Sempre Pronto!

POLÍTICA DE CONTINUIDADE DE NEGÓCIOS

Versão: 1.0
Aprovação: Conselho de Administração
Revisão: anual ou sempre que houver alterações relevantes

1. OBJETIVO

Esta Política tem por objetivo definir os **princípios, diretrizes e responsabilidades** da Pronto! Serviços de Pagamento Ltda. para garantir a **continuidade das operações críticas e a resiliência organizacional** em situações de interrupção, desastre ou crise, assegurando:

- A **prestação ininterrupta e segura dos serviços de pagamento**, em conformidade com as exigências do Banco Central do Brasil (BACEN);
- A **proteção dos dados, sistemas, clientes e parceiros** contra eventos disruptivos;
- A **preservação da integridade operacional, reputacional e regulatória** da instituição;
- A **aderência às normas de continuidade de negócios e segurança operacional** aplicáveis ao setor financeiro.

2. ABRANGÊNCIA

Esta Política aplica-se a **todas as áreas, processos, sistemas, serviços e colaboradores** da Pronto!, incluindo prestadores de serviço, parceiros tecnológicos, fornecedores e terceiros que desempenhem atividades essenciais ou relacionadas aos **serviços de pagamento e gestão de dados.**

Aplica-se, em especial, aos seguintes componentes:

- Infraestrutura tecnológica e de telecomunicações;
- Processos operacionais e regulatórios;
- Atividades críticas de crédito, liquidação, compensação, atendimento e gestão de riscos;
- Sistemas de informação e armazenamento de dados.

3. GLOSSÁRIO E REFERÊNCIAS

Continuidade de Negócios (Business Continuity): conjunto de medidas, políticas e processos que asseguram a manutenção ou a rápida retomada das operações críticas durante e após uma interrupção.

Plano de Continuidade de Negócios (PCN): documento que define estratégias, procedimentos, responsabilidades e recursos necessários para garantir a resposta e a recuperação das operações em caso de eventos disruptivos.

Tempo de Recuperação Objetivo (RTO): tempo máximo tolerável para a restauração de um processo, sistema ou serviço após uma interrupção.

Ponto de Recuperação Objetivo (RPO): quantidade máxima de dados que pode ser perdida em um evento de interrupção, expressa em tempo entre o último backup e o evento.

Eventos de Interrupção: situações não planejadas que podem comprometer a operação — como falhas sistêmicas, desastres naturais, ataques cibernéticos, indisponibilidade de fornecedores, pandemias, greves, incidentes de segurança da informação, ou outros eventos de força maior.

4. DIRETRIZES GERAIS

4.1 Estrutura de Governança e Responsabilidades

4.1.1 Liderança Institucional

- Aprovar o **Plano de Continuidade de Negócios (PCN)** e assegurar sua integração à estratégia corporativa;
- Deliberar sobre a **tolerância a riscos de interrupção operacional** e o apetite de risco da instituição;
- Garantir **recursos humanos, tecnológicos e financeiros** suficientes à implementação do PCN;
- Assegurar **comunicação tempestiva e transparente** com o Banco Central e demais autoridades em caso de eventos críticos;
- Supervisionar relatórios e resultados de testes e simulações

4.1.2 Gestão de Riscos e Compliance

- Coordenar a **elaboração, revisão e validação do PCN**;
- Identificar, avaliar e priorizar **ameaças e vulnerabilidades** que possam comprometer a continuidade operacional;
- Garantir **conformidade regulatória** com as normas do Banco Central (Res. BCB nº 179/2021 e 195/2022);
- Integrar o PCN com os **planos de resposta a incidentes de segurança, PLD/FT e controles internos**;
- Elaborar relatórios de conformidade e **monitoramento do risco de continuidade**.

4.1.3 Tecnologia da Informação

- Implementar e monitorar **soluções de redundância, replicação e backup** de sistemas críticos;
- Assegurar a **disponibilidade e resiliência** das plataformas de pagamento e sistemas de compensação;
- Definir e monitorar **RTO e RPO** para cada sistema essencial;
- Implementar e testar periodicamente **planos de recuperação de desastres (DRP – Disaster Recovery Plan)**;
- Manter integração com o **Plano de Segurança da Informação (PSI).**

4.2 Identificação e Classificação de Processos Críticos

- Identificar e registrar **todos os processos críticos** da instituição, com base em critérios de **impacto financeiro, operacional, legal, regulatório e reputacional**;
- Determinar **RTO e RPO específicos** para cada processo ou sistema;
- Definir **prioridades de recuperação** conforme impacto e dependências;
- Avaliar riscos de fornecedores terceirizados e parceiros estratégicos;
- Garantir que as funções críticas possuam **planos de continuidade específicos** (mínimo, principal e alternativo).

4.3 Estrutura e Conteúdo do Plano de Continuidade de Negócios (PCN)

O PCN é o documento central desta Política e deve conter, no mínimo:

i. **Cenários de ativação:** interrupções físicas, tecnológicas, humanas ou externas;

ii. **Procedimentos de resposta e recuperação:** instruções detalhadas para retomada dos serviços;

iii. **Planos de comunicação interna e externa:** incluindo canais oficiais com autoridades, clientes e mídia;

iv. **Recursos e infraestrutura alternativos:** escritórios secundários, provedores de backup, data centers redundantes;

v. **Identificação de responsáveis e substitutos:** cadeia hierárquica de acionamento;

vi. **Plano de retomada e normalização das operações** após o evento.

A elaboração e atualização do PCN devem seguir as boas práticas da **ISO 22301:2019 – Business Continuity Management Systems.**

4.4 Testes, Simulações e Treinamentos

- Realizar **testes periódicos de continuidade** (mínimo anual) abrangendo falhas de TI, indisponibilidade de infraestrutura, ausência de pessoal crítico e simulações de desastre;
- Documentar resultados e **planos de melhoria contínua**;
- Promover **treinamentos regulares** para todos os colaboradores e terceiros relevantes;
- Assegurar que os resultados dos testes sejam **reportados à alta administração** e integrados aos processos de revisão do PCN.

4.5 Comunicação e Monitoramento

4.5.1 Comunicação Interna e Externa

- Estabelecer **canais prioritários e alternativos de comunicação** com autoridades regulatórias (BACEN), clientes, parceiros e mídia;
- Garantir **transparência e tempestividade** na comunicação de incidentes que impactem os serviços;
- Coordenar mensagens públicas e respostas institucionais para **mitigar riscos reputacionais**;
- Manter registro das comunicações realizadas durante eventos críticos.

4.5.2 Monitoramento Contínuo e Revisões

- Monitorar o **ambiente operacional, regulatório e tecnológico** para identificar novos riscos;
- Revisar o PCN ao menos **uma vez ao ano** ou após incidentes relevantes;
- Validar a eficácia dos controles implementados;
- Atualizar o plano com base em **lições aprendidas e recomendações de auditoria.**

5. PROTEÇÃO DE DADOS E LGPD

Todas as ações previstas nesta Política e no PCN devem observar integralmente a **Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD)**.

Durante incidentes ou crises, devem ser assegurados:

- O tratamento adequado e seguro de dados pessoais;
- A preservação de logs e trilhas de auditoria;

- O cumprimento dos princípios de **minimização, finalidade e confidencialidade**;
- O reporte imediato de **incidentes de segurança com dados pessoais** ao Encarregado de Dados (DPO) e, quando aplicável, à ANPD.

6. CANAIS DE ATENDIMENTO E COMUNICAÇÃO

Para dúvidas, sugestões ou esclarecimentos sobre esta Política, a Pronto! disponibiliza os seguintes canais:

- **Ouvidoria:** ouvidoria@semprepronto.com.br
- **Oficial de Dados (DPO):** dpo@comolatti.com.br

7. DISPOSIÇÕES FINAIS

- Esta Política é de **caráter público** e reflete o compromisso da Pronto! com a **resiliência operacional, integridade e continuidade de seus serviços**;
- O descumprimento das disposições aqui previstas sujeitará o infrator às **medidas disciplinares e legais cabíveis**;
- A política deve ser **revisada e aprovada anualmente** pela alta administração;
- Casos omissos serão analisados pela **Área de Compliance**, com deliberação final pelo Conselho de Administração.