POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A **Intermed Pay Instituição de Pagamento LTDA** (doravante "Intermed Pay") estabelece esta Política de Segurança da Informação (PSI) com o objetivo de proteger seus ativos de informação, incluindo dados de clientes, colaboradores, parceiros e da própria instituição. Nosso compromisso é garantir a **confidencialidade** (acesso à informação apenas por pessoas autorizadas), a **integridade** (precisão e completude da informação, protegendo-a contra alterações não autorizadas) e a **disponibilidade** (garantir que a informação e os sistemas estejam acessíveis quando necessários) de todos os dados sob nossa responsabilidade, em conformidade com as melhores práticas de mercado e a regulamentação vigente.

1. Princípios Fundamentais

A segurança da informação na Intermed Pay é baseada nos seguintes princípios:

- Defesa em Profundidade: Implementação de múltiplas camadas de segurança (físicas, lógicas, administrativas) para proteger os ativos de informação, de modo que a falha de uma camada não comprometa a segurança total do ambiente.
- Gestão de Riscos: Identificação, avaliação, tratamento e monitoramento contínuo dos riscos de segurança da informação.
- Conformidade Legal e Regulatória: Atendimento às leis e regulamentos aplicáveis, incluindo as Resoluções do Banco Central do Brasil (BACEN) nº 496 e 497, ambas de 2025, que tratam da cibersegurança e da política de segurança cibernética para instituições financeiras.
- Responsabilidade Compartilhada: A segurança da informação é responsabilidade de todos os colaboradores, parceiros e prestadores de serviço que interagem com os sistemas e dados da Intermed Pay.

2. Controles de Segurança

A Intermed Pay implementa e mantém controles de segurança robustos, incluindo, mas não se limitando a:

- Controle de Acesso: Acesso lógico e físico aos sistemas e dados concedido com base no princípio do "mínimo privilégio" (cada usuário recebe apenas as permissões estritamente necessárias para suas funções) e "necessidade de conhecer". Utilização de senhas fortes, políticas de expiração e bloqueio automático após tentativas falhas.
- Criptografia: Aplicação de criptografia (codificação de dados sensíveis para protegê-los contra acesso não autorizado) para dados em trânsito (durante a comunicação) e em repouso (armazenados em bancos de dados e dispositivos).
- Autenticação Multifator (MFA): Exigência de múltiplos fatores de verificação (ex: senha e código enviado por SMS) para acesso a sistemas críticos e contas de usuários.
- Proteção de Rede: Implementação de firewalls (barreiras de segurança que controlam o tráfego de rede), sistemas de detecção e prevenção de intrusões (IDS/IPS) e segmentação de rede.

- Monitoramento e Auditoria: Monitoramento contínuo de eventos de segurança, registros de auditoria (logs) e análise de vulnerabilidades para identificar e responder a ameaças.

3. Plano de Continuidade de Negócios

Em conformidade com a Resolução BACEN nº 496/2025, a Intermed Pay mantém um Plano de Continuidade de Negócios (PCN) e um Plano de Recuperação de Desastres (PRD) para garantir a resiliência de suas operações. Estes planos incluem:

- Backup e Recuperação: Realização de backups regulares e testados de dados e sistemas críticos, com procedimentos claros para recuperação em caso de falhas ou desastres.
- Infraestrutura Redundante: Manutenção de infraestrutura tecnológica redundante para minimizar o tempo de inatividade em caso de falha de componentes.
- Testes Periódicos: Realização de testes periódicos dos planos de continuidade e recuperação para assegurar sua eficácia e atualização.

4. Resposta a Incidentes de Segurança

A Intermed Pay possui um processo formal de resposta a incidentes de segurança, que inclui:

- Identificação e Reporte: Qualquer suspeita ou ocorrência de incidente de segurança deve ser reportada imediatamente à equipe de Segurança da Informação através dos canais designados (e-mail: **seguranca@intermedpay.com.br** ou hotline interna).
- Análise e Contenção: A equipe especializada analisará o incidente, conterá sua propagação e mitigará seus impactos.
- Erradicação e Recuperação: Eliminação da causa raiz do incidente e restauração dos sistemas e dados afetados.
- Pós-Incidente: Análise das lições aprendidas para aprimorar os controles de segurança e prevenir futuras ocorrências.

5. Treinamentos e Responsabilidades

Todos os colaboradores da Intermed Pay, bem como terceiros que tenham acesso aos sistemas e informações da empresa, são obrigados a participar de treinamentos anuais sobre segurança da informação. A Diretoria de Tecnologia e a área de Segurança da Informação são responsáveis pela implementação, monitoramento e revisão desta política, que será atualizada anualmente ou sempre que houver mudanças significativas no ambiente de ameaças ou regulatório.