PicPay

POLÍTICA

Segurança da Informação

1. Objetivo

Estabelecer diretrizes de segurança da informação, a fim de garantir a confidencialidade, integridade e disponibilidade das informações de propriedade ou responsabilidade do PicPay.

Visa também prevenir, detectar e reduzir as vulnerabilidades inerentes ao ambiente cibernético do PicPay, através de processos, tecnologias e pessoas.

2. Escopo

Devem ser cumpridas por todos os colaboradores, parceiros e fornecedores de serviço, abrangendo todas as informações e o ambiente computacional do PicPay.

3. Estrutura

A área de Segurança da Informação, sob gestão do Diretor de Tecnologia e Produtos, é responsável por zelar pela aplicação das diretrizes desta política.

4. Atribuições

Os **Diretores estatutários** devem zelar pelo cumprimento das diretrizes estabelecidas nesta política através de suas alçadas competentes, bem como por comprometer-se, na medida do possível, na dedicação de recursos que permitam a adequada gestão da segurança da informação e evolução do Plano Diretor de Segurança da Informação.

A área de **Segurança da Informação** é responsável pela adoção e implementação de tecnologias, processos e controles que possam garantir ao PicPay salvaguardar seus ativos de informação, além de ser responsável por orientar e informar os colaboradores, parceiros, fornecedores e prestadores de serviços, sobre a comunicação de possíveis incidentes e/ou violações das diretrizes da presente política.

A área de **Governança de Segurança da Informação** é responsável por estabelecer e manter um modelo de gestão de Segurança da Informação, através da adoção de um *framework*, com intuito de apoiar as estruturas de gestão e processos para garantir a conformidade com as diretrizes de segurança e aderência às regulamentações necessárias.

A área de ***Compliance*** é responsável pela divulgação desta Política aos colaboradores e deve ser envolvida sempre que houver qualquer descumprimento das diretrizes expostas nessa Política, para avaliar e direcionar as medidas cabíveis.

A área de **Pessoas & Cultura (P&C)** deve cumprir os controles de segurança da informação relacionados aos processos de contratação, encerramento e modificação das atividades dos colaboradores, bem como atuar em análises sempre que houver qualquer descumprimento destas diretrizes.

A área de **Assuntos Legais** é responsável por envolver, sempre que necessário, a área de segurança da informação em contratações para a avaliação e posterior inclusão do Anexo de Segurança da Informação, além de prestar o devido apoio em questões jurídicas e atuar em análises sempre que houver qualquer descumprimento destas diretrizes.

A área de **Privacidade** é responsável por estabelecer regras de tratamentos de dados com base na legislação vigente, bem como envolver a área de segurança da informação em questões de compartilhamento, processamento e armazenamento de dados pessoais e dados pessoais sensíveis, sempre que necessário.

5. Diretrizes de Segurança da Informação

As diretrizes são os princípios adotados, para mitigar os riscos de segurança e atingir os objetivos definidos com base nos pilares de segurança da informação, sendo eles:

I. Confidencialidade: Garantia de que toda informação estará acessível apenas para pessoas autorizadas;
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.

Os controles adotados pelo PicPay para garantir que as diretrizes e objetivos sejam cumpridos são:

5.1. Uso Aceitável de Recursos Tecnológicos

Os recursos disponibilizados aos colaboradores devem ser utilizados somente para fins profissionais e em conformidade com o Código de Ética e Conduta - CODEC.

O PicPay, através das áreas responsáveis, reserva-se ao direito de monitorar e auditar, sem aviso prévio, todos os ativos disponibilizados.

5.2. Controle de Acesso

Os acessos físicos devem ser protegidos por controles apropriados de entrada e saída, com o objetivo de assegurar que somente pessoas autorizadas tenham acesso às instalações e as dependências do PicPay, além de serem devidamente monitorados e os respectivos registros serem protegidos.

Os acessos lógicos devem ser centralizados e gerenciados pela Área de Segurança da Informação. Deve-se incluir, identificação, autenticação garantindo a gestão sobre o ciclo de vida da identidade e respeitando o princípio de menor privilégio possível.

5.3. Rastreabilidade da Informação

Os ativos tecnológicos do PicPay, como por exemplo, sistemas e aplicações devem ser capazes de gerar trilhas de auditoria com as informações necessárias para a identificação adequada das ações desempenhadas.

Todos estes registros devem ser armazenados por um período estabelecido, com acesso restrito, proteção de adulteração e analisados regularmente.

5.4. Classificação e Proteção da Informação

Todas as informações do PicPay devem ser classificadas, protegidas e monitoradas conforme o procedimento de classificação da informação, de acordo com o seu grau de sensibilidade para o negócio e não sendo permitido ao colaborador, fornecedor e prestador de serviço compartilhar informações internas, restritas e confidenciais, exceto quando expressamente autorizado.

A Área de Segurança da Informação deve aplicar controles, processos e tecnologias que identifiquem e previnam de forma tempestiva o vazamento de dados e compartilhamento de informações de forma não autorizada.

5.5. Incidentes de Segurança da Informação

Devem ser empregados controles e processos que garantam a devida prevenção, detecção e tratamento de incidentes de segurança da informação. Todo incidente de segurança da informação deve ser identificado a partir do monitoramento de segurança ou reportado por colaboradores, fornecedores ou prestadores de serviços, posteriormente sendo classificado e priorizado de acordo com o impacto técnico, serviços e operações, considerando a criticidade dos recursos e usuários afetados de acordo com o Procedimento de Resposta à Incidentes de Segurança da Informação.

O PicPay tem o compromisso com a transparência e se compromete a compartilhar com as autoridades regulatórias todos os incidentes relevantes, bem como atender a quaisquer solicitações adicionais que possam contribuir para a resolução de questões que ainda não foram prontamente resolvidas.

Em conformidade com as diretrizes estabelecidas pelo Banco Central do Brasil, será disponibilizado um relatório anual de incidentes de segurança da informação, considerando todos os aspectos desde a identificação e a tratativa do incidente.

5.6. Gestão de Ameaças

Todos os ativos tecnológicos do PicPay devem possuir mecanismos de detecção e proteção contra ameaças em sua versão mais atual disponível. A área de Segurança da Informação tem autonomia para caso necessário, tomar medidas para combater ou prevenir a disseminação de agentes maliciosos. Além destes mecanismos, devem ser empregados controles que garantam a prevenção e detecção de intrusão.

5.7. Segurança nas Operações

Deve-se empregar o uso de criptografia robusta sempre que possível, sendo estritamente necessário quando envolver dados pessoais, dados pessoais sensíveis, dados de cartão de crédito ou quaisquer outras informações relevantes ou críticas para o negócio, sejam dados em trânsito ou em repouso.

A Área de Segurança da Informação deve realizar de forma periódica e contínua varreduras de vulnerabilidades no ambiente tecnológico do *PicPay*, comunicando às áreas responsáveis para a devida

correção e acompanhando os ajustes com base no prazo estabelecido levando em consideração a severidade de cada vulnerabilidade.

A Área de Segurança da Informação é responsável por acompanhar o processo de backup periodicamente e verificar a realização das cópias e testes de restauração das informações.

5.8. Fornecedores e Prestadores de Serviço

Todos os fornecedores e prestadores de serviço devem, previamente à contratação e periodicamente após a contratação, serem avaliados sobre seus controles, processos e tecnologias de segurança da informação com o objetivo de identificar e acompanhar se o seu nível de maturidade atende os requisitos estabelecidos pelo PicPay e quando necessário, pelas as entidades reguladoras, incluindo sobre os procedimentos e controles voltados à prevenção e tratamento de incidentes.

5.9. Redes

A Área de Segurança da Informação é responsável por assegurar a existência, conformidade e aplicação de controles de segurança para a proteção adequada de sua rede, devidamente monitorada e segregada, fisicamente ou logicamente, quando aplicável.

5.10. Desenvolvimento Seguro e Adoção de Novas Tecnologias

A Área de Segurança da Informação deve zelar para que durante o ciclo de desenvolvimento seguro, assim como na adoção de novas tecnologias, existam controles e processos capazes de identificar vulnerabilidades e corrigi-las antes da entrada em produção. Os ambientes devem ser segregados conforme procedimento de desenvolvimento seguro.

5.11. Conformidade

A área de Segurança da Informação é responsável pela conformidade de seus processos, controles e tecnologias, devendo testá-los, medindo sua eficiência através de indicadores e aplicando melhorias na medida do possível. Além disso, riscos de segurança da informação que sejam identificados devem ser endereçados para tratamento a fim de serem mitigados ou eliminados.

5.12. Cultura de Segurança da Informação

A Área de Segurança da Informação é responsável pela implementação de um programa de treinamentos e ações de conscientização de segurança da informação que visam capacitar e avaliar todos os colaboradores, fornecedores e prestadores de serviço. Além disso, é responsável por elaborar e divulgar um programa de prestação de informação na utilização de produtos e serviços do PicPay.

6. Disposições Gerais

6.1. Sanções e Penalidades

O não cumprimento desta política e demais procedimentos de segurança da informação, poderá incorrer em sanções administrativas e/ou legais, podendo culminar com o desligamento e eventuais processos criminais, se aplicável.
A área de Segurança da Informação é responsável por avaliar o grau de criticidade da violação, e solicitar o envolvimento de outras para a análise das punições cabíveis, como a área de P&C, *Compliance* e Assuntos legais.