POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Resumo Público — Linhas Gerais

SIM PAUL CORRETORA DE CÂMBIO E VALORES MOBILIÁRIOS S.A. ("sim;paul")

Em atendimento ao Art. 5º da Resolução BCB nº 85/2021 e à Resolução CVM nº 35/2021, a SIM PAUL CORRETORA DE CÂMBIO E VALORES MOBILIÁRIOS S.A. ("sim;paul" ou "Instituição") divulga, a seguir, o resumo com as linhas gerais de sua Política de Segurança da Informação e Segurança Cibernética. Este documento tem caráter informativo e não substitui nem detalha a totalidade dos controles técnicos e operacionais internos, que permanecem descritos em documento interno de uso restrito (POL-SEG-001).

1. Objetivo e Princípios

A Política estabelece os princípios, diretrizes e responsabilidades adotados pela sim;paul e pelas demais sociedades do grupo econômico sim;paul no Brasil para assegurar a confidencialidade, a integridade e a disponibilidade dos dados, sistemas e ativos de informação sob sua responsabilidade, incluindo os ativos virtuais de clientes.

- Confidencialidade: a informação é acessível apenas a pessoas autorizadas;
- Integridade: a informação é exata, completa e somente modificável por pessoas autorizadas;
- Disponibilidade: a informação está acessível a quem dela necessite, no momento adequado.

A Política é compatível com o porte, o perfil de risco, o modelo de negócio, a natureza das atividades e a sensibilidade dos dados sob responsabilidade da Instituição, e busca prevenir incidentes, detectar tempestivamente ameaças, reduzir a exposição a riscos cibernéticos e assegurar a conformidade regulatória, no Brasil e nas demais jurisdições aplicáveis ao grupo econômico.

2. Abrangência

A Política aplica-se à sim;paul e a qualquer outra sociedade do grupo econômico sim;paul com atuação no país, a todos os Colaboradores, administradores e parceiros/prestadores de serviço que tenham acesso aos sistemas de informação da Instituição, independentemente do ambiente de execução das atividades.

3. Governança de Segurança da Informação e Segurança Cibernética

A gestão de segurança da informação e segurança cibernética integra a estrutura de governança corporativa da Instituição, com segregação formal entre a liderança estratégica e a supervisão independente da segurança da informação e a liderança operacional de tecnologia, em linha com as boas práticas de mercado (ISO/IEC 27001 e NIST CSF).

- Diretoria Executiva: aprova a Política e assegura recursos adequados ao Programa de Segurança;
- Diretor de Tecnologia da Informação: membro estatutário responsável perante o Banco Central do Brasil pela política de segurança cibernética;
- CISO (Chief Information Security Officer): responsável pela estratégia, pelos requisitos de segurança e pela supervisão independente de sua efetividade;
- Comitê de Tecnologia e Segurança da Informação e Comitê de Riscos e Compliance: fóruns colegiados de acompanhamento e deliberação sobre riscos cibernéticos e de segurança da informação;
- Auditoria Interna: avalia de forma independente a efetividade dos controles implementados.

4. Diretrizes Gerais de Segurança

A Instituição adota controles de segurança da informação e segurança cibernética compatíveis com as boas práticas de mercado e com a regulamentação aplicável, incluindo, entre outros:

- Autenticação multifator e controle de acessos baseado em necessidade de uso;

- Criptografia de dados em repouso e em trânsito, incluindo controles específicos de guarda e proteção de chaves privadas de ativos virtuais de clientes;
- Prevenção, detecção e resposta a códigos maliciosos e intrusões, com monitoramento contínuo por Centro de Operações de Segurança (SOC);
- Gestão de vulnerabilidades e testes de intrusão (penetration testing) periódicos, conduzidos por terceiros independentes;
- Diligência de segurança na contratação de parceiros e de prestadores de serviços de processamento, armazenamento de dados e computação em nuvem;
- Controles específicos de proteção dos ambientes críticos do Sistema Financeiro Nacional, incluindo Pix, SPI e STR;
- Desenvolvimento seguro de sistemas e aplicações, com testes de segurança antes da entrada em produção;
- Segregação patrimonial e mecanismos de prova de reservas para os ativos virtuais de clientes.

5. Gestão de Incidentes

A Instituição mantém Plano de Ação e de Resposta a Incidentes, com o objetivo de preparar, detectar e responder a incidentes de segurança da informação e segurança cibernética, determinando escopo e risco, adotando as medidas de contenção e remediação cabíveis e comunicando os resultados às partes interessadas, inclusive aos órgãos reguladores competentes, quando aplicável.

6. Continuidade de Negócios e Resiliência Operacional

O Programa de Segurança da Informação e Segurança Cibernética atua de forma integrada com o Plano de Continuidade de Negócios da Instituição, contemplando planos de recuperação de desastres, de gestão de crises e de retorno à normalidade, com o objetivo de assegurar a continuidade dos serviços prestados a clientes.

7. Cultura de Segurança e Conscientização

A Instituição promove a disseminação contínua da cultura de segurança da informação e segurança cibernética entre seus Colaboradores e parceiros, por meio de treinamentos obrigatórios, programas de conscientização, simulações periódicas e orientações a clientes sobre boas práticas de segurança e prevenção a fraudes.

8. Conformidade Regulatória

A Política é revisada e atualizada de forma contínua para observar a regulamentação aplicável às atividades da Instituição, bem como padrões e boas práticas internacionais de segurança da informação e segurança cibernética reconhecidos pelo mercado.

9. Revisão e Atualização

Esta Política, e consequentemente este resumo, é revisada, no mínimo, anualmente, ou sempre que houver alteração regulatória relevante, sendo formalizada e arquivada pelo prazo exigido pela regulamentação aplicável.

10. Contato

Dúvidas ou esclarecimentos sobre esta Política podem ser encaminhados à área de Compliance / Segurança da Informação da sim;paul, pelos canais oficiais de atendimento disponíveis em nosso site.