POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

A27 Instituição de Pagamentos SA

1 OBJETIVO

Esta política tem como objetivo estabelecer de acordo com as leis, regulamentações e boas práticas que nortearão as normas e padrões que tratam das informações que transitam na A27 Bank Instituição de Pagamento S/A, em forma física, digital ou verbal, bem como prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, de acordo com as diretrizes da Resolução nº 85, de 08 de abril 2021 do Banco Central do Brasil.

2 PÚBLICO-ALVO

Esta Política tem o caráter público.

3 PRINCÍPIOS

Os processos e atividades desenvolvidas para cumprimento das determinações estabelecidas ao ambiente cibernético e ao gerenciamento das informações devem observar os princípios da:

a) Integridade: consiste na preservação da exatidão da informação e dos métodos de processamento;
b) Confidencialidade: garantindo que a informação é acessível somente por pessoas autorizadas a terem acesso;
c) Disponibilidade: diz respeito à garantia de que as pessoas físicas e jurídicas autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

4 CONTROLES E MONITORAMENTOS

A A27 adota controles e monitoramentos com o objetivo de garantir uma adequada estrutura de segurança aos ambientes cibernéticos e das informações tratadas, tais como:

- Gestão de acessos e autenticação segura;
- Criptografia e anonimização de dados pessoais e sensíveis;

- Testes de intrusão e varredura periódica de vulnerabilidades;
- Proteção contra vírus, malwares e outras ameaças digitais;
- Políticas de backup e preservação de dados;
- Medidas de prevenção para arquivos físicos e digitais.

5 CLASSIFICAÇÃO DOS DADOS E INFORMAÇÕES

Os dados e as informações da A27 são classificados de acordo com o nível de relevância e recebem o tratamento e as proteções adequados a esta classificação, sendo classificados em Restrito, Confidencial, Interno e Público.

6 DILIGÊNCIAS QUANTO A CONTRATAÇÃO DE TERCEIROS

Previamente à efetivação da contratação do terceiro são realizadas verificações de conformidade e de segurança da estrutura utilizada pelo potencial prestador de serviços, visando identificar restrições e eventuais riscos aos quais a Instituição poderá ser submetida com a celebração do vínculo e fundamentar a tomada de decisões.

No que se refere ao gerenciamento e à segurança das informações compartilhadas entre a A27 e o terceiro, os contratos devem estabelecer, no mínimo, as responsabilidades das partes no tratamento de dados pessoais, os limites para sua utilização, as medidas de conformidade a serem observadas pelo terceiro, a garantia de atendimento aos direitos dos titulares, a obrigação de comunicar eventuais incidentes envolvendo dados tratados no âmbito da relação contratual e a responsabilização do contratado em caso de descumprimento contratual ou da legislação aplicável, especialmente a LGPD.

7 RESPOSTA A INCIDENTES

A A27 possui plano estruturado para identificação, tratamento e comunicação de incidentes relevantes, incluindo medidas de contenção, recuperação e aprimoramento contínuo.

8 CULTURA DE SEGURANÇA

A instituição estabelece programas de conscientização, divulgação e reciclagem sobre o tema segurança cibernética.

9 MEDIDAS DISCIPLINARES

O uso de qualquer recurso ou informação para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a A27 cooperará ativamente com as autoridades competentes.