Política de Segurança da Informação e Cibernética – Versão pública

CONTROLE DE DOCUMENTO

INFORMAÇÕES DO DOCUMENTO

DOCUMENTO	
Título	Política de Segurança da Informação e Cibernética – Versão Pública
Código	PSIC-VP
Número da Versão	01
Data	12/12/2023
Departamento	Tecnologia da Informação
Responsável	Leandro Andreo Rodrigues

REVISÃO

HISTÓRICO DA REVISÃO			
Data	Assunto	Responsável	Nº Rev.
12/12/2023	Elaboração da Política de Segurança da informação e Cibernética	Leandro Andreo Rodrigues	01

APROVAÇÃO

Nº Revisão.	Diretoria Executiva	
	Data	Responsável
01	12/12/2023	Diretoria de Compliance

1. OBJETIVO

O programa de Segurança da Informação e Cibernética da OneKey visa proteger todos os ativos, incluindo dados, observando os princípios de:

a) Confidencialidade: garantir que as informações e dados sejam acessíveis somente ao pessoal especificamente autorizado;

b) Integridade: manter a exatidão das informações e dados, sem modificações indevidas (sejam intencional ou não);

c) Disponibilidade: permitir que somente pessoas autorizadas a tratar as informações e dados tenham acesso ao seu conteúdo e possam consultá-las a qualquer momento;

2. RESPONSABILIDADE

A OneKey possui departamento dedicado de segurança da informação, que visa planejar, propor, implementar, controlar e melhorar continuamente as políticas, procedimentos, tecnologias e treinamentos de segurança da informação.

3. COLABORADORES

Todos os colaboradores da OneKey:

a) Executam as suas atividades cumprindo expressamente as diretrizes da Política de Segurança da Informação da OneKey, publicada em seu portal de compliance.
b) São treinados no mínimo anualmente sobre as boas práticas de segurança da informação
c) Possuem canal dedicado para abrir e reportar incidentes de segurança
d) Participam de testes de intrusão, testes de phishing, auditorias internas e externas, visando a contínua confirmação da eficácia do programa de segurança da informação.

4. DIRETRIZES

Toda informação de propriedade da Onekey Payments deve ser protegida de forma a não comprometer a sua confidencialidade, integridade e disponibilidade.

Para isto, o departamento de tecnologia da OneKey disponibiliza:

- Computadores corporativos, protegidos com ferramentas de segurança adequadas, como antivírus, firewall, MDM e criptografia.

- Locais seguros, em rede, para armazenamento e produtividade dos arquivos, providos de backup e retenção de dados.
- Serviços seguros para troca de e-mails, mensagens e videoconferências.
- Canais de suporte preparados para auxiliar os colaboradores no caso de incidentes de segurança da informação.

O programa de segurança da informação, em conjunto com os programas de compliance, controles internos, prevenção a fraudes e prevenção à lavagem de dinheiro, visam atender às leis e normas que regulamentam as atividades da Onekey Payments.

O programa de segurança da informação adota procedimentos e controles para reduzir a vulnerabilidade da Instituição a incidentes e atender aos objetivos de segurança cibernética, dentre eles: a autenticação, e criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, entre outras atividades.

A OneKey realiza ações para prevenir, identificar, registrar e responder incidentes e crises de segurança que envolvam o seu ambiente tecnológico da e que possam ocasionar o comprometimento dos pilares de segurança da informação ou gerar impacto de imagem, financeiros ou operacionais.

A OneKey também adota mecanismos para disseminação da cultura de segurança da informação e cibernética na Companhia, incluindo:

a) A implementação de programa de avaliação periódica de colaboradores quanto ao nível de conhecimento do tema segurança da informação e cibernética;
b) A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos
c) O comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética

A Onekey Payments possui diversos controles de acesso físico, que impedem o acesso não autorizado em suas instalações, protegendo seus ativos e a integridade física de seus colaboradores

Nos ativos físicos da OneKey deve-se utilizar apenas softwares licenciados ou autorizados pela unidade responsável, bem como endpoint para fins de controle de ameaças eletrônicas, vírus, zero-day, ransomware.

5. AUTENTICACÃO

Todos os sistemas da OneKey Payments possuem controle de identidades e de acessos, com as

melhores práticas de mercado:

- Senha forte, com troca recorrente
- Duplo fator de autenticação
- VPN
- Revisão periódica de acessos.

6. PREVENÇÃO CONTRA VAZAMENTO DE INFORMAÇÕES

Em observância à LGPD, a OneKey possui treinamento para os colaboradores sobre o tema, além de políticas, procedimentos e controles para garantir boas práticas na utilização de dados pessoais, mitigando riscos de vazamentos.

7. TESTES DE INTRUSÃO

A OneKey realiza periodicamente testes de intrusão interno e externo, garantindo a proteção de sua infraestrutura e sistemas, para garantia da Confidendialidade, Integridade e Disponibilidade.

8. GERENCIAMENTO DE RISCOS

Em conjunto com o departamento de compliance, a Onekey Payments possui programa de gerenciamento e prevenção de riscos, que se estendem para riscos de segurança da informação.

9. CONTINUIDADE DE NEGÓCIOS

A Onekey Payments possui plano de continuidade de negócios e testa regularmente os cenários de crise, visando garantir a seus colabores e clientes o máximo funcionamento de seus serviços e a prevenção contra ações de larga escala que possam causar indisponibilidades.

10 REVISÃO E APROVAÇÃO

Data	Revisão	Responsável	Descrição
12/12/2023	0	Leandro Andreo Rodrigues	Criação da Política