RESUMO PÚBLICO DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Simpay Instituição de Pagamento LTDA

Referência: PSC-001 | **Versão da política resumida:** 2.0 | **Última atualização deste resumo:** 22/11/2026

1. SOBRE ESTE DOCUMENTO

A **Simpay Instituição de Pagamento LTDA** mantém uma Política de Segurança Cibernética (PSC), em conformidade com a regulamentação do Banco Central do Brasil, que orienta como protegemos nossos sistemas, redes, aplicações e dados contra ataques, indisponibilidade, adulteração e vazamento de informações. Este resumo apresenta, de forma transparente, os principais compromissos dessa política. A PSC completa é um documento interno, pois detalha controles técnicos que, se divulgados, poderiam enfraquecer a própria segurança.

2. NOSSOS OBJETIVOS

Nossa política busca assegurar:

- a **confidencialidade** das informações de clientes e da empresa;
- a **integridade** das transações, dos saldos e dos registros;
- a **disponibilidade** dos serviços de pagamento;
- a **continuidade** da operação diante de falhas e incidentes;
- o **cumprimento** das leis e normas aplicáveis às instituições de pagamento.

3. A QUEM SE APLICA

A política abrange toda a infraestrutura tecnológica utilizada pela Simpay, incluindo ambientes em nuvem, aplicações, bancos de dados, redes e equipamentos de trabalho, e todas as pessoas com acesso técnico a esses ativos: colaboradores, administradores de sistemas, desenvolvedores, prestadores de serviços e terceiros. Nossa operação é predominantemente remota, e a política abrange também esse modelo de trabalho.

4. PRINCIPAIS PRÁTICAS

Infraestrutura e nuvem. Os ambientes são segregados, os sistemas são configurados apenas com o necessário, as vulnerabilidades são identificadas e corrigidas de forma periódica e os dados são protegidos por criptografia em trânsito e em repouso. Adotamos proteção contra códigos maliciosos e contra o vazamento de dados.

Identidade e acessos. Concedemos somente os acessos necessários a cada função, com autenticação multifator em sistemas relevantes e controle reforçado sobre contas privilegiadas. Operações sensíveis exigem dupla aprovação, e segredos e chaves são guardados em cofres seguros.

Redes e trabalho remoto. O acesso aos ambientes internos ocorre por conexão segura. Os equipamentos são gerenciados centralmente, com proteção, atualização e possibilidade de bloqueio remoto, e o acesso a sistemas críticos depende da identidade do usuário e da conformidade do dispositivo. Aplicações expostas à internet contam com proteção contra ataques.

Desenvolvimento seguro e mudanças. Sistemas são desenvolvidos e alterados com práticas de codificação segura, revisão por pares, testes e plano de reversão. Mantemos controles que garantem a integridade e a rastreabilidade das transações e dos saldos.

Monitoramento e prevenção a fraudes. Registramos e monitoramos os eventos de segurança de forma contínua e mantemos mecanismos de monitoramento de transações para identificar comportamentos suspeitos e bloquear operações de risco.

Resposta a incidentes. Possuímos plano de ação e de resposta a incidentes, com equipe, papéis e etapas definidos para identificar, conter, eliminar a causa e recuperar o ambiente, além de registrar e analisar cada ocorrência. Incidentes relevantes são comunicados ao Banco Central do Brasil e, quando houver risco ou dano relevante a titulares de dados pessoais, à Autoridade Nacional de Proteção de Dados (ANPD) e aos próprios titulares, nos termos da regulamentação.

Continuidade e recuperação. Mantemos cópias de segurança protegidas, testamos periodicamente sua restauração e definimos metas de recuperação para os serviços críticos, de modo a retomar a operação com rapidez.

Conectividade com o sistema financeiro e o Pix. As conexões com o Sistema Financeiro Nacional e com o Pix utilizam canais protegidos, autenticação mútua e certificados digitais gerenciados, e os componentes responsáveis por essa comunicação operam em ambiente isolado e monitorado, com chaves criptográficas protegidas.

Fornecedores, nuvem e terceiros. Avaliamos a relevância e os riscos dos prestadores de serviços de processamento, armazenamento de dados e computação em nuvem antes da contratação, exigimos requisitos de segurança, de proteção de dados e de notificação de incidentes nos contratos, acompanhamos o desempenho dos prestadores e mantemos plano de continuidade e de saída para os serviços críticos. As contratações relevantes são comunicadas ao Banco Central do Brasil, conforme a regulamentação.

Proteção dos dados. Os dados são classificados conforme sua relevância e protegidos de forma proporcional, coletados apenas na medida necessária e descartados de forma segura ao fim do prazo de guarda. Dados reais de clientes não são utilizados em ambientes de desenvolvimento e testes sem proteção equivalente.

Cultura e conscientização. Colaboradores e prestadores com acesso técnico recebem treinamento periódico, incluindo prevenção a golpes de *phishing* e engenharia social, realizamos simulações e mantemos canal para reporte imediato de eventos suspeitos, sem retaliação a quem comunica de boa-fé.

5. TESTES E MELHORIA CONTÍNUA

Realizamos testes de segurança periódicos, incluindo testes de invasão e varreduras de vulnerabilidades, e acompanhamos as correções até sua conclusão. Os resultados da implementação do plano de ação e de resposta a incidentes são consolidados em relatório anual submetido à Alta Direção.

6. GOVERNANÇA E REVISÃO

A política é aprovada pelo Comitê Gestor de Segurança da Informação e pela Alta Direção e executada pela Área de Tecnologia e Segurança Cibernética. Há um diretor responsável pela política de segurança cibernética e pelo plano de resposta a incidentes. A política é revisada, no mínimo, uma vez por ano, ou antes disso quando houver mudanças relevantes, novas ameaças, alterações regulatórias ou incidentes críticos.

Nossas práticas observam, no que for aplicável, a Resolução BCB nº 85/2021, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), o Marco Civil da Internet (Lei nº 12.965/2014), a regulamentação da ANPD sobre

incidentes de segurança, o Manual de Segurança do Pix e as demais normas do Banco Central do Brasil aplicáveis às instituições de pagamento.

7. DOCUMENTAÇÃO

A política, o plano de ação e de resposta a incidentes, os relatórios anuais e os registros de incidentes relevantes são mantidos à disposição do Banco Central do Brasil pelo prazo mínimo de cinco anos.

8. CONTATO

Dúvidas sobre privacidade e proteção de dados, ou solicitações de titulares (acesso, correção, eliminação, portabilidade, entre outras), podem ser enviadas ao nosso Encarregado de Dados (DPO):

E-mail: dpo@somossimpay.com.br