

CONTROLE DE DOCUMENTO**INFORMAÇÕES DO DOCUMENTO**

DOCUMENTO	
Título	Política de Segurança Cibernética e da Informação
Código	PSC-004
Número da Versão	004
Data	26/05/2026
Departamento	Segurança da Informação
Responsável	Renato Yamada

Interno

Sumário

CONTROLE DE DOCUMENTO	1
REVISÃO	Erro! Indicador não definido.
1. OBJETIVO	4
2. GLOSSÁRIO	5
3. REGULAMENTAÇÃO APLICÁVEL	8
4. DEFINIÇÃO DE RESPONSABILIDADES	10
4.1 DIRETORIA EXECUTIVA	10
4.2 GERENTE DE SEGURANÇA DA INFORMAÇÃO	10
4.3 GESTÃO DE RISCOS	10
4.4 AUDITORIA INTERNA	10
4.5 TECNOLOGIA DA INFORMAÇÃO	11
4.6 COLABORADORES	11
5. DIRETRIZES	12
5.1 SEGURANÇA DA INFORMAÇÃO	12
5.2 SEGURANÇA CIBERNÉTICA	12
6. PROCEDIMENTOS DE SEGURANÇA	14
6.1 PROTEÇÃO E GERENCIAMENTO DO AMBIENTE FÍSICO	14
GERENCIAMENTO DAS INSTALAÇÕES	14
GERENCIAMENTO DE SERVIDORES	15
GERENCIAMENTO DE DISPOSITIVOS	15
INVENTÁRIO FÍSICO	16
6.2 PROTEÇÃO E GERENCIAMENTO DE AMBIENTE LÓGICO	16
GESTÃO DE ACESSOS ÀS INFORMAÇÕES	16
AUTENTICAÇÃO	17
CLASSIFICAÇÃO DA INFORMAÇÃO	17
CONCESSÃO, REVISÃO E REVOGAÇÃO DE ACESSOS	18
SENHAS	18
REDE	19
AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS	19
PROCESSAMENTO E ARMAZENAMENTO DE INFORMAÇÕES	20
BACKUP	21

COMPARTILHAMENTO DE INFORMAÇÕES	21
PREVENÇÃO A VAZAMENTO DE INFORMAÇÕES	21
GERENCIAMENTO DE AMEAÇAS E VULNERABILIDADES DE TI	22
CRIOGRAFIA.....	22
RASTREABILIDADE	22
6.3 GERENCIAMENTO DE INCIDENTES.....	23
CLASSIFICAÇÃO DA CRITICIDADE DOS INCIDENTES.....	23
PLANO DE AÇÃO AOS INCIDENTES.....	23
TESTES DE INTRUSÃO	24
TESTE DE CONTINUIDADE DE NEGÓCIOS	24
7 PRESTADORES DE SERVIÇOS DE TI.....	25
8 RECOMENDAÇÕES DE SEGURANÇA A CLIENTES E USUÁRIOS.....	25
PHISHING.....	25
SPAM	26
VPN	26
9 TREINAMENTO	27
10 SANÇÕES	27
11 COMUNICAÇÃO	27
12 REVISÃO E APROVAÇÃO.....	Erro! Indicador não definido.

1. OBJETIVO

O objetivo desta política é definir as regras e diretrizes relacionadas à segurança cibernética e à proteção de todo o ativo de tecnologia e informação de propriedade da OneKey Payments, bem como, o cumprimento dos requisitos que garantam a confidencialidade, integridade, disponibilidade, autorização e não-repúdio dos acessos, dados e sistemas.

Ainda, disciplina a estrita observância aos requisitos que assegurem a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, em aderência a legislação e regulamentação vigentes, mais precisamente a Resolução BCB nº 85 de 08 de abril de 2021.

Todos os usuários e departamentos da OneKey Payments devem cumprir esta política, que exige leitura integral imediata e atualização anual obrigatória.

Para assegurar que as informações e dados sob propriedade da OneKey Payments estejam gerenciados e protegidos contra roubo, fraude, espionagem, perda e quaisquer outras ameaças, todas as ações inerentes a este assunto inspiram-se nos pilares da Segurança da Informação e cibersegurança:

- 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 para as pessoas autorizadas, as informações e dados estejam sempre disponíveis e possam ser consultadas a qualquer momento;
- d) **Autenticidade:** assegura a veracidade da origem dos dados e a ausência de modificações não autorizadas;
- e) **Não repúdio:** garantir que o legítimo autor de ações em sistemas de informação não possa repudiar os atos realizados em 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.

Interno

2. GLOSSÁRIO

Segurança da Informação	Conjunto de conceitos, técnicas e estratégias, as quais visam proteger os ativos de informação
Segurança Cibernética	Conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado. Esse conjunto de práticas protege a informação armazenada nos computadores, nos aparelhos de computação e nas transmissões efetuadas por meio das redes de comunicação, incluindo internet e telefones celulares.

Ativos de informação	São todas as informações geradas ou desenvolvidas para o negócio e podem estar presentes em diversas formas, tais como: arquivos digitais, consentimentos de clientes e pessoas ligadas à OneKey Payments, documentos impressos, documentos digitalmente assinados, bancos de dados, conversas e gravações
Ativo de Software	São aplicativos, sistemas, ferramentas de desenvolvimento e utilitários utilizados para o negócio.
Ativos Físicos	São equipamentos computacionais, equipamentos de comunicação, mídias externas removíveis, dispositivos móveis e outros equipamentos;
Informação	São todos os dados referentes às atividades desenvolvidas pela OneKey Payments na execução de seu objeto social, incluindo dados de clientes, pessoais ou não, e classificados de acordo com a norma interna específica sobre o tema.

Interno

Incidente	Qualquer ocorrência que realmente ou potencialmente comprometa a confidencialidade, integridade ou disponibilidade de um sistema de informação ou a informação que o sistema processa, armazena e transmita ou que constitua uma violação ou ameaça iminente de violação de políticas de segurança, procedimentos de segurança ou políticas de uso aceitáveis.
Prestador de Serviço	Pessoa física ou jurídica, devidamente contratada pela OneKey Payments, prestadora de serviços: (i) de tecnologia; (ii) de armazenamento ou qualquer forma de tratamento de Dados e Informações; ou (iii) que venha a ter acesso, por conta do escopo de sua contratação, a Dados confidenciais, como classificados nesta Política.
TI	Tecnologia da informação;
PGCN	Programa de Gestão de Continuidade de Negócios

NDA	Sigla em inglês para Non-Disclosure-Agreements, ou simplesmente Acordo de Sigilo de Informações.
KRI	Do inglês Key Risk Indicators, os Indicadores Chave de Risco são, como o nome sugere, indicadores sobre os principais riscos aos quais a organização está exposta.
Softwares	É a parte lógica, o conjunto de instruções e dados processados nos servidores e computadores. Toda interação dos usuários de computadores é realizada por meio de softwares.
Backup	É a cópia de dados de um dispositivo de armazenamento a outro para que possa ser restaurado em caso da perda dos dados originais, o que pode envolver apagamentos acidentais ou corrupção de dados.
Mídias Removíveis	Dispositivos que permitem a leitura e gravação de dados tais como: CD, DVD, Disquete, Pen Drive, cartão de memória entre outros.

Interno

Virtual Private Network	Modalidade de acesso à rede corporativa, que possibilita a conectividade, via internet, de um equipamento externo à rede interna da corporação, provendo funcionalidades e privilégios como se o mesmo estivesse conectado física e diretamente à rede interna. Comumente é utilizado por funcionários em trânsito.
Firewall	É um dispositivo de uma rede de computadores que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede
Controle de Acesso	Assegurar que os acessos aos ativos sejam sempre autorizados e restringidos baseados nos negócios e nos requerimentos de segurança da Companhia.
Ataque	Acesso Não Autorizado, tentativa de acesso para destruir

Governança de Segurança das Informações	Sistema pelo qual as atividades de segurança das informações são direcionadas e controladas.
Software EndPoint	Atua na interrupção de ameaças, no monitoramento da integridade geral do sistema e na geração de relatórios com informações sobre detecção e status. O software cliente é instalado em cada sistema, porém possui um orquestrador centralizado. O sistema de proteção engloba gerenciamento de permissões de instalação e de acessos a aplicativos, controle de acesso à rede e à Internet, controle de dispositivos, gerenciamento contra perda de dados (DLP), detecção e resposta de ameaças e principalmente, proteção anti-malware.
	Em outras palavras, o sistema protege servidores, sistemas de computadores, laptops e tablets contra ameaças conhecidas e desconhecidas. Essas ameaças incluem malware, comunicações suspeitas, sites não confiáveis e arquivos baixados.
Riscos Cibernéticos	São os riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, entre outros, que possam expor dados, redes e sistemas da OneKey Payments, causando danos financeiros e/ou de reputação consideráveis, podendo, em algumas circunstâncias, prejudicar a continuidade das atividades.

3. REGULAMENTAÇÃO APLICÁVEL

- Lei nº 12.965/2014 – Marco Civil da Internet;
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados;
- Lei nº 9.609/1998 – Lei de Software;
- Resolução BCB nº 85 de 08 de abril de 2021;
- ISO 27.001;
- Código de Ética e Conduta da OneKey Payments.

Interno

4. DEFINIÇÃO DE RESPONSABILIDADES

4.1 DIRETORIA EXECUTIVA

Cabe à Diretoria Executiva:

- a) Revisar e aprovar as disposições e diretrizes contidas na política de Segurança da Informação, bem como apoiar em todos os recursos necessários para o cumprimento das práticas relacionadas a esta política.
- b) Aprovar toda a criação e a revisão de documentação complementar inerente ao assunto, como, por exemplo, o Plano Diretor de SI (PDSI), o Plano de Continuidade de Negócios (PCN) e o Plano de Resposta a Incidentes (PRI).

4.2 GERENTE DE SEGURANÇA DA INFORMAÇÃO

- a) O Gerente de Segurança da Informação é o responsável pela Política de Segurança da Informação, bem como por todas as ações referentes ao controle e defesa cibernética;
- b) Definir e manter a governança de Segurança da Informação, com responsabilidades claras, processos de reporte à Diretoria, e supervisão contínua de conformidade regulatória e privacidade (LGPD); e
- c) Encontra-se devidamente cadastrado no Banco Central do Brasil.

4.3 GESTÃO DE RISCOS

Cabe a área de Gestão de Riscos estabelecer as principais diretrizes e processos relacionados ao gerenciamento dos riscos corporativos, sendo responsável pela identificação, avaliação e monitoramento de riscos relacionados à Segurança da Informação da Instituição e a seu setor, em atendimento às regulamentações, normativos aplicáveis e boas práticas de mercado.

4.4 AUDITORIA INTERNA

Cabe à Auditoria Interna fornecer opiniões independentes, autônomas e imparciais acerca da qualidade e da efetividade dos sistemas e dos processos de gerenciamento de Segurança da Informação, Gestão de Riscos, Controles Internos e Governança Corporativa, identificando desvios e providências cabíveis, recomendando melhorias que visam resguardar os interesses da

Instituição.

4.5 TECNOLOGIA DA INFORMAÇÃO

Cabe ao departamento de Tecnologia da Informação:

- a) Coordenar os esforços requeridos para atingir os objetivos de Segurança da Informação, bem como a proteção de dados e as atividades constantes nesta Política;
- b) Investigar eventos, com o objetivo de detectar se houve a quebra da estrutura de Segurança e Privacidade da Informação, e a subsequente implementação de medidas apropriadas, quando aplicável.

4.6 COLABORADORES

Cabe aos colaboradores:

- a) Conhecer e cumprir as diretrizes desta Política;
- b) Aderir formalmente e cumprir o Termo de Responsabilidade e Confidencialidade, entregue junto com os equipamentos de tecnologia.
- c) Rer a política de Segurança da Informação, no mínimo, uma vez ao ano, ou quando houver comunicação formal de alterações relevantes.
- d) Utilizar os recursos disponibilizados pela OneKey de acordo com o previsto nesta e em outras Políticas pertinentes, sujeito a medidas disciplinares em caso de descumprimento.
- e) Obrigatoriamente, abrir chamado para solicitar acessos, requisições de serviço, suporte e dúvidas.

5. DIRETRIZES

5.1. SEGURANÇA DA INFORMAÇÃO

- a) Toda informação de propriedade da OneKey Payments deve ser protegida de forma a não comprometer a sua confidencialidade, integridade, disponibilidade, autenticidade, irretratabilidade ou conformidade, independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada.
- b) Os ativos de informação e equipamentos devem ser utilizados apenas para a sua finalidade profissional devidamente autorizada, sendo sujeitos a monitoramento compulsório e auditoria, independentemente do local onde sejam utilizados.
- c) A OneKey Payments estabelece que todo o ativo de informação de sua propriedade possui um responsável e deve ser classificado de acordo com os critérios de confidencialidade estabelecidos nesta política.

5.2. SEGURANÇA CIBERNÉTICA

Interno

O departamento de Segurança da Informação deve:

- a) Criar mecanismos de proteção dos dados e ativos contra acessos indevidos, modificações indevidas, destruições ou divulgações não autorizadas
- b) Dispende esforços para que os sistemas e dados sob sua responsabilidade estejam devidamente protegidos e sejam utilizados apenas para o cumprimento de suas atribuições;
- c) Adotar as medidas necessárias para prevenir ameaças, como vírus, programas nocivos ou outras falhas que possam ocasionar acessos, manipulações ou usos não autorizados de dados internos e confidenciais, por meio, dentre outros aspectos: (i) da manutenção de softwares antivírus e firewall instalados e atualizados; (ii) da manutenção dos programas de computador instalados no ambiente; (iii) da concessão e revogação de acessos mediante severa avaliação e devidamente justificada; (iv) das revisões de acessos periódicas adequadas.
- d) Atender às leis e normas que regulamentam as atividades da OneKey Payments.

- e) Adotar procedimentos e controles para reduzir as vulnerabilidades da Instituição e atender aos objetivos de segurança cibernética, dentre eles: a autenticação, e criptografia, a prevenção e 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, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações, conforme normativos internos vigentes.
- f) Controlar, monitorar, restringir o acesso aos ativos de informação e sistemas, seguindo sempre o princípio da mínima permissão e privilégios possíveis, podendo, inclusive, revogar qualquer acesso que se mostre nocivo sem prévio conhecimento ou concordância do colaborador.
- g) Aplicar os procedimentos e controles para o desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da Instituição.
- h) Realizar o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da Instituição, que abrange inclusive informações recebidas de empresas prestadoras de serviços e terceiros.
- i) Elaborar inventário dos cenários de crises cibernéticas relacionados aos incidentes de segurança considerados nos testes de continuidade de serviços de pagamento prestados e realizar testes para garantir a eficácia dos processos no ambiente tecnológico OneKey Payments.
- j) Previamente à contratação de serviços relevantes de processamentos e armazenamento de dados e de computação em nuvem, adotar os procedimentos previstos na regulamentação do BACEN em vigor específica sobre o tema.
- k) Avaliar, previamente à contratação, empresas prestadoras de serviços que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução de atividades operacionais, assegurando que adotam procedimentos e controles voltados à prevenção e ao tratamento de incidentes em níveis de complexidade, abrangência e precisão compatíveis com os adotados pela OneKey Payments
- l) Estabelecer regras e padrões para assegurar que a informação receba o nível adequado de proteção quanto à sua relevância e confidencialidade. Toda informação relevante deve possuir um

proprietário, ser classificada e receber os devidos controles que garantam a sua confidencialidade, condizente com as boas práticas de mercado e regulamentações vigentes.

m) Adotar mecanismos para disseminação da cultura de segurança da informação e cibernética na OneKey, incluindo: (i) A implementação de programa de avaliação periódica de colaboradores quanto ao nível de conhecimento do tema segurança da informação e cibernética; (ii) A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos; (iii) Obtenção do comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança da informação e cibernética.

6. PROCEDIMENTOS DE SEGURANÇA

Para garantir a segurança das informações e ativos, a OneKey Payments utiliza diversos meios, como as políticas internas e instruções normativas, comunicados corporativos, controles tecnológicos, monitoração e a realização de testes e treinamentos periódicos de segurança da informação.

6.1. PROTEÇÃO E GERENCIAMENTO DO AMBIENTE FÍSICO

a) A OneKey Payments possui diversos controles e procedimentos para garantir a segurança física de suas instalações, conforme descrito nos tópicos abaixo:

GERENCIAMENTO DAS INSTALAÇÕES

- a) Os recursos e instalações de processamento de informações críticas para as atividades da OneKey Payments são mantidos em nuvem pública de notável reputação, a qual possui todos os níveis de segurança, redundância e disponibilidade exigidos por lei, além de proteção contratual.
- b) Este contexto torna menos crítica a proteção ao escritório e às instalações físicas, dado que nenhum ativo importante pode ser comprometido através da localidade do escritório.
- c) Ainda assim, a OneKey controla o acesso físico ao seu escritório, utilizando dupla barreira de autenticação:

Para entrada nas catracas e estacionamento do condomínio, utiliza:

- QR-Code de aproximação via aplicativo de celular

- Reconhecimento facial em sistema gerenciado pelo condomínio
- Reconhecimento de placa de veículo

Para entrada na sala comercial (escritório), utiliza:

- Reconhecimento facial gerenciado por sistema interno

Para entrada na sala de TI do escritório, utiliza:

- Reconhecimento facial gerenciado por sistema interno, com alto nível de restrição.

GERENCIAMENTO DE SERVIDORES

a) Os servidores que armazenam dados e sistemas críticos à operação da OneKey Payments são hospedados em Serviço de Nuvem que possui acessos controlados e monitorados, bem como garantia de alta disponibilidade dos ativos informacionais, inclusive quando acionado o Plano de Continuidade de Negócio – PCN.

b) Os provedores de serviços em nuvem ^{externo} devem aderir às Políticas pertinentes da OneKey Payments bem como atender às quaisquer solicitações desta instituição, além de garantir sua capacidade de resposta a incidentes e continuidade de negócio. Além disso, devem ter notória reputação de mercado.

GERENCIAMENTO DE DISPOSITIVOS

a) Informações de e-mails e arquivos dos colaboradores e terceiros que atuem na OneKey Payments são armazenadas em nuvem, contando com backups automáticos fornecidos pelos provedores, para proteção contra danos e perdas, bem como o acesso, uso ou exposição indevidos.

b) Observa-se que os ativos físicos devem utilizar apenas softwares licenciados ou autorizados pelo departamento de Tecnologia da OneKey, de modo que, em regra, os colaboradores não possuem privilégios administrativos para realizar instalações ou configurações em seu dispositivo.

c) Admite-se exceção à restrição dos privilégios administrativos nos seguintes casos: (i) colaboradores da área de tecnologia; (ii) colaboradores que utilizam MacBook.

d) Não é permitido aos colaboradores acessarem o leitor de DVD e/ou porta USB do computador.

As portas, inclusive, são bloqueadas pelas ferramentas de segurança corporativas.

e) É vedado ao colaborador utilizar computador corporativo, fornecido pela OneKey Payments, para desempenho de atividades que não sejam estritamente as necessárias para as entregas profissionais. Para tanto, a OneKey monitora todo o uso do computador, incluindo websites acessados, horários das atividades realizadas e, se aplicável, gravação de tela em tempo real.

f) Não implicará jornada, sobreaviso ou plantão do colaborador a mera possibilidade de acesso remoto, porte, uso ou recebimento de informações da OneKey Payments fora do horário de expediente por meio de dispositivos de mobilidade fornecidos pela OneKey Payments ou particular quando utilizados para finalidades profissionais, pois estes permanecem ativos ou disponíveis independentemente da vontade do colaborador ou comando da OneKey Payments. Assim, as atividades desempenhadas fora do expediente normal dependerão de comprovação expressa de requisição de trabalho em registros adequados para serem remuneradas.

INVENTÁRIO FÍSICO

O departamento de Segurança da informação deve efetuar um mapeamento dos ativos físicos e ativos de software da Instituição, além de identificar seu respectivo responsável. Este mapeamento é apoiado por ferramentas de inventário e descoberta eletrônica, sendo realizados de forma sistêmica e automática.

Convém executar periodicamente um inventário físico dos ativos, para identificar e corrigir desvios de informação relacionados ao uso de inventário eletrônico automatizado.

6.2 PROTEÇÃO E GERENCIAMENTO DE AMBIENTE LÓGICO

Todo acesso às informações e aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuamente, com papéis de responsabilidade claramente definidos. Os dados, as informações e os sistemas de informação das entidades devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir os objetivos desta política.

GESTÃO DE ACESSOS ÀS INFORMAÇÕES

A OneKey Payments segue as boas práticas no sentido de orientar que todos os usuários devem possuir acesso à informação de acordo com as necessidades de negócio, respeitando a segregação de função baseada em cargo/função. Todo funcionário, estagiário ou prestador de serviços possui apenas um identificador (login) de acesso à informação.

A OneKey Payments segue o princípio do mínimo acesso necessário, de modo a, sempre que possível, detalhar o nível de acesso para evitar concessões e permissões que não sejam estritamente necessárias para o desempenho das atividades.

AUTENTICAÇÃO

O controle de acesso aos sistemas deve ser formalizado e contemplar, no mínimo, os seguintes controles:

- i) A utilização de identificadores (credencial de acesso) individualizados, monitorados e passíveis de bloqueios e restrições (automatizados e manuais);
- ii) A remoção de autorizações dadas a ^{externo}usuários afastados ou desligados da Instituição, ou ainda que tenham mudado de função; e
- iii) A revisão periódica das autorizações concedidas.

Quando disponível, o acesso aos sistemas de informação da OneKey Payments é integrado a um controlador central de acessos (IAM) e realizado via senha única SSO (Single Sign-On).

Já para os sistemas que não puderem ser integrados ao IAM, deve existir um pré-requisito mínimo para as parametrizações de senhas, definidos mais abaixo, nesta política.

A área de Segurança da Informação tem permissão para realizar o gerenciamento das parametrizações de segurança, podendo alterar as configurações de acesso, senha e segurança, bem como bloquear contas que coloquem em risco o ecossistema de segurança.

CLASSIFICAÇÃO DA INFORMAÇÃO

- a) Todo Ativo da Informação deve estar associado a um proprietário e deverá ser classificado

com base em sua relevância e impacto para a OneKey.

b) A informação deve ser classificada e rotulada para indicar o nível esperado de proteção quando de seu tratamento.

c) As classificações possíveis, bem como o seu nível de proteção, são os seguintes:

- **Pública:** Informação cujo conteúdo pode ser livremente divulgado e disponibilizado para qualquer parte externa, sem nenhuma restrição
- **Interna:** Informação cujo conteúdo pode circular livremente dentro da instituição, por todos os seus colaboradores e departamentos, mas não pode ser divulgado, em nenhuma hipótese, para partes externas à organização
- **Restrita:** Informação que pode circular entre alguns departamentos, mas não pode ser divulgada para todos os colaboradores da instituição.
- **Confidencial:** Informação que circula entre um grupo muito restrito de pessoas (no máximo 3), mantida em sigilo para os demais colaboradores da organização.

Conforme a LGPD, informações que contenham dados pessoais e/ou sensíveis devem ser classificadas, no mínimo, como restritas e submetidas a controles adicionais de compartilhamento e DLP.

Interno

d) Quando possível e aplicável, a organização pode utilizar softwares e aplicativos que auxiliem a rotulação e a proteção de dados. Quando não aplicável, cabe ao colaborador rotular e compartilhar os arquivos e informações seguindo as diretrizes acima descritas.

CONCESSÃO, REVISÃO E REVOGAÇÃO DE ACESSOS

a) Sobre este tópico, a OneKey possui uma política dedicada ao assunto. Trata-se da **Política de Gestão de Acessos**.

SENHAS

a) Todas as senhas, de todos os sistemas, incluindo aqueles que não puderem ficar sob o SSO, atenderão aos seguintes requisitos:

- Mínimo de 12 caracteres.
- Máximo de 256 caracteres.
- Combinação obrigatória entre ao menos 3 entre os 4 grupos de caracteres abaixo:

- Letra maiúscula
- Letra minúscula
- Números
- Caracteres Especiais
- Não similar às últimas 10 senhas

b) Sempre que aplicável, será configurado um duplo fator de autenticação, preferencialmente através de código informado em aplicativo de celular e/ou confirmação via ação em tela.

c) As políticas de expiração de senhas são configuradas em conformidade com os requisitos estabelecidos pela norma ISO/IEC 27001, assegurando que as credenciais sejam submetidas a revisão e renovação periódicas conforme determinado pelos controles aplicáveis da norma.

d) Qualquer evento que considere uma credencial arriscada ou vazada terá a senha imediatamente alterada pelo departamento de Segurança da Informação

e) Credenciais de serviço, ou fora do IAM/SSO ou que não puderem ter o MFA habilitado sofrerão alteração no número mínimo de caracteres, passando a no mínimo 12 caracteres.

REDE

a) A segurança de rede é garantida por meio de recursos de monitoramento e controle de acesso disponibilizados pelas plataformas de nuvem utilizadas pela organização: Google Cloud e JumpCloud.

b) Não é permitida a conexão direta de terceiros. No caso de pastas compartilhadas com contas externas, estas terão que se utilizar dos requisitos de senha forte e autenticação de duplo fator parametrizados conforme nossas políticas.

c) O departamento de segurança da informação pode vedar o compartilhamento de pastas para contas que considere suspeitas ou inseguras.

d) Todos os arquivos criados, alterados, compartilhados e deletados das redes estão sob monitoramento do DLP e podem sofrer políticas de segurança definidas pela área de Segurança da Informação.

AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

Os requisitos de segurança de sistemas de informação devem ser identificados e acordados antes do seu desenvolvimento e/ou de sua implementação, para que assim possam ser protegidos visando a manutenção de sua confidencialidade, autenticidade ou integridade por meios criptográficos.

Todo o processo de aquisição, desenvolvimento e manutenção de softwares devem seguir as melhores práticas de Segurança da Informação e, quando desenvolvido internamente, ter varredura de vulnerabilidades através da ferramenta Snyk.

PROCESSAMENTO E ARMAZENAMENTO DE INFORMAÇÕES

Toda contratação de serviços de processamento e armazenamento de dados e de computação em nuvem devem estar aderentes com as diretrizes indicadas na Resolução BCB 85/2021.

Na contratação de serviços relevantes para processamento e armazenamento de dados e de computação em nuvem, o departamento de Segurança da Informação deve:

- i) Observar a contratação com aderência à estratégia, apetite e gestão de riscos da OneKey Payments;
- ii) Assegurar que o potencial prestador de serviço tenha capacidade de fornecer o produto/serviço dentro das especificações técnicas bem como garantir a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e informações processados ou armazenados;
- iii) Assegurar que o potencial prestador de serviço esteja em condições de cumprir a legislação vigente e fornecer à OneKey Payments, a qualquer tempo, o acesso aos dados e informações a serem processados ou armazenados;
- iv) Contratos de nuvem devem garantir o direito de acesso do BACEN aos dados e informações, bem como a segregação lógica entre ambientes/tenants, quando aplicável;
- v) Assegurar que o potencial prestador de serviço seja devidamente certificado para a prestação do serviço e disponibilize para OneKey Payments relatórios de auditoria independente – contratada pelo prestador – a respeito dos procedimentos e controles adotados na prestação do serviço;
- vi) Assegurar que o potencial prestador de serviço demonstre a identificação e segregação dos dados dos clientes da OneKey Payments por meio de controles físicos ou lógicos, bem como a qualidade dos controles de acessos voltados à proteção de dados e

informações dos clientes da instituição;

vii) Quando pertinente, comunicar ao Banco Central do Brasil a respeito das contratações de serviços relevantes de processamento e armazenamento de dados, bem como quaisquer alterações contratuais relevantes;

viii) Garantir que o contrato firmado entre as partes apresente de maneira clara a adoção de medidas de segurança para transmissão e armazenamento de dados, além da manutenção da segregação de dados e controle de acesso para proteção de informações dos clientes da OneKey Payments;

ix) Garantir que o contrato firmado entre as partes apresente de maneira clara as cláusulas, em caso de extinção, que versam sobre a transferência de dados e informações ao novo prestador de serviço bem como a exclusão dos mesmos após a transferência.

Todas as informações trocadas ou armazenadas nos recursos de informação da OneKey Payments independente do conteúdo, são de propriedade única e exclusiva da instituição.

BACKUP

a) Os arquivos armazenados nas nuvens corporativas da Google e da Microsoft estão protegidos pelas ferramentas de backup e restauração destas nuvens. Cópias de segurança e restauração seguem requisitos regulatórios e de continuidade.

b) Arquivos podem ser armazenados no computador, desde que nas pastas “Área de Trabalho” ou “Documentos”, que são sincronizadas com a ferramenta de nuvem Microsoft OneDrive

c) Arquivos armazenados fora destas pastas não estão sob proteção de backup e podem não ser recuperados, caso necessário.

COMPARTILHAMENTO DE INFORMAÇÕES

a) A OneKey Payments buscando sempre atuar com transparência e objetivando a melhoria dos seus procedimentos relacionados à Segurança Cibernética, tem o compromisso de compartilhar com o BACEN todos os incidentes relevantes, tempestivamente, sempre que solicitado.

PREVENÇÃO A VAZAMENTO DE INFORMAÇÕES

A OneKey possui mecanismos de controle para prevenção de perda de dados através de ferramenta

DLP, responsável por garantir que dados confidenciais não sejam perdidos, roubados, mal utilizados ou vazados na web por usuários não autorizados.

Os controles de DLP devem contemplar especificamente a proteção de dados pessoais, com regras de detecção, bloqueio e alertas para compartilhamento externo indevido, em aderência à LGPD.

GERENCIAMENTO DE AMEAÇAS E VULNERABILIDADES DE TI

- a) O ambiente possui instalado software de antivírus para a proteção contra vírus, arquivos e softwares maliciosos, atualizados periodicamente.
- b) Todas as atualizações de segurança do Windows são gerenciadas, priorizadas e atualizadas em frequência segura.
- c) A varredura de vulnerabilidades dos dispositivos é executada diariamente. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade

CRIPTOGRAFIA

- a) Toda solução de criptografia utilizada na OneKey Payments deve seguir as regras de Segurança da Informação e os padrões de segurança dos órgãos reguladores.
- b) Os dispositivos de usuário possuem criptografia ativada contra tentativas de acesso indevidos, perda ou roubo.
- c) As chaves de criptografia são armazenadas e gerenciadas pela área de Segurança da Informação

RASTREABILIDADE

- a) Trilhas de auditoria automatizadas devem suportar rastreabilidade e ser implantadas para todos os componentes de sistema, para reconstruir os seguintes eventos e ser utilizada como evidência de conformidade:
 - i) Autenticação de usuários (tentativas válidas e inválidas);
 - ii) Acesso a informações;
 - iii) Ações executadas pelos usuários, incluindo criação ou remoção de arquivos ou componentes de sistemas.

6.3 GERENCIAMENTO DE INCIDENTES

- a) A OneKey Payments entende que é de extrema importância a existência de um procedimento que possibilita a detecção tempestiva e a pronta comunicação de incidentes e vulnerabilidades, assegurando assim, a eficácia das medidas a serem tomadas na sequência. A OneKey Payments possui os controles que permitem detectar e identificar os incidentes e vulnerabilidades que afetam o ambiente de Segurança Cibernética.
- b) Os incidentes são armazenados e tratados: (i) dentro da console do Microsoft Defender, permanecendo lá pelo período de 6 meses OU; (ii) na ferramenta de ITSM GLPI, permanecendo armazenadas por tempo indeterminado.
- c) Na ferramenta GLPI são registrados os incidentes de segurança que não são detectados pelo ecossistema do Antivírus, Gestão de Vulnerabilidades e DLP.
- d) As responsabilidades em relação ao registro, análise e comunicação dos incidentes estão devidamente detalhadas em normativos específicos.

CLASSIFICAÇÃO DA CRITICIDADE DOS INCIDENTES

Os incidentes relacionados à Segurança Cibernética serão considerados críticos e prioritários em relação a quaisquer outros incidentes e tratados com máxima prioridade

A prioridade poderá ser reconsiderada quando, após a primeira análise, se considerar que não há risco iminente para a OneKey. Nestes cenários, o departamento de Segurança da Informação deve classificar a criticidade como baixa e pode direcionar esforços prioritários a outros assuntos

PLANO DE AÇÃO AOS INCIDENTES

- a) O Plano de Ação de Resposta a Incidentes está definido na política de Continuidade de Negócios.
- b) A elaboração e acompanhamento do plano de ação são coordenados pela Diretoria de TI e a Área de Segurança da Informação, com participação de outras áreas.
- c) O Plano de Ação e de Resposta a Incidentes Cibernéticos, que deve abranger:

Política de Segurança da Informação

OneKey Payments Instituição de Pagamento S.A.

- i) Mapeamento dos principais incidentes, tanto observado em base histórica quanto incidentes de probabilidade significativa;
- ii) As rotinas, os procedimentos, os controles e a tecnologia empregada na prevenção e na resposta aos incidentes mapeados;
- iii) Produção de relatório anual onde conste os incidentes registrados e a efetividade das ações adotadas, os resultados obtidos e quaisquer mudanças necessárias para evolução da cibersegurança.

TESTES DE INTRUSÃO

Testes de Intrusão interno e externo nas camadas de rede e aplicação devem ser realizados no mínimo anualmente.

TESTE DE CONTINUIDADE DE NEGÓCIOS

- a) A OneKey Payments assume o compromisso de manter a continuidade dos negócios em caso de incidentes que possam comprometer o funcionamento normal de suas atividades.
- b) O processo de continuidade de negócios é implementado com o intuito de reduzir os impactos e perdas de ativos da informação após um incidente crítico a um nível aceitável, por meio do mapeamento de processos críticos, análise de impacto nos negócios e testes periódicos de recuperação de desastres.
- c) Incluem-se nesse processo, a continuidade de negócios relativos aos serviços contratados na nuvem e os testes previstos para os cenários de ataques cibernéticos. Vide maiores informações na Política de Continuidade de Negócios da OneKey Payments.

7 PRESTADORES DE SERVIÇOS DE TI

Os procedimentos e controles voltados à prevenção e ao tratamento de incidentes em relação aos prestadores de serviço de Tecnologia da Informação – TI são previamente definidos em contratos, além disso, todos os contratos firmados com a OneKey Payments possuem termo (Non Disclosure Agreement – NDA) ou cláusulas de confidencialidade.

8 RECOMENDAÇÕES DE SEGURANÇA A CLIENTES E USUÁRIOS

AUTENTICAÇÃO E SENHA

O cliente/usuário é responsável pelos atos executados com seu identificador (login / sigla), que é único e acompanhado de senha exclusiva para identificação/autenticação individual no acesso à informação e aos recursos de tecnologia.

A área de Segurança da Informação recomenda a todos que:

- i) Mantenha a confidencialidade, memorize e não registre a senha em lugar algum. Ou seja, não contar a ninguém e não anotar em papel;
- ii) Alterar a senha sempre que existir qualquer suspeita do comprometimento dela;
- iii) Elaborar senhas de qualidade, de modo que sejam complexas e de difícil adivinhação;
- iv) Impedir o uso do seu equipamento por outras pessoas, enquanto este estiver conectado com a sua credencial;
- v) Bloquear sempre o equipamento ao se ausentar;
- vi) Habilitar um segundo fator de autenticação via aplicativo de autenticação.

PHISHING

a) O *phishing* é uma técnica utilizada por cibercriminosos para enganar os usuários por meio de envio de e-mails maliciosos, a fim de obter informações pessoais como senhas, cartão de crédito, CPF, número de contas bancárias, entre outros. As abordagens dos e-mails de *phishing* podem ocorrer das seguintes maneiras:

- i) Quando procuram atrair as atenções dos usuários, seja pela possibilidade de obter alguma vantagem financeira, seja por curiosidade ou seja por caridade;

- ii) Quando tentam se passar pela comunicação oficial de instituições conhecidas como: Bancos, Lojas de comércio eletrônico, entre outros sites populares;
- iii) Quando tentam induzir os usuários a preencherem formulários com os seus dados pessoais e/ou financeiros, ou até mesmo a instalação de softwares maliciosos que possuem o objetivo de coletar informações sensíveis dos usuários;

b) Sempre que desconfiar de algum e-mail fraudulento, ou qualquer outra forma de comunicação, acionar o departamento de Segurança da Informação para análise antes de clicar sobre qualquer link ou anexo, ou antes de fornecer qualquer informação.

c) Periodicamente, a OneKey Payments realiza testes simulados de Phishing, para treinamento de seus funcionários e medição de seus riscos de cair nesta tentativa de fraude.

SPAM

- a) A OneKey possui filtro antispam ativado, para bloquear remetentes indesejados.
- b) Os usuários devem enviar remetentes indesejados para o time de Segurança da Informação, que providenciará os bloqueios.
- c) A mesma ferramenta e procedimento servirá para bloquear remetentes de Phishing

VPN

- a) A OneKey disponibiliza VPN para seus colaboradores acessarem os principais sistemas que possuem dados sensíveis, dentre os quais (mas não só) o ERP Matera e o sistema BackOffice.
- b) A autenticação na VPN se dá mediante SSO com o mesmo usuário utilizado para login no computador e nos principais serviços.
- c) O uso do acesso via VPN deve ser restrito e utilizado para as finalidades relacionadas com os negócios devendo abster-se de usar a funcionalidade para quaisquer outras atividades, sendo vetado aos usuários do serviço compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros

funcionários.

9 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.

10 SANÇÕES

A área de Segurança da Informação realiza o monitoramento contínuo do ambiente tecnológico por meio de métodos diversos para assegurar a conformidade e adesão a esta Política. Caso haja violação das regras nela dispostas, bem como às demais normas e procedimentos de Segurança da Informação, mesmo que por omissão ou tentativa não consumada, tal violação pode ser classificada como incidente de segurança cibernética, os quais são passíveis de penalidades.

11 COMUNICAÇÃO

Interno

Quaisquer indícios de irregularidades no cumprimento das determinações desta política serão alvo de investigação interna e devem ser comunicadas imediatamente para o departamento de segurança da informação

Sanções administrativas e/ou legais poderão ser adotadas, sem prévio aviso, podendo culminar com o desligamento e eventuais processos, se aplicáveis. O infrator poderá ser notificado e a ocorrência da transgressão imediatamente comunicada ao seu gestor imediato e a Diretoria.

12 **PUBLICAÇÃO**

A aprovação desta política é fundamental para manutenção da licença operacional e para a segurança dos ativos da OneKey Payments.

Esta política é revisada e aprovada pela Diretoria anualmente ou em prazo menor em caso de alteração de legislação que regule o assunto, ou ainda em casos de alteração nas estratégias de negócios, assuntos societários que justifiquem.

Esta política após aprovada entra automaticamente em vigor na data de sua aprovação.

Interno