POLÍTICA DE SEGURANÇA CIBERNÉTICA

A Cappta Instituição de Pagamento S.A. adota um conjunto abrangente de diretrizes e práticas voltadas à proteção dos seus ambientes digitais, garantindo a prevenção, detecção e mitigação de riscos cibernéticos. A Política está alinhada aos requisitos legais e regulatórios, incluindo a Resolução BCB nº 85/2021, e reflete o compromisso da Cappta com a segurança da informação, a continuidade dos negócios e a conformidade regulatória.

Objetivo

Assegurar a proteção dos dados e sistemas da Cappta, prevenindo acessos não autorizados, falhas, ataques cibernéticos e incidentes que possam comprometer suas operações, reputação e os direitos dos titulares de dados.

Princípios Fundamentais

1. Confidencialidade: Garantir que as informações sejam acessadas apenas por pessoas autorizadas.
2. Integridade: Preservar a precisão e consistência dos dados desde sua criação até seu uso.
3. Disponibilidade: Manter os sistemas e informações acessíveis quando necessário.

Diretrizes e Controles Adotados

1. Gestão de Acesso e Informações: Controle rigoroso sobre acessos, com rastreabilidade e revisões periódicas, além de classificação e rotulagem das informações conforme sensibilidade.

2. Proteção de Dados Pessoais: Conformidade com a LGPD e demais legislações aplicáveis, com medidas específicas para coleta, processamento e compartilhamento de dados pessoais.

3. Desenvolvimento Seguro de Sistemas: Aplicação de boas práticas de mercado, como segregação de funções, testes, homologações e gestão de mudanças.

4. Segurança Tecnológica: Implementação de tecnologias avançadas como:

    - WAF (Web Application Firewall): Proteção contra ataques a aplicações web.
    - Firewall e VPN Segmentada: Monitoramento de tráfego e segmentação segura de redes.
    - Pentests e Scans de Vulnerabilidades: Identificação e correção proativa de falhas.
    - Soluções Antivírus e Proxy: Proteção contra malwares, ransomware e navegação insegura.

5. Gestão de Riscos e Incidentes: Monitoramento contínuo, respostas estruturadas e comunicação obrigatória de incidentes ao Banco Central do Brasil (BCB) e à Autoridade Nacional de Proteção de Dados (ANPD).

6. Continuidade de Negócios: Planos específicos para recuperação de desastres e administração de crises, incluindo simulações periódicas com cenários reais de incidentes.

7. Conscientização e Cultura: Treinamentos regulares para colaboradores e parceiros, atualizados com base em mudanças regulatórias, além de campanhas educativas para disseminar boas práticas de segurança.

Governança e Responsabilidades

A alta administração, liderada pelo Diretor Responsável, garante a aplicação, supervisão e conformidade das diretrizes. A área de TI implementa controles tecnológicos e monitora acessos e atividades suspeitas.

Comunicação e Denúncias

Qualquer irregularidade pode ser comunicada de forma anônima por meio do e-mail ouvidoria@cappta.com.br, assegurando o tratamento adequado.

Revisão e Atualização

A Política é revisada anualmente ou em caso de alterações regulatórias, garantindo sua efetividade e alinhamento com as melhores práticas do mercado.

OUTUBRO DE 2024