PicPay	**Área responsável:** Segurança Cibernética
Política	**Classificação:** Externa
	Site: 01
SEGURANÇA CIBERNÉTICA	

Índice

1. Objetivo

Esta Política de Segurança Cibernética (“Política”), tem por objetivo estabelecer diretrizes e orientar os Colaboradores, Parceiros, Clientes e Prestadores de Serviços sobre as regras para assegurar a aplicação de controles e medidas administrativas necessárias para proteger as Informações de propriedade ou responsabilidade das entidades PicPay Instituição de Pagamento S.A., PicPay Bank- Banco Múltiplo S.A., PicPay Invest DTVM S.A, Cred novo SEP S.A e de todas as suas respectivas subsidiárias (entidades controladas direta ou indiretamente), doravante referidas como (“Grupo PicPay”), para fins de atendimento as principais normativas vigentes do Branco Central do Brasil e demais Órgãos competentes.

2. Fórum de Aprovação

Esta Política é aprovada pelo Comitê de Diretoria.

3. Vigência

Esta Política terá vigência de 1 (um) ano, ou, em menor prazo, quando o fórum responsável que a aprovou considerar necessário, tendo por início a data de aprovação do Comitê de Diretoria.

4. Aplicação e Público-Alvo

Esta Política se aplica, no Brasil e no Exterior, às empresas do Grupo PicPay bem como, a todos os seus administradores e colaboradores, incluindo também qualquer interação com clientes, parceiros, fornecedores e demais públicos de relacionamento.

5. Definições e Abreviaturas

Para melhor entendimento desta Política, listamos em ordem alfabética, os principais conceitos referidos neste documento, de forma a evitar dificuldades de interpretação ou ambiguidades:

Ativo de Informação: Qualquer recurso que tenha a condição de processar, armazenar ou transmitir as informações.

Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano para os sistemas ou informações da companhia.

Backup: Processo de cópia de dados de um dispositivo de armazenamento para outro com o objetivo de proporcionar a proteção contra a perda dos originais.

Controle de Acesso: São barreiras lógicas ou físicas que impedem ou limitam o acesso à informação, bem como protegem as mesmas de modificações não autorizadas.

Colaborador: Denominação dada à pessoa contratada cujo vínculo de cunho empregatício é regido pela CLT - Consolidação das Leis do Trabalho.

Criptografia: Técnicas utilizadas para transformar a informação da sua forma original para outra ilegível, de forma que possa ser conhecida apenas por seu destinatário (detentor da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado.

Classificação da Informação: Processo que tem como objetivo identificar e definir níveis e critérios adequados para a proteção das informações, de acordo sua importância para as organizações.

Código-fonte: Um conjunto de arquivos de texto contendo todas as instruções que devem ser executadas pelo computador de forma lógica numa linguagem de programação.

6. Diretrizes

A Política de Segurança Cibernética estabelece as diretrizes que, norteiam a implementação de controles, processos e procedimentos voltados a segurança cibernética no Grupo PicPay, seguindo os seguintes princípios:

I. **Confidencialidade:** garantia de que toda Informação estará acessível apenas para pessoas autorizadas, garantindo o conceito de "mínimo privilégio possível".
II. **Integridade:** garantia de que a informação, armazenada ou em trânsito, seja completa, exata e não sofrerá qualquer modificação ou exclusão não autorizada.
III. **Disponibilidade:** garantia de que a Informação sempre estará disponível quando necessário; e
IV. **Autenticidade**: garantia da veracidade da informação, certificando que a Informação é verdadeira e que não sofreu alteração em seu ciclo de vida.

6.1 Gestão de Riscos Cibernéticos

O Grupo PicPay adota processos para identificar, avaliar, corrigir e monitorar riscos cibernéticos. Analisamos a criticidade e o impacto de cada risco cibernético, adotando ações para mitigação e revisão periódica para garantir conformidade com as melhores práticas de segurança.

6.2 Gestão de Ativos e Tratamento de Informações

As informações do Grupo PicPay são classificadas e protegidas dentro dos Ativos de Informação conforme sua sensibilidade e importância para o negócio.

6.3 Postura de Segurança

A postura de segurança se fundamenta na prevenção e na prontidão para responder a riscos cibernéticos, no monitoramento contínuo das ameaças, na aplicação de boas práticas de segurança e na busca da melhoria contínua dos processos de segurança.

6.4 Controle de Acesso Lógico

Os controles de acesso lógico são implementados com o objetivo de controlar os acessos às informações sensíveis, aplicando, portanto, o princípio do menor privilégio, com revisões periódicas de autorizações onde é possível assegurar a adequação dos acessos.

6.5 Controle de Acesso Físico

Mantemos o controle de acesso físico às instalações do Grupo PicPay mediante a cadastros e autorização, além de identificação única por meio de crachás e o uso de biometria, quando necessário.

6.6 Monitoramento, Controle e Auditoria

O Grupo PicPay utiliza mecanismos para garantir a rastreabilidade das informações, este monitoramento contínuo das ações no ambiente tecnológico nos permite identificar e corrigir possíveis falhas, garantindo a rastreabilidade e proteção de dados.

6.7 Gestão de Ameaças e Incidentes

O Grupo PicPay possui processos e mecanismos que realizam o monitoramento contínuo de ameaças em nossos Ativos de Informação garantindo a identificação e eliminação que possam resultar em comprometimento das nossas informações.

6.8 Segurança nas Operações

O Grupo PicPay desenvolve mecanismos que garantam que nossos produtos e serviços oferecidos aos nossos usuários estejam sempre disponíveis e protegidos de falhas ou indisponibilidades utilizando protocolos robustos de criptografias e revisões periódicas de

vulnerabilidades.

6.9 Continuidade de Negócios

O Grupo PicPay possui estratégias de continuidade de negócios para processos críticos, onde são avaliados e testados regularmente para garantir que os serviços permaneçam ativos em situações de crise.

6.10 Gestão de Fornecedores, Prestadores de Serviços e Parceiros

O Grupo PicPay possui processos e metodologia que garantem a avaliação de seus fornecedores, parceiros e prestadores de serviços a fim de identificar possíveis riscos cibernéticos que possam comprometer os princípios de segurança da informação.

6.11 Redes e Comunicações

O Grupo PicPay adota medidas adequadas de proteção de rede e meios de comunicação para garantir o acesso seguro para colaboradores e terceiros autorizados.

6.12 Desenvolvimento Seguro e Adoção de Novas Tecnologias

O Grupo PicPay adota práticas de desenvolvimento seguro durante o ciclo de vida do desenvolvimento em seus produtos e serviços. Controles capazes de identificar e corrigir as vulnerabilidades são praticados em todo ambiente tecnológico.

6.13 Gestão de Conformidade de Segurança

O Grupo PicPay implementa processos e procedimentos robustos para identificar potenciais desvios de conformidade em relação aos requisitos de segurança da informação, atendendo às regulamentações aplicáveis e alinhados às melhores práticas de mercado.

6.14 Cultura e Conscientização

O Grupo PicPay estabelece de forma contínua treinamentos sobre segurança da informação para colaboradores e prestadores de serviços, reforçando a importância da segurança e promovendo boas práticas através de campanhas de conscientização regulares.

6.15 Demandas Regulatórias

O Grupo PicPay é está comprometido com o cumprimento das regulamentações locais e internacionais, incluindo à Lei 13.709/2018 que trata de proteção à dados pessoais de todas as pessoas físicas que fazem parte deste ecossistema, além de realizar avaliações periódicas para garantir a conformidade e mantermos os registros documentados para revisão regulatória.

6.16 Violação da Política Cibernética e Sanções

O Grupo PicPay entende que a violação das diretrizes desta Política constitui falta grave, sujeitando os responsáveis a medidas administrativas e judiciais cabíveis. Incidentes de segurança ou desvios de conduta são registrados e avaliados, podendo resultar em sanções após análise pela área de Compliance e Jurídico.

7. Normativos Internos Vinculados

Esta Política foi desenvolvida com base nos principais Frameworks de Segurança Cibernética, a fim de atender às diretrizes de Segurança estabelecidas pelo Banco Central do Brasil e outras entidades reguladoras.

a) Resolução BCB no 85/2021;
b) Resolução CMN no 4.893/2021;
c) LGPD - Lei Geral de Proteção de Dados 13.709/2018;
d) CVM - Instrução de Comissão de Valores Mobiliários no 35/2021;
e) NIST - National Institute of Standards and Technology;
f) ISO/IEC 27001:2022 e ISO/IEC 27002:2022;
g) PCI DSS - Payment Card Industry – Data Security Standard;
h) ISO/IEC 27005:2023.

8. Anexos

N/A

10. Histórico de alterações

Tópico alterado	Detalhamento	Data da alteração
N/A	Criação do Documento	04/11/2024