjetivas sobre as possíveis perdas.

- **Contexto**: Os contextos externos e internos na qual a Beeteller opera devem ser considerados para a definição adequada dos objetivos, visto que, a gestão dos riscos ocorre no contexto dos objetivos e atividades da organização. Fatores sociais, culturais, políticos, jurídicos, regulatórios, financeiros, tecnológicos, econômicos e ambientais, em nível local, regional, nacional ou internacional podem interferir diretamente e ou indiretamente nos objetivos da Organização.

- **Identificação**: A etapa de identificação de riscos consiste em encontrar, reconhecer e descrever riscos que possam afetar de maneira positiva ou negativa no alcance dos objetivos definidos pela Beeteller. Dentre os fatores que devem ser considerados nesta fase estão as fontes tangíveis e intangíveis de riscos, causas e ventos, ameaças e oportunidades, mudanças nos contextos, consequências e impactos nos objetivos, limitações de conhecimento e de confiabilidade das informações, vieses, hipóteses e crença dos envolvidos e outros fatores que forem considerados relevantes.

- **Análise de riscos**: A análise de riscos tem por finalidade compreender a natureza e características do risco. Deve ser realizada considerando a análise detalhada das incertezas, fontes de risco, consequências, probabilidades, eventos, cenários, controle e sua eficácia. Convém que sejam registradas e comunicadas possíveis influências na

análise dos riscos oriundas de opiniões, vieses, julgamentos e percepções de risco para colaborar com a melhor tomada de decisão.

- **Avaliação de riscos:** A avaliação de riscos tem como propósito apoiar a tomada de decisão, através da comparação do resultado da análise dos riscos agregando os critérios de risco estabelecidos para determinar se e onde é necessária uma ação adicional como manter os controles existentes, reconsiderar os objetivos, não fazer nada ou realizar análises adicionais para compreender melhor os riscos.

- **Tratamento de riscos**: O tratamento de riscos é a etapa da implementação de melhorias através de planos de ação, planos de mitigação de riscos, recomendações de gestão de continuidade de negócios, estabelecimento de procedimentos operacionais, limites operacionais. Os riscos devem ser selecionados para tratamento balanceando o custo versus benefício, esforços ou desvantagens da implementação das ações de tratamento.

- **Monitoramento e comunicação**: O monitoramento deve ocorrer em todas as etapas do processo de gestão de riscos e deve incluir o planejamento, coleta e análise de informações, registro de resultados e fornecimento de retorno. Os resultados do processo de gestão de riscos devem ser devidamente documentados e comunicados por canais adequados visando comunicar as atividades e resultados da gestão de riscos, fornecer informações para tomada de decisão, melhorar as atividades de gestão de riscos e auxiliar a interação com todas as partes interessadas.

8. RESPONSABILIDADES

8.1. Alta Administração ou Diretoria

- Definir os objetivos organizacionais observando os resultados gerados pelo processo de gestão de riscos;
- Aprovar e revisar, anualmente, a Política de Gerenciamento de Riscos;
- Aprovar os planos estratégicos de gestão de risco, os limites de Tolerância ao Risco (RAS), plano de mitigação de riscos e plano de gestão de continuidade de negócios;
- Manifestar-se sobre as ações incluídas nos relatórios Controles Internos, bem como fazer constar nos relatórios, sua responsabilidade sobre as informações divulgadas;
- Garantir que a estrutura de remuneração da instituição não incentive comportamentos incompatíveis com os níveis de apetite a risco dispostos na RAS;
- Promover a disseminação da cultura de gerenciamento de riscos na instituição;
- Assegurar recursos adequados e suficientes para o exercício das atividades de gerenciamento de riscos, de forma independente, objetiva e efetiva;
- Assegurar o cumprimento desta política;
- Nomear o Diretor de Riscos (CRO).

8.2. Diretor de Compliance e Riscos

- Definir objetivos do departamento, determinar a elaboração e ou revisão das políticas e procedimentos relacionados ao planejamento estratégicos de risco, definir a prioridade de construção e aplicação das matrizes de riscos, acompanhar e reportar se os limites de Tolerância ao Risco estão sendo respeitados, determinar a elaboração e ou revisão do Plano de Mitigação de Riscos e plano de gestão de continuidade de negócios;
- Avaliar e garantir a adequação, à RAS e aos objetivos estratégicos da instituição, da política, dos processos, dos relatórios, dos sistemas e dos modelos utilizados no gerenciamento de risco de operacional;
- Monitorar o processo de gestão de riscos;
- Monitorar outros riscos relevantes, como, por exemplo, a não conformidade com leis e regulamentos aplicáveis a instituição;
- Informar periodicamente à Alta Administração ou Diretoria sobre os resultados oriundos do processo de gestão de riscos;
- Assegurar a integração desta política nas atividades da organização, respectivamente, as partes interessadas;
- Reportar eventuais inconsistências diretamente à Alta Administração;
- Identificar mudanças nos contextos externos e internos;
- Elaborar treinamentos e ações de disseminação de cultura de conformidade.

8.3. Comitê de Governança, Riscos & Controles Internos

- Analisar as revisões da política de gerenciamento de risco operacional no mínimo anualmente;
- Compreender, de forma abrangente e integrada, os riscos que podem impactar o capital e a liquidez;
- Assessorar a Alta Administração no desempenho de suas atribuições relacionadas à adoção de estratégias, políticas e medidas voltadas à disseminação da cultura, mitigação de riscos e da conformidade com as normas aplicáveis.
- Consumir os relatórios oriundos do processo de monitoramento de riscos;
- Dirimir sobre eventos específicos que causem ou possam causar impactos relevantes na organização;
- Assegurar a conformidade no âmbito da governança da Organização;
- Deliberar sobre situações atípicas oriundas do programa de Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo;
- Garantir a implementação de melhorias definidas no processo de gestão de riscos.

8.4. Comitê de Segurança da Informação

- Apreciar as revisões as políticas e diretrizes de segurança da informação e cibernética;
- Avaliar os diversos tipos de riscos relacionados à Segurança Cibernética e continuidade de negócios e deliberar sobre as ações de mitigação apresentadas.

- Acompanhar periodicamente o resultado do processo de monitoramento de riscos cibernéticos;
- Atuar na resolução de eventos de riscos cibernéticos que se materializaram, garantindo o adequado registro do evento, das ações de correção, das ações para mitigar nova ocorrência do mesmo risco e a devida guarda do dossiê que documenta o respectivo processo.

8.5. Área de Gestão de Riscos

- Elaborar e documentar as políticas, estratégias, planos de mitigação de riscos e de continuidade de negócios;
- Apresentar relatórios periódicos para o Comitê de Governança, Riscos & Controles Internos e para a Alta Administração;
- Implementar estrutura de gerenciamento de riscos com base nas normas internas, externas e nas melhores práticas de mercado;
- Disseminar a cultura de gestão de riscos, compartilhar o conhecimento sobre o tema e subsidiar as demais áreas visando o melhor desempenho possível;
- Auxiliar na definição de apetite de risco, bem como reportar adequadamente as informações relacionadas ao tema em todas as linhas de negócio;
- Aplicar as metodologias adequadas para os riscos financeiros (mercado e liquidez), riscos organizacionais (estratégicos e operacionais) para identificar, avaliar, monitorar, mensurar, controlar e mitigar os riscos, buscando a melhoria contínua, junto aos gestores de cada área bem como os comitês e a Alta Administração;
- Elaborar relatórios sobre o desempenho da gestão de riscos financeiros e organizacionais no mínimo anualmente;
- Documentar, armazenar, classificar e agregar as informações referentes às perdas associadas ao risco operacional;
- Identificar previamente os riscos inerentes a novos produtos e serviços, bem como em produtos e serviços existentes, mudanças significativas em processos, sistemas, operações, modelo de negócio e reorganizações societárias significativas;
- Disseminar à instituição, em seus diversos níveis, o apetite a risco documentado na RAS, bem como o procedimento para reporte de ocorrência relacionadas a não observância dos níveis de apetite por riscos.

8.6. Área de Controles Internos

- Garantir a segurança razoável das operações da Beeteller;
- Realizar testes de aderência;
- Avaliar a eficiência dos controles internos com base em riscos;
- Identificar oportunidades de melhoria nos procedimentos operacionais;
- Apoiar na estruturação e gestão dos riscos;
- Contribuir no processo de prevenção de fraudes internas e externas;
- Apoiar nas investigações internas quando solicitado;
- Apoiar a manutenção de processos operacionais alinhados com a estratégia e apetite a risco da instituição.

- Intermediar as demandas oriundas das auditorias interna e externa, assim como, nas inspeções por parte do regulador e ou de outras autoridades;
- Atuar de forma proativa na manutenção da conformidade, principalmente, no programa de Prevenção à Lavagem de Dinheiro e Financiamento do Terrorismo.

8.7. Auditoria Interna

- Incluir no planejamento da auditoria a verificação do desempenho do processo de gestão de riscos e de continuidade de negócios;
- Reportar à Alta Administração possíveis riscos identificados através da condução da auditoria;
- Desenvolver um plano de auditoria anual priorizando processos que exponham a instituição a um maior risco e um planejamento cíclico de longo prazo com possibilidade de ajustes ao longo do tempo em caso de necessidade;
- Avaliar a eficácia dos controles estabelecidos para assegurar conformidade com as políticas, procedimentos, leis, regras e objetivo do negócio;
- Avaliar os métodos de salvaguardas de ativos da organização e seus clientes;
- Avaliar a confiabilidade e segurança das informações financeiras e gerenciais, além dos sistemas e operações que geram esses dados;
- Acompanhar os pontos identificados para assegurar o cumprimento das ações recomendadas, no prazo estabelecido.
- Atuar consultivamente com as áreas para a correção de inconformidades e para a melhoria contínua dos controles.

8.8. Área de Segurança da Informação

- Identificar, classificar, documentar processos críticos de negócio, bem como avaliar potenciais impactos decorrentes de interrupção deles;
- Estabelecer estratégias para assegurar a continuidade das atividades da instituição;
- Elaborar planos de continuidades de negócios que estabeleçam procedimentos e prazos estimados para reinício e recuperação das atividades em caso de interrupção dos processos críticos de negócio, bem como as ações de comunicação necessárias;
- Realizar testes e revisões dos planos de continuidade de negócios com periodicidade adequada;
- Assegurar a integridade, segurança e disponibilidade de dados e dos sistemas de informação utilizados, sendo adequados às necessidades e às mudanças do modelo de negócio, incluindo mecanismos de proteção e segurança da informação com vistas a prevenir, detectar e reduzir a vulnerabilidade de ataques digitais;
- Implementar estrutura de governança de TI consistente com os níveis de apetite por riscos estabelecidos na RAS.

8.9. Área Antifraude

- Prevenir, identificar e responder a fraudes;

- Garantir a conformidade no compartilhamento de situações de fraudes;
- Garantir a salvaguarda dos documentos relativos ao compartilhamento de fraudes;
- Elaborar relatório anual com dados quantitativos e qualitativos sobre o processo de prevenção a fraudes;
- Proteger os ativos da BEETELLER e dos seus clientes;
- Informar à Área de Gestão de Riscos qualquer situação risco identificado no desempenho de suas atividades;
- Auxiliar nas respostas a usuários e clientes relativas ao processo de prevenção de fraudes;

9. TIPOS DE RISCOS

A gestão integrada de riscos, também conhecida como gestão de riscos empresariais (ERM), é um componente essencial para melhorar a governança corporativa ao apoiar o processo de tomada de decisão para atingir os objetivos da organização, pois permite aos tomadores de decisão identificarem as ações necessárias para mitigar, transferir ou aceitar os riscos. Ademais, o processo de gestão integrada de riscos ajuda a melhorar os controles internos dos processos de negócios, enfatizando os riscos considerados essenciais que serão identificados, avaliados e aprimorados pelos controles essenciais da instituição.

9.1. RISCOS ORGANIZACIONAIS

9.1.1. Riscos Operacionais

Considera-se Risco Operacional a possibilidade de ocorrência de perda e/ou prejuízos decorrentes de situações internas ou externas ou de falha, deficiência ou inefetividade de processos internos, pessoas ou sistemas. Também se considera dentro do escopo do risco operacional o risco legal, associado à inconformidade ou não observância da legislação em contratos firmados, além de sanções que possam ser impostas em razão das mencionadas inobservâncias legais.

São exemplos de possíveis riscos operacionais, mas não se limitando, os abaixo mencionados:

- 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 BEETELLER;

- Ocorrências que acarretem a interrupção das atividades da BEETELLER de pagamento ou a descontinuidade dos serviços de pagamento prestados.
- Falhas em sistemas, processos ou infraestrutura de tecnologia da informação;
- Falhas na execução, cumprimento de prazos e gerenciamento das atividades envolvidas em arranjos de pagamento;
- Falhas na iniciação de transação de pagamento.

9.1.2. Riscos Estratégicos

Os riscos estratégicos ajudam ou prejudicam os objetivos estratégicos da Beeteller. Eles podem trazer oportunidades ou ameaças para a organização. Os modelos de percepção, que são fornecidos pelos especialistas que participam do processo de gestão estratégica, são usados para identificar e medir esses riscos. Isso permite a construção de matrizes de riscos que incorporam as duas facetas da ameaça e da oportunidade. A reavaliação dos riscos estratégicos deve ocorrer anualmente e ser considerada no planejamento estratégico desta instituição.

9.1.3. Riscos Cibernéticos

Dentro do escopo dos riscos operacionais, destaca-se o risco cibernético em razão do modelo de negócio da BEETELLER. Entende-se por risco cibernético a probabilidade de exposição, perda financeira e de ativos críticos e informações sensíveis e de danos à reputação como resultado de um ataque ou violação cibernética na rede de uma organização.

A BEETELLER adota metodologia de avaliação e tratamento de riscos inerentes à segurança da informação com o propósito de definir o nível aceitável de riscos de acordo com a norma ISO/IEC 27001. A avaliação de riscos aplica-se a todo o escopo do Sistema de Gestão da de segurança da Informação (SGSI), isto é, prioritariamente a todos os ativos constantes na declaração de aplicabilidade ou aqueles que podem ter um impacto relevante sobre a segurança da informação ou proteção de dados pessoais no SGSI.

São referência para a aplicação da metodologia a Norma ISO/IEC 27001 nas cláusulas 6.1.2, 6.1.3, 8.2 e 8.3, a Política de segurança da informação e cibernética, a lista de requisitos legais, regulatórios, contratuais e outros e a Declaração de aplicabilidade, todos eles documentos integrantes do SGSI.

A BEETELLER, em caso de incidente de segurança da informação ou incidente relevante, realiza o tratamento de incidentes através do registro, comunicação, a análise do risco, análise da causa e do impacto, bem como o controle dos efeitos de incidentes de acordo com sua relevância e conforme a classificação das informações envolvidas e o impacto na continuidade dos serviços.

São adotados procedimentos para mitigar os efeitos dos incidentes relevantes e a interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a

substituição da empresa contratada e o reestabelecimento da operação normal da instituição;

Os cenários de incidentes considerados nos testes de continuidade de serviços de pagamento prestados, constam no plano de continuidade de serviços, parte integrante do SGSI.

9.1.4. O SGSI trata-se de um conjunto de documentos em sua maioria classificados como de uso INTERNO e poderá ser disponibilizado a autoridades regulatórias se solicitado. O SGSI é auditado anualmente internamente e externamente por auditores independentes para fins de certificação ISO27001.

No que diz respeito ao tratamento de incidentes relevantes, sempre que ocorrerem, deverá ser elaborado um plano de ação visando a melhoria ou implementação de um controle.

9.2. RISCOS FINANCEIROS

9.2.1. Riscos de Liquidez

Considera-se evento de Risco de Liquidez a incapacidade de arcar, de forma eficaz, com as obrigações financeiras esperadas e inesperadas, correntes e futuras, sem que sejam afetadas as operações diárias da BEETELLER e sem incorrer em perdas significativas.

São exemplos de possíveis riscos operacionais, mas não se limitando, os abaixo mencionados:

- A incapacidade de honrar, eficientemente, as obrigações esperadas e inesperadas, correntes e futuras, sem que sejam afetadas as operações diárias da BEETELLER e sem incorrer em perdas significativas;
- A incapacidade de converter moeda eletrônica em moeda física ou escritural no momento da solicitação do usuário.

O Risco de Liquidez pode ser classificado como:

- **Risco de descasamento**: a possibilidade de que as diferenças entre as estruturas de vencimentos dos ativos e os passivos gerem um descasamento no caixa. Isto levaria a incapacidade de honrar seus pagamentos e, pela natureza do negócio, esse risco está relacionado principalmente à incapacidade de honrar os recursos utilizados pelos clientes.
- **Risco de Financiamento**: a possibilidade de que a BEETELLER seja incapaz de cumprir suas obrigações decorrentes da incapacidade de vender ativos ou financiar-se;
- **Risco de Contingência**: a possibilidade de não dispor de opções adequadas para a obtenção de liquidez como consequência de um evento externo que implique maiores necessidade de financiamento.

9.3. OUTROS RISCOS RELEVANTES

9.3.1. Risco Social, Ambiental e Climático

Define-se o risco social como a possibilidade de ocorrência de perdas para a instituição ocasionadas por eventos associados à violação de direitos e garantias fundamentais ou a atos lesivos a interesse comum.

Por sua vez, o risco ambiental é definido como a possibilidade de ocorrência de perdas para a instituição ocasionadas por eventos associados à degradação do meio ambiente, incluindo o uso excessivo de recursos naturais.

Por fim, o risco climático, em suas vertentes de risco de transição e de risco físico, é definido como: risco climático de transição: possibilidade de ocorrência de perdas para a instituição ocasionadas por eventos associados ao processo de transição para uma economia de baixo carbono, em que a emissão de gases do efeito estufa é reduzida ou compensada e os mecanismos naturais de captura desses gases são preservados; risco climático físico: possibilidade de ocorrência de perdas para a instituição ocasionadas por eventos associados a intempéries frequentes e severas ou a alterações ambientais de longo prazo, que possam ser relacionadas a mudanças em padrões climáticos.

São exemplos de riscos social, ambiental e climático, mas não se limitando, os abaixo mencionados:

Risco Social:

- Ato de assédio, de discriminação ou de preconceito com base em atributos pessoais, tais como etnia, raça, cor, condição socioeconômica, situação familiar, nacionalidade, idade, sexo, orientação sexual, identidade de gênero, religião, crença, deficiência, condição genética ou de saúde e posicionamento ideológico ou político;
- Prática relacionada ao trabalho em condições análogas à escravidão;
- Exploração irregular, ilegal ou criminosa do trabalho infantil;
- Prática relacionada ao tráfico de pessoas e à exploração sexual.

Risco Ambiental:

- Existir alguma conduta ou atividade irregular, ilegal ou criminosa contra a fauna ou a flora, incluindo desmatamento, provocação de incêndio em mata ou floresta, degradação de biomas ou da biodiversidade e prática associada a tráfico, crueldade, abuso ou maus-tratos contra animais;
- Poluição irregular, ilegal ou criminosa do ar, das águas ou do solo;
- Exploração irregular, ilegal ou criminosa dos recursos naturais, relativamente à degradação do meio ambiente, entre eles recursos hídricos, florestais, energéticos e minerais, incluindo, quando aplicável, a implantação e o desmonte das respectivas instalações;

- Desastre ambiental resultante de intervenção humana, relativamente à degradação do meio ambiente, incluindo rompimento de barragem, acidente nuclear ou derramamento de produtos químicos.

Risco Climático de transição:

- Alteração em legislação, em regulamentação ou em atuação de instâncias governamentais, associada à transição para uma economia de baixo carbono, que impacte negativamente a instituição;
- Inovação tecnológica associada à transição para uma economia de baixo carbono que impacte negativamente a instituição;
- Alteração na oferta ou na demanda de produtos e serviços, associada à transição para uma economia de baixo carbono, que impacte negativamente a instituição;
- Percepção desfavorável dos clientes, do mercado financeiro ou da sociedade em geral que impacte negativamente a reputação da instituição relativamente ao seu grau de contribuição na transição para uma economia de baixo carbono; e

Risco Climático Físico:

- Condição climática extrema, incluindo seca, inundação, enchente, tempestade, ciclone, geada e incêndio florestal; e
- Alteração ambiental permanente, incluindo aumento do nível do mar, escassez de recursos naturais, desertificação e mudança em padrão pluvial ou de tempera.

A estrutura de gerenciamento dos riscos social, ambiental e climático abrange todos os processos, pessoas e sistemas que dão suporte à identificação, avaliação, mensuração, monitoramento, controle e reporte desses riscos na BEETELLER.

10. MATRIZ DE CLASSIFICAÇÃO DE TRANSAÇÕES DE RISCO

Todo problema identificado por meio dos instrumentos descritos nas etapas anteriores exige análise e definição de planos de ação, visando à melhoria dos processos e manutenção dos níveis de risco dentro dos patamares de exposição aceitáveis de acordo com RAS definido pela BEETELLER.

- **Definição do RAS**: o RAS será definido e aprovado de acordo com as responsabilidades da Estrutura de Risco. O procedimento interno da BEETELLER irá descrever o processo relativo à construção e monitoramento do limite de risco operacional.
- **Mapeamento dos riscos e controles das atividades**: a BEETELLER determinará sua Matriz de Riscos, com o objetivo de identificar os riscos associados aos processos/atividades, classificando-os quanto à probabilidade e ao impacto, suas consequências e controles utilizados. A sua aplicação tem o objetivo de fornecer uma visão integral do fluxo do processo, suas dependências e interações.

11. GESTÃO DE CONTINGÊNCIAS E DE CONTINUIDADE DE NEGÓCIOS

A fim de se garantir os objetivos desta Política, a BEETELLER deve elaborar políticas a procedimentos específicos para o tratamento de contingências gestão de continuidade de negócios, observando-se as seguintes diretrizes:

- A efetividade da implementação do plano, políticas e procedimentos para a gestão de contingência e de continuidade de negócios, seguindo as atribuições e responsabilidades da Estrutura de Riscos;
- O tratamento adequado para o gerenciamento de crise, da continuidade operacional e recuperação de desastres;
- A garantia de recursos, humanos e materiais, para a implementação do plano, políticas e procedimentos para a gestão da continuidade de negócios;
- A estabilidade organizacional em nível adequado durante a recuperação, após a indisponibilidade de processos e serviços críticos;
- A resposta adequada, coordenada e tempestiva em situações de crise;
- Assegurar a validação dos ambientes e procedimentos de contingência por meio de teste periódicos.
- Serão elaborados procedimentos a serem seguidos no caso de incidentes relevantes relacionados ao ambiente cibernético e da interrupção dos serviços relevantes de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo hipóteses que considerem a substituição da empresa contratada e o reestabelecimento da operação normal da instituição;
- Serão elaborados cenários de incidentes a serem considerados nos testes de continuidade de serviços de pagamento prestados;
- Serão estipulados prazos para reinício ou normalização das atividades ou dos serviços relevantes interrompidos;
- Serão elaborados procedimentos para gerenciamento de riscos no tocante à continuidade de negócios, da comunicação tempestiva ao Bacen das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes, que configurem uma situação de crise pela instituição de pagamento, bem como das providências para o reinício das atividades;
- Serão elaborados processos de auditoria interna dos mecanismos de acompanhamento e de controle da política de segurança cibernética.

12. PROCEDIMENTOS DE CORREÇÃO DE FALHAS

Os procedimentos de correção de falhas deverão abordar:

- **Identificação de Perdas Operacionais**: a apuração da perda decorrente de Incidente constitui fator importante para o cumprimento das exigências dos órgãos reguladores além de prover a BEETELLER com informações consistentes, padronizadas e atualizadas, decisivas para uma análise quantitativa do gerenciamento do risco na BEETELLER.

- **Avaliação da Qualidade dos Controles**: a avaliação dos controles tem como objetivo avaliar a efetividade/eficiência dos controles, a fim de verificar se estes estão sendo executados conforme descritos nas matrizes de risco e políticas internas.
- **Plano de Treinamento**: o plano de treinamento tem como objetivo, por meio de simulações de Incidentes e avaliação de Incidentes ocorridos, tem o objetivo de garantir que os Colaboradores estejam preparados para lidar com Incidentes e aptos a identificar situações de riscos e vulnerabilidades.

13. DA PARTICIPAÇÃO NO OPEN FINANCE

A BEETELLER, participando do Open Banking, atenderá os requisitos de compartilhamento de iniciação de transação de pagamento, quando solicitados pelos clientes, observando as regras impostas para o devido compartilhamento de dados das etapas do consentimento, da autenticação e da confirmação.

Todo o processo ocorrerá com segurança, agilidade, precisão e conveniência a serem realizados por meio da interface dedicada, realizadas exclusivamente por canais eletrônicos, de forma sucessiva e ininterrupta, e com duração compatível com os seus objetivos e nível de complexidade.

A BEETELLER deve assegurar que suas políticas para gerenciamento de riscos, bem como esta Política de Riscos Operacionais, disponham, com relação à continuidade de negócios, sobre:

- os procedimentos a serem seguidos no caso da indisponibilidade das interfaces utilizadas para o compartilhamento;
- o prazo estipulado para reinício ou normalização da disponibilidade da interface;
- o tratamento de incidentes relacionados com a violação da segurança dos dados relacionados ao compartilhamento e as medidas tomadas para a sua prevenção e solução; e
- a execução de testes de continuidade de negócios, considerando os cenários de indisponibilidade das interfaces e a avaliação dos seus resultados.

A BEETELLER é responsável pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação ao compartilhamento de dados e serviços em que esteja envolvida, bem como pelo cumprimento da legislação e da regulamentação em vigor.

A BEETELLER, previamente ao compartilhamento de dados pelo Open Banking, deverá:

- identificar o cliente e obter o seu consentimento por meio de linguagem clara, objetiva e adequada;
- informar as finalidades determinadas;

- ter o prazo de validade compatível com as finalidades determinadas, limitado a doze meses;
- discriminar a instituição transmissora de dados ou detentora de conta, conforme o caso;
- discriminar os dados ou serviços que serão objeto de compartilhamento, observada a faculdade de agrupamento dos dados;
- incluir a identificação do cliente.

É vedado à BEETELLER obter o consentimento do cliente por meio de contrato de adesão, formulário com opção de aceite previamente preenchido, ou de forma presumida, sem manifestação ativa pelo cliente. No caso de transações de pagamento sucessivas, o cliente, a seu critério, poderá definir prazo superior ao estabelecido, podendo condicionar o prazo de validade do consentimento ao encerramento das referidas transações.

É vedado a BEETELLER, nas atividades de ITP:

- armazenar o conjunto de dados relacionados com as credenciais de seus Clientes para autenticar a transação de pagamento perante a instituição detentora da conta, salvo quando os serviços forem prestados para as instituições autorizadas a funcionar pelo Banco Central do Brasil, com base em relação contratual, relativas a: (i) Política de Prevenção da Lavagem de Dinheiro e ao Financiamento do Terrorismo; (ii) a Política de Segurança Cibernética; (iii) e ao Sistema Financeiro Aberto (Open Banking);
- exigir de seus Clientes quaisquer outros dados além dos necessários para prestar o serviço de iniciação da transação de pagamento;
- utilizar, armazenar ou acessar os dados para outra finalidade que não seja a prestação do serviço de iniciação de transação de pagamento expressamente solicitado pelos clientes, salvo quando os serviços forem prestados para as instituições autorizadas a funcionar pelo Banco Central do Brasil, com base em relação contratual, relativas a: (i) Política de Prevenção da Lavagem de Dinheiro e ao Financiamento do Terrorismo; (ii) a Política de Segurança Cibernética; (iii) e ao Sistema Financeiro Aberto (Open Banking);
- alterar o montante ou qualquer outro elemento da transação de pagamento autorizada pelos Clientes; e
- iniciar transação de pagamento envolvendo conta de pagamento mantida por instituição não integrante do Sistema de Pagamentos Brasileiro.

14. DA APLICAÇÃO DOS RECURSOS MANTIDOS EM CONTAS DE PAGAMENTO

A BEETELLER deverá manter recursos líquidos correspondentes aos saldos de moedas eletrônicas mantidas em contas de pagamento, acrescidos dos saldos de moedas eletrônicas em trânsito entre contas de pagamento na mesma instituição; e valores recebidos pela instituição para crédito em conta de pagamento, enquanto não

disponibilizados para livre movimentação pelo usuário final da conta de pagamento destinatária.

Quando a BEETELLER possuir acesso ao Sistema de Transferência de Reservas (STR) do Bacen, até o encerramento do horário estabelecido para o funcionamento do STR, os recursos apurados deverão ser alocados em espécie, mediante transferência a crédito em conta específica no Bacen; ou títulos públicos federais, registrados no Sistema Especial de Liquidação e de Custódia (Selic), inclusive por meio das operações compromissadas.

Quando a BEETELLER não possuir acesso ao Sistema de Transferência de Reservas (STR) do Bacen, os recursos apurados deverão ser custodiados em conta corrente, em nome da BEETELLER, em banco de primeira linha, segregada de seus recursos próprios; ou títulos públicos federais, registrados no Sistema Especial de Liquidação e de Custódia (Selic), inclusive por meio das operações compromissadas.

A BEETELLER deverá seguir as regras do Bacen que dispõem sobre custódia e aplicação de recursos mantidos em conta de pagamento.

15. DISPOSIÇÕES FINAIS

O cumprimento desta Política é dever de todos os Colaboradores. Além disso, esta Política contém o modelo do Termo de Adesão à Política de Gerenciamento de Riscos e Termo de Adesão às Alterações da Política de Gerenciamento de Riscos, que deverão ser assinados por todos os Colaboradores que tenham, de algum modo, sua atividade vinculada às práticas e procedimentos estabelecidos nesta Política.

Esta Política será aprovada pela Diretoria e pela Alta Administração da BEETELLER, e adequadamente documentada e submetida a revisões periódicas, com a documentação mantida à disposição do Bacen.

Esta Política está disponível em local acessível a todos Colaboradores, em linguagem clara e acessível. É possível acessá-la no site https://beeteller.bitrix24.com.br/docs/path/.

ANEXO I

TERMO DE ADESÃO À POLÍTICA DE GERENCIAMENTO DE RISCOS

Eu, _____, inscrito no CPF sob o n. _____, declaro ter conhecimento desta Política de Gerenciamento de Riscos, bem como das diretrizes contidas nas demais políticas, normas e procedimentos internos da BEETELLER.

Declaro ainda ter conhecimento de que, diante de um risco mencionado nesta Política, devo comunicar imediatamente à área responsável por meio do e-mail tesouraria@beeteller.com

_____ /_____ /_____

Data

_____

Assinatura

ANEXO II

TERMO DE ADESÃO ÀS ALTERAÇÕES DA POLÍTICA DE GERENCIAMENTO DE RISCOS

Eu, _____, inscrito no CPF sob o n. _____, declaro ter conhecimento das alterações da Política de Gerenciamento de Riscos, bem como das diretrizes contidas nas demais políticas, normas e procedimentos internos da BEETELLER.

Declaro ainda ter conhecimento de que, diante de um risco mencionado nesta Política, devo comunicar imediatamente à área responsável por meio do e-mail tesouraria@beeteller.com

_____ /_____ /_____

Data

_____

Assinatura