Sempre Pronto!

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Versão: 1.0
Aprovação: Conselho de Administração
Revisão: anual ou sempre que houver atualização normativa relevante

1. OBJETIVO

Esta Política define os **princípios, diretrizes e responsabilidades** da Pronto! Serviços de Pagamento Ltda. em relação à **segurança cibernética e proteção dos ativos de informação**, assegurando a **confidencialidade, integridade e disponibilidade dos dados e sistemas**, conforme as exigências do **Banco Central do Brasil** e as normas de **governança e gestão de riscos tecnológicos**.

A Pronto! compromete-se a:

- Proteger suas redes, sistemas e dados contra acessos não autorizados, vazamentos, fraudes, sabotagens ou ataques cibernéticos;
- Assegurar a **continuidade operacional** dos serviços de pagamento;
- Implementar controles e medidas técnicas compatíveis com os **padrões internacionais de segurança da informação**;
- Promover uma cultura organizacional de **conscientização, prevenção e resposta a incidentes cibernéticos**.

2. ABRANGÊNCIA

Esta Política aplica-se a todos os **sistemas, redes, aplicações, dispositivos, dados, processos e pessoas** que compõem o ambiente tecnológico e operacional da Pronto!, incluindo:

- Colaboradores, administradores e prestadores de serviço;
- Parceiros tecnológicos, fornecedores e terceiros com acesso a dados ou sistemas;
- Plataformas de pagamento, APIs, aplicativos e bases de dados;
- Ambientes em **nuvem, infraestrutura local e ambientes híbridos**.

3. GLOSSÁRIO

Segurança da Informação: conjunto de políticas, controles e práticas voltadas à proteção dos ativos informacionais, garantindo **confidencialidade, integridade e disponibilidade**.

Segurança Cibernética: aplicação de tecnologias e processos para proteger redes, sistemas e dados contra-ataques e ameaças digitais.

Ativo de Informação: qualquer dado, sistema, infraestrutura, hardware ou software relevante para a operação da Pronto!.

Incidente Cibernético: evento adverso confirmado ou suspeito que possa comprometer a segurança das informações.

Risco Cibernético: possibilidade de perda, vazamento ou interrupção decorrente de ameaça digital ou falha tecnológica.

Plano de Resposta a Incidentes: documento que define os procedimentos para contenção, comunicação, recuperação e análise pós-incidente.

4. DIRETRIZES GERAIS

4.1 Governança e Responsabilidade

A Pronto! mantém uma **estrutura de governança dedicada à segurança cibernética**, com **supervisão direta da Alta Administração** e **alocação de recursos adequados** à implementação e manutenção dos controles de segurança.

Responsabilidades principais:

- **Conselho de Administração:** aprova esta política e supervisiona sua efetividade;
- **Diretoria Executiva:** garante a aplicação dos controles e medidas de mitigação;
- **Área de Segurança da Informação:** implementa, monitora e aprimora continuamente as práticas de segurança;
- **Compliance e Riscos:** monitora a conformidade regulatória e o risco cibernético;
- **Colaboradores e Terceiros:** devem cumprir integralmente as normas internas e participar dos programas de conscientização.

4.2 Controles de Acesso e Autenticação

- Aplicação do princípio do **menor privilégio**, concedendo acessos apenas conforme necessidade funcional;
- Uso obrigatório de **autenticação multifator (MFA)** em sistemas críticos;
- Bloqueio automático de contas inativas e revisão periódica de perfis de acesso;
- Registro e auditoria de todos os acessos em sistemas e redes;
- Proibição de compartilhamento de credenciais ou senhas.

4.3 Proteção de Dados e Criptografia

- Utilização de **criptografia forte** (AES, TLS ou equivalentes) para proteção de dados em repouso e em trânsito;
- Armazenamento de chaves criptográficas em módulos de segurança (HSM);
- Aplicação de políticas de **mascaramento e pseudo-anonimização** de dados sensíveis;
- Proteção adicional para dados pessoais, financeiros e credenciais de acesso, em conformidade com a **LGPD** e Res. Bacen 4.658/2018.

4.4 Gestão de Vulnerabilidades e Patches

- Varreduras regulares de vulnerabilidades e **testes de penetração (pentests)** realizados por equipe independente;
- Correção tempestiva de falhas críticas e priorização de atualizações de segurança;
- Inventário atualizado de ativos tecnológicos e de software;
- Avaliação de impacto antes da aplicação de patches em sistemas críticos.

4.5 Monitoramento Contínuo e Detecção de Ameaças

- Adoção de sistemas de **Security Information and Event Management (SIEM)** para monitoramento 24x7;
- Configuração de alertas automáticos para atividades anômalas, tentativas de invasão ou incidentes de fraude;
- Integração de logs de sistemas, firewalls, endpoints e servidores;
- Revisão periódica dos indicadores de segurança (KRI/KPI cibernético).

4.6 Resposta a Incidentes

- Manutenção de um **Plano de Resposta a Incidentes Cibernéticos (PRIC)** formalmente documentado;
- Procedimentos de **contenção, erradicação, recuperação e comunicação** a autoridades e partes afetadas;
- Reporte obrigatório de incidentes significativos ao **Banco Central do Brasil**, conforme Res. CMN 4.658/2018;
- Registro e análise de **lições aprendidas** para aprimoramento contínuo.

4.7 Continuidade de Negócios e Recuperação de Desastres

- Integração do **Plano de Continuidade de Negócios (PCN)** e do **Plano de Recuperação de Desastres (DRP)** à política de segurança cibernética;
- Testes regulares de restauração de dados, redundância e failover;
- Definição de **RTO (Recovery Time Objective)** e **RPO (Recovery Point Objective)** para cada sistema crítico;
- Garantia de comunicação entre times de TI, segurança, risco e compliance durante eventos de contingência.

4.8 Segurança no Ciclo de Desenvolvimento e Fornecedores

- Implementação de práticas de **DevSecOps**, com integração de controles de segurança ao ciclo de desenvolvimento de software;
- Revisões de código, testes de vulnerabilidade e auditorias antes da publicação;
- Avaliação de segurança e **due diligence técnica e regulatória** de fornecedores com acesso a dados ou sistemas;
- Inclusão de cláusulas contratuais específicas de **sigilo, confidencialidade e proteção de dados** em contratos com terceiros.

4.9 Conscientização e Treinamento

- Programas obrigatórios de **conscientização em segurança cibernética** para todos os colaboradores;
- Treinamentos periódicos sobre **phishing, engenharia social, privacidade e uso seguro da informação**;
- Realização de campanhas internas e simulações de ataques (phishing tests) para mensurar efetividade;
- Responsabilidade da área de **RH e Segurança da Informação** pela atualização dos conteúdos.

4.10 Conformidade Regulatória e Reporte

- Garantia de aderência integral às normas do Banco Central do Brasil e à LGPD;
- Registro, rastreabilidade e guarda de evidências de todos os eventos relevantes;
- Comunicação de incidentes às autoridades competentes e aos titulares de dados afetados, conforme art. 48 da LGPD;

- Disponibilização de relatórios de segurança cibernética à Alta Administração e ao Comitê de Riscos e Compliance.

5. DIREITOS DOS TITULARES DE DADOS

Em conformidade com a **Lei nº 13.709/2018 (LGPD)**, a Pronto! assegura aos titulares o exercício dos seguintes direitos em relação aos dados pessoais tratados no contexto de segurança cibernética:

- Confirmação da existência de tratamento;
- Acesso e informação sobre dados pessoais tratados;
- Correção, anonimização, bloqueio ou eliminação de dados;
- Oposição ou limitação ao tratamento, quando aplicável;
- Comunicação sobre incidentes de segurança que possam afetar seus dados.

6. CANAIS DE COMUNICAÇÃO E ATENDIMENTO

Para comunicar incidentes de segurança ou esclarecer dúvidas sobre esta Política:

- **E-mail:** suporte@sempreprontо.com.br
- **Ouvidoria:** ouvidoria@sempreprontо.com.br
- **Encarregado (DPO):** dpo@comolatti.com.br

7. DISPOSIÇÕES FINAIS

- Esta Política é de **caráter público**, refletindo o compromisso da Pronto! com a **segurança cibernética, governança e conformidade regulatória**;
- O descumprimento das disposições desta política sujeitará o infrator a medidas disciplinares e legais;
- A Política será **revisada anualmente** ou sempre que houver mudanças significativas na estrutura tecnológica, regulatória ou organizacional;
- Casos omissos serão tratados pela **Área de Segurança da Informação e Compliance**, com aprovação final pela **Alta Administração**;
- A observância desta Política é condição essencial para a **proteção dos clientes, da instituição e do Sistema Financeiro Nacional**.