CONTROLE DE DOCUMENTO

INFORMAÇÕES DO DOCUMENTO

DOCUMENTO	
Título	Política de Segurança da Informação e Cibernética – Versão Pública
Data	07/01/2025
Departamento	Segurança da Informação

APROVAÇÃO

HISTÓRICO DA REVISÃO		
Data	**Assunto**	**Nº Rev.**
12/12/2023	Elaboração da Política de Segurança Cibernética e da Informação – Versão Pública	001
07/01/2025	Revisão da Política de Segurança Cibernética e da Informação – Versão Pública	002

1. OBJETIVO

O programa de Segurança da Informação e Cibernética da OneKey visa proteger todos os ativos de informação, incluindo tecnologia, sistemas, dados e pessoas, 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;

d) ***Autenticidade***: assegurar que a informação seja proveniente da fonte original e que não foi alvo de alterações.

e) ***Irretratabilidade ou não repúdio***: garantir que o legítimo autor da informação não possa repudiar sua autoria, como, por exemplo, ao dar aceite em um contrato digital utilizando credenciais de acesso, entende-se que o aceitante não pode negar a sua assinatura posteriormente.

f) ***Conformidade:*** assegurar que os processos da Instituição estejam de acordo com os regulamentos, normativos e leis vigentes, de forma a seguir rigorosamente todos os protocolos exigidos no setor de atuação da Instituição em decorrência das suas atividades realizadas.

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, além de disseminar uma cultura que proporcione que cada um dos seus colaboradores, juntamente com políticas, processos e tecnologia, sejam parte valiosa da estratégia de defesa cibernética da Companhia.

3. COLABORADORES

Todos os colaboradores da OneKey:

- Executam as suas atividades cumprindo expressamente as diretrizes da Política de Segurança da Informação, publicada em sua intranet.
- Utilizam os equipamentos corporativos cumprindo as diretrizes da Política de Segurança da Informação, publicada em sua intranet.
- Utilizam os acessos e sistemas corporativos cumprindo as diretrizes da Política de Segurança da informação, publicada em sua intranet.
- São treinados, no máximo anualmente, sobre as boas práticas de segurança da informação
- Possuem canal dedicado para abrir e reportar incidentes de segurança
- Possuem canal dedicado para abrir solicitações relacionadas a liberação de acessos.
- 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, os departamentos de Tecnologia da Informação e Segurança da Informação da OneKey disponibilizam:

- 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.
- Escritório corporativo com ambiente protegido para o desempenho seguro das atividades.
- Conexão Privada Virtual (VPN) segura para o exercício das atividades fora do ambiente do escritório.
- Serviços seguros e criptografados para troca de e-mails, mensagens e videoconferências.
- Canais de suporte preparados para auxiliar os colaboradores no caso de incidentes de tecnologia ou segurança da informação.

- Canal de Denúncias para receber e tratar indícios de violações e fraudes.

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,
- a 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
- treinamento e testes para detecção de Phishing
- Revisão periódica de Acessos
- Entre outras atividades regulares

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 implementação de programa de avaliação periódica de colaboradores quanto ao nível de conhecimento do tema segurança da informação e cibernética;
- A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos
- 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 e lógico, que impedem o acesso não autorizado em suas instalações, sistemas e dados, protegendo seus ativos e a integridade física

de seus colaboradores

Nos ativos físicos da OneKey utiliza-se apenas softwares licenciados ou autorizados pela unidade responsável, bem como sistemas de segurança para proteção contra ameaças eletrônicas, malwares, zero-day exploits, ransomware etc.

5. AUTENTICAÇÃO

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
- Single Sign-On
- VPN
- Revisão periódica de acessos.

6. PREVENÇÃO A 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 confidencialidade, integridade e disponibilidade.

8. GERENCIAMENTO DE RISCOS

Em conjunto com o departamento de compliance, a Onekey Payments possui programas 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 colaboradores e clientes o máximo funcionamento de seus serviços e a prevenção contra ações de larga escala que possam causar indisponibilidades.

10. TREINAMENTO

A cultura de Segurança Cibernética é disseminada internamente por meio de programas de capacitação ministrados periodicamente para todos os colaboradores, garantindo assim que todos estejam cientes das possíveis ameaças e vulnerabilidades que ocorrerem no âmbito da Segurança Cibernética, bem como quais são os procedimentos que devem ser adotados em casos de incidentes.